Symantec™ Enterprise Security Manager Microsoft SQL Modules Installation Guide

Version 4.1.2

Symantec

Symantec™ Enterprise Security Manager Microsoft SQL Modules Installation Guide

Documentation version: 4.1.2

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

Chapter 1

Installation and configuration of MS SQL Server Databases

This chapter includes the following topics:

Before you install

Before you install Symantec ESM SQL Server modules for MS SQL Server 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 superuser 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.
ESM Security Update 17	SU 17 or later versions must be installed on the computer where Symantec ESM manager is installed.
SQL Client Tools	The following MS SQL Client Tools must be installed on each Symantec ESM agent where the modules must run: ■ Management tools ■ Client connectivity You need not install any other components of the MS SQL Client Tools on the agents.

System requirements

Table 1-1 lists the operating systems on which the ESM application modules for MS SQL Server can report.

Note: As per Symantec's End of Life product support policy, the ESM MS SQL Server Release 4.0 or later are not supported on ESM 6.0 and 6.1.

Table 1-1 Supported MS SQL versions and operating systems

Supported operating systems	Supported OS versions	Architecture	Supported MS SQL versions
Windows	2003	x86 and x64	2005, 2008, 2008 R2, 2012
Windows	2003 R2	x86 and x64	2005, 2008, 2008 R2, 2012
Windows	2008	x86 and x64	2005, 2008, 2008 R2, 2012

Table 1-1 Supported MS SQL versions and operating systems *(continued)*

Supported operating systems	Supported OS versions	Architecture	Supported MS SQL versions
Windows	2008 R2	x64	2005, 2008, 2008 R2, 2012

Table 1-2 lists the cluster support on Windows.

Table 1-2 Cluster support on Windows

Supported operating systems	Architecture	Supported OS versions	Supported MS SQL versions
Windows	x86, x64	2003	2005, 2008, 2008 R2
Windows	x64	2008 R2	2005, 2008, 2008 R2

Table 1-3 lists the disk space requirements for Symantec ESM SQL Server modules for MS SQL Server Databases.

Table 1-3 Disk space requirements

Operating system	Hard disk space
Windows 2003 (32-bit)	90 MB
Windows 2003 (64-bit)	116 MB
Windows 2008 (32-bit)	90 MB
Windows 2008 (64-bit)	130 MB

About installing the ESM SQL Server modules for MS SQL Server Databases

You can install the MS SQL Server Databases module on the ESM agent computer by using the esmmssqltpi.exe.

The installation program does the following:

- Extracts and installs module executables, configuration (.m) files, and the template files.
- Registers the .m and the template files by using the ESM agent's registration program.

Note: You can skip this step if you have already registered the package for other agents that are installed on the same platform.

To install the ESM SQL Server modules for MS SQL Server Databases

1. From the product disc, run \Databases\MSSQL\Modules\<architecture>\esmmssqltpi.exe.

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

2. Choose one of the following option:

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

3. The **Do you want to register the template or .m files?** message appears. Do one of the following:
   - Type a Y, if the files are not registered with the manager.
   - Type an N, if the files have already been registered and skip to See "To configure for the MS SQL Server Databases on the ESM agent computers" on page 13.

Note: You must register the template and the .m files once for the agents that use the same manager on the same operating system.

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

   Usually, it is the name of the computer that the manager is installed on.
5. Enter the ESM access name (logon name) for the manager.
6. Enter the ESM password that is used to log on to the ESM manager.
7. Enter the network protocol that is used to contact the ESM manager.
8. Enter the port that is used to contact the ESM Manager. The default port is 5600.
9. 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.
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.

When the extraction is complete, you are prompted to add configuration records to enable the ESM security checking for your MS SQL Server Databases.

11 The **Continue and add configuration records to enable ESM security checking for your MS SQL Server? [yes]** message appears. Do one of the following:

- Type a **Y**, to configure the ESM SQL Server modules on the agent computer. The installation program reads the existing configuration records and displays them.
- Type an **N**, the program installation continues without configuration.

When the extraction is complete, you are asked if you want to add configuration records to enable ESM security checking for your SQL servers.

To configure for the MS SQL Server Databases on the ESM agent computers

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

- Type a **Y**, to continue the installation.
  The installation program automatically detects broadcasting SQL servers and displays them in a list
- Type an **N**, to end the installation without adding the security checks.

2 The **Would you like to continue [This action will erase the existing server configuration records]? [yes]** message appears. Do one of the following:

- Type a **Y**, to continue the installation and add a configuration record for each displayed server.
- Type an **N**, to find another server

3 Verify the SQL Server name by pressing Enter, or type an alias.

You must enter the SQL Server name in the format: MachineName\InstanceName. If the SQL server is installed on a clustered node, then you must enter the SQL Server name in the format: VirtualServername\Instancename.

4 Enter the Login ID that is used to log on to the SQL Server.

Note: If your SQL Server is configured to use mixed mode authentication, you can use either SQL login or Windows login. When entering a Windows authentication user ID, use the <domain>\<username> format. The Windows user must also be able to log on to the local Symantec ESM agent computer.

5 Enter the password of the SQL login or the Windows login that you use to log on to the designated SQL Server.

6 Retype the password for verification.

The program displays the added SQL server details.

7 The **Is this information correct? [yes]** message appears. Do one of the following:

- Type a **Y**, if the displayed information is correct.
- Type an **N**, if the displayed information is incorrect and re-enter the required information.

8 The **Do you want to validate this SQL Server connection? [yes]** message appears. Do one of the following:

- Type a **Y** to verify the SQL server connection.
  A message is displayed that the connection validation is successful.
- Type an **N** to skip the verification of SQL server connection.

9 Repeat steps 2–6 until you have installed the security checks or skipped the installation for every SQL Server that the installation program has found.

Note: The encryption that is used to store the credentials is 256-bit AES encryption algorithm.

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 **esmmssqlcontenttpi.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 1-4 shows the file types and folder paths of the Application modules.

Table 1-4 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 **esmmssqlcontenttpi.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 **esmmssqlcontenttpi.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 17.
   - 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 esmmssqlcontenttpi.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 - Microsoft SQL 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 Microsoft SQL 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 MSSQL Applcation modules type the following command:

  ```
  importcontent -L MSSQL -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 MSSQL, type the following command:

  ```
  importcontent -T -L MSSQL -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 SQL Server modules for MS SQL Server Databases

You can silently install the Symantec ESM SQL Serevr modules for MS SQL Server Databases by using the command line options with esmmssqltpi.exe.

Table 1-5 lists the command line options for silently installing the ESM modules for MS SQL Server Databases.

Table 1-5 Options to silently install the ESM SQL Server modules for MS SQL Server Databases

Option	Description
-i	Install this tune-up/third-party package
-d	Display the description and contents of this tune-up/third-party package
-U	Specify the ESM access record name
-P	Specify the ESM access record password
-p	Specify the TCP port to use
-m	Specify the ESM manager name
-t	Connect to the ESM manager by using TCP
-x	Connect to the ESM manager by using IPX (Windows only)
-g	Specify the ESM agent name to use for registration
-K	Do not prompt for and do the re-registration of the agents
-n	No return is required to exit the tune-up package (Windows only)
-N	Do not update the report content file on the manager
-Y	Update the report content file on the manager
-e	Do not execute the before and after executables (install the ESM modules for MS SQL Server databases without configuring).

To silently install the ESM modules for MS SQL Server Databases and configure MS SQL Server, type the following at the command prompt:

```
esmmssqltpi.exe -it -m <manager name> -U <Username> -p <port no> -P
<password> -g <agent name > -Y -n -e
```

If the installation succeeds, the return value is 0. If the installation fails, the return value is 1.

Post-installation tasks

After installation, you can begin using Symantec ESM Modules for MS SQL Server Databases.

Agent registration

Each Symantec ESM agent must reregister with a Symantec ESM manager. The esmmssqltpi.exe program prompts you for the required information when the agent is installed with new modules.

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

If connection errors are reported while running security checks, examine the \\<Install directory>\ESM\config\manager.dat file on the agent. You can add the manager's fully-qualified name to the file or, if the file is missing, manually reregister the agent to the manager.

Configuration of the ESM SQL Server modules for MS SQL Server Databases

After installing Symantec ESM SQL Server modules for MS SQL Server Databases, you can edit the configuration records. A configuration record is created for each MS SQL Server Database when you enable the security checking during installation.

Editing the configuration records

You can add, modify, remove, reconfigure the SQL database instances that Symantec ESM includes in security checks by using the MSSQLSetup.exe program. By default, MSSQLSetup.exe is located in the \\<Install directory>\ESM\bin\<platform> directory.

Table 1-6 lists the options that you can use when running the MSSQLSetup.exe program in the interactive mode.

Table 1-6 Editing configuration records

To do this	Type
Display help.	MSSQLSetup -h
Create new configuration records for detected MS SQL servers.	MSSQLSetup -c
Add a configuration record for undetected MS SQL servers.	MSSQLSetup -a
Modify existing MS SQL Server configuration records.	MSSQLSetup -m
List existing MS SQL Server configuration records.	MSSQLSetup -l
Remove specified SQL Server instance from configuration records	MSSQLSetup -r
List the MS SQL Servers instances that are available in the network	MSSQLSetup -C
List the MS SQL Server instance and cluster instances that are installed on the ESM agent computer. Prompt for configuration of the MS SQL server and instances that are installed on the ESM agent computer.	MSSQLSetup -i
List the MS SQL Server instance and cluster instances that are installed on the ESM agent computer, from which a user runs the MS SQL setup.	MSSQLSetup -I
Add configuration records for the generic credentials.	MSSQLSetup -G

Note: If no option is specified, MSSQLSetup.exe program runs with the -C option. For host-based deployments, use MSSQLSetup.exe -i. For network-based deployments, use MSSQLSetup.exe -c.

Use the redirection operator '>' to redirect the output of the following commands into a file:

- MSSQLSetup.exe -C
- MSSQLSetup.exe -I

Editing the .m file

Module configuration (.m) files contain the message information that ESM uses to report security check results.

For instructions for editing .m files, see the *Symantec Enterprise Security Manager Security Update User's Guide*.

Silently configuring the Symantec ESM SQL Server mModules for MS SQL Server Databases

You can silently configure the Symantec ESM SQL Server modules for MS SQL Server Databases by using the MSSQLSetup.exe.

Table 1-7 lists the command line options for silently configuring the ESM SQL Server modules for MS SQL Server Databases.

Table 1-7 Options for silently configuring the MS SQL Server Databases

To do this	Type
Specify the name of the SQL Server or the instance.	MSSQLSetup -S
Specify the name of the user to connect to the SQL Server.	MSSQLSetup -A
Specify the ClearTextPassword.	MSSQLSetup -P
Remove the configuration record.	MSSQLSetup -r
Specify the file name which that contains the encrypted generic credential record.	MSSQLSetup-gif <infile>
Specify the file name that should be created with the encrypted generic credentials record.	MSSQLSetup-gof <outfile>
Skip connection validation.	MSSQLSetup -sv
Import or export all the server configuration records.	MSSQLSetup {-sif|-sof} -all
Export the existing configuration records of local cluster instances to an output file. If you specify '-sof' switch with 'all' option, then all the configuration records that are available within the module's configuration file are exported.	MSSQLSetup -sof

Table 1-7 Options for silently configuring the MS SQL Server Databases *(continued)*

To do this	Type
Import the configuration records of local cluster instances from the input file. If you specify '-sif' switch with 'all' option, then all the configuration records that are available within the input file are imported.	MSSQLSetup -sif

To silently configure the MS SQL Server, type the following at the command prompt:

```
Mssqlsetup.exe -S <SQL Server Name\Instance name> -A <user name to
connect to SQL Server> -P < ClearTextPassword>
```

To silently configure the MS SQL Server without validating the server, type the following at the command prompt:

```
Mssqlsetup.exe -S <SQL Server Name\Instance name> -A <user name to
connect to SQL Server> -P < ClearTextPassword> -sv
```

If the installation succeeds, the return value is 0. If the installation fails, the return value is -1.

Specify the user name that is used to connect to the MS SQL Server using Windows authentication in the following format:

<domain name\user name> OR <machine name\user name>

You can configure only one instance at a time. For the default instance, only the MS SQL Server name needs to be specified.

To remove MS SQL Servers that have been configured, type the following at the command prompt:

```
Mssqlsetup.exe -r <SQL Server Name\Instance name>
```

For the default instance, only the MS SQL Server name needs to be specified.

After running the MSSQLSetup.exe, logs are created in \\<Install directory>\ESM\system\<machine name>.

Configuring the ESM modules for MS SQL Server clusters (Not used in MSSQL 4.1 deliverable)

You should consider the following before you configure the ESM modules for MS SQL Server clusters:

- Install ESM MSSQL modules in the Network mode.

Do not install the ESM MSSQL modules on the computers that are present in the cluster.

- Provide a virtual name or virtual IP for the MS SQL Server.

Configuring the SQL Server by using the SQL Server SQL Server Discovery module

The ESM SQL Server Discovery module is a host-based module that automates the process of detection and configuration of new server instances that are not yet configured on the local ESM agent computers.

The ESM SQL Server Discovery module does the following:

- Detects the new local server and cluster instances and let them be configured.
- Detects the unreachable and the deleted server instances that are still configured on the ESM agent computers.
- Lets you delete the unreachable server instances from the ESM agent computers.

Configuring a new SQL Server instance

To report on the SQL Server, you must first configure the SQL Server on an ESM agent computer. The configuration helps the ESM application modules for SQL Server to understand which server instances the module should report on.

To configure a new SQL server instance

1. Run the ESM SQL Server Discovery module on the ESM agent computers that have the SQL Server installed. The module lists all the new server instances that were not previously configured.
2. Select multiple database instances from the console and do one of the following:
   - Right-click and select **Correction** option.
     The **Correction** option configures the server instances with custom credentials.
   - Right-click and select **Snapshot Update** option.
     The **Snapshot Update** option configures the server instance with generic credentials.

To configure a new SQL server instance automatically

1. Enable the check, **Automatically Add New Instance**.

   The check automatically configures the newly discovered instances in the configuration file, `MSSQLSeverModule.dat`. The check uses the generic credentials and attempts to connect to the server. After each successful connection, the ESM SQL Server Discovery module adds a configuration record in the configuration file. If the connection attempt fails then the module returns a correctable message.

2. To use the **Correctable** option, do the following:
   - Right-click on the message.
   - Choose **Correction** option.
     You are prompted to enter the credentials to connect to the server again.
   - Enter the credentials that you want to configure for the detected SQL server.

Configuring generic credentials

You can configure a generic credential for the ESM SQL Server modules. The generic credential option helps you to configure a common MS SQL server credential for all the SQL server instances on an ESM agent computer.

To specify generic credentials

1. On the command prompt , type **MSSQLSETUP.exe -G**.
2. Enter the Generic Login ID: User name.
3. Enter a password for the generic login. Reconfirm the password.
4. Press **Enter**.

   The generic credentials are configured in the `MSSQLSeverModule.dat` file.

Reusing generic credentials of a SQL Server

If you want to configure common generic credentials on multiple ESM agents, then you do not have to use the MSSQLSETUP.exe -G option on every ESM agent. Instead, you can use -gof and -gif options to export and then import the generic credentials on the desired ESM agents. The exported generic credentials are stored in an encrypted format in the specified file. You can use the same file by specifying the import option on every desired ESM agent.

To export generic credentials

1. On the agent computer where generic credentials have already been configured, go to command prompt and type **MSSQLSETUP.exe -gof <filepath>**.

   For example: < C:\Program Files\Symantec\ESM\bin\w3s-ix86>MSSQLSetup.exe -gof gencred.dat>

2. Press **Enter**.

   The `gencred.dat` file is created with the encrypted generic credentials that are specified in Step 1.

To import generic credentials

1. Copy the `gencred.dat` file on the ESM agent computer where you want to import the generic credentials.
2. On the command prompt, type **MSSQLSETUP -gif <filepath>**.

   For example: < C:\Program Files\Symantec\ESM\bin\w3s-ix86>MSSQLSetup.exe -gif C:\gencred.dat>

   The generic credentials are imported in the `MSSQLSeverModule.dat` file.

   See "To configure a new SQL server instance" on page 25.

Removing unreachable/deleted instances

Although, you may have deleted a SQL server instance, the configuration information still exists in the MSSQLSeverModule.dat file. The ESM SQL Server Discovery module when executed reports the deleted SQL server instances as deleted unreachable instances.

To remove unreachable/ or deleted instances manually

1. Run the ESM SQL Server Discovery module on the target ESM agent computers. The module lists all the unreachable and deleted instances that were configured earlier.
2. Select multiple database instances, right-click, and select **Snapshot Update** option. The **Snapshot Update** option removes the configuration information of such SQL server instances.

To remove unreachable or deleted instances automatically

- Enable the check, **Automatically Delete Unreachable Instances**.

  The module automatically removes the corresponding instance records from the configuration file. `MSSQLSeverModule.dat`.

About ESM Application module for MS SQL Server clusters

The ESM Application module for MS SQL Server also reports on clustered instances.

The ESM SQL Server module for MS SQL Server has the following features:

- The ESM MSSQL setup and ESM SQL Server Discovery module detects the local SQL Server virtual instances within a cluster. When the ESM SQL Server Discovery module runs on a clustered node, it detects and reports the local SQL Server virtual instances.
- During configuration, you must configure the ESM SQL Server modules on all nodes (active or failover) where MS SQL server instance is installed. The MS SQL Server instances are configured with their virtual names or virtual IP addresses on every node in the cluster.
- By default, the modules report from all the nodes irrespective of whether the node is active or not. If you want the module to report only from the active node, you must specify a value greater than 0 on the **Report only from active node** text box of **Servers to check** check. In this case, for the non-active nodes in the cluster, the module reports, **the host is not an active node for the concerned SQL instance, hence skipping scanning of the instance**. The default value of the text box is 0.
- The configuration information exists on all the nodes of the cluster for a given SQL server instance. Therefore, the agent node does not require re-configuration of the SQL server instance in case of a failover, provided the password has not been changed.
- The records of the configured SQL servers exist in the configuration files of the application module on the agent computer. The ESM MSSQL setup allows exporting the configuration records from one agent to another.
- If the ESM SQL Server module's password management feature is enabled for cluster instances, then Symantec recommends that you configure the ESM SQL Server modules with separate user accounts for every node on which the cluster instance is installed. This ensures that in case of a failover scenario, the failover node continues to successfully run the ESM policy for the cluster instance.

Exporting and importing of the SQL Server configuration records from one agent to another

The MSSQL setup module provides the -sof and -sif options, use to which you can export the SQL server configuration records to a file from an agent and then import the same on another agent.

The export/import feature does the following:

- Exports the existing configuration records to an output file using the following command:

  ```
  mssqlsetup.exe -sof out_file [-all]
  ```

  - The -sof switch invokes the export functionality.
  - The -all switch exports all the configuration records that are available within the module's configuration file to out_file.
  - If -all switch is not provided, only configuration records of local cluster instances within the module's configuration file, are exported to the out_file.
  - If any of the configuration records that are being exported to out_file uses generic credentials, then the generic credentials (if available) are also exported to the out_file. The server record that has been exported in this case, indicates that it is supposed to use generic credentials.
  - If no configuration records are exported to the out_file (or if the application is not able to create the out_file) then mssqlsetup application's return code is -1, else it returns 0.

- Imports the existing configuration records of SQL server from a file using the following command:

  ```
  mssqlsetup.exe -sif in_file [-all]
  ```

  - The -sif switch invokes the import functionality.
  - If -all switch is provided , all the configuration records that are available within in_file are imported to the module's configuration file.
  - If -all switch is not provided, only configuration records of local cluster instances (if available) within the in_file are imported to the module's configuration file.
  - During import, the configuration records of the SQL servers available within the in_file are appended to the existing records within the configuration file. If an entry for the server records being imported, already exists within the module's configuration file, this entry isoverwritten.
  - If any of the configuration record that is being imported from in_file uses generic credentials, then the generic credentials (if available within in_file)

are also imported from the in_file into the configuration file of the module. If generic credential already exists, then the generic credentials are overwritten.

About the MS SQL Password Management

The Symantec ESM SQL Server modules for MS SQL databases refer to the ESM SQL configuration file for the list of servers to scan. These servers either use a SQL server login account or a Windows login account for configuration. The ESM Application modules for MS SQL database server manages the passwords of SQL server login accounts wherein you specify a period for the password to change at random, specify the length of the password, and specify the special characters that you want to use.

The ESM SQL Server modules for the MS SQL database server also manages the password for the SQL servers that are configured to use generic credentials provided the generic credential is of the SQL server login account. The ESM SQL Server modules do not manage the passwords if the SQL servers that are configured use 'sa' login accounts or Windows login accounts.

Symantec recommends the following guidelines for the Password Management:

- You must ensure that same SQL server instances are not configured to be monitored from more than two ESM agents.
- You must strictly adhere to the SQL server's password policy when you create the configuration file.

About enabling the Password management for SQL Server login accounts

You can enable the Password management for SQL Server login accounts by configuring the password management parameters that are present in an environment configuration file called 'mssqlenv.dat'. This file is created at the following location: '#esm\config'.

Note: By default, the Password management functionality is disabled. You must change the default values of the password management parameters to enable the Password management functionality.

You can do one of the following to create an mssqlenv.dat file:

- Go to the ESM SQL Server Discovery module and run the **Password management configuration parameters** check. By default, the password

management is disabled. The check's name list contains the configuration parameters and their default values. When you enable the check and run the SQL Server Discovery module, the module creates the `mssqlenv.dat` file on every agent. The `mssqlenv.dat` file contains the parameter values that you define in the name list. Symantec recommends this approach as you can automatically create an `mssqlenv.dat` file on every ESM agent computer. You can update the password management parameters when you run the check. You must enable the **Password management configuration parameter** check before you run the SQL Server Discovery module.

- On every ESM agent computer, you must go to the specified location and manually create the `mssqlenv.dat` file and add the appropriate configuration parameter values.

Note: If the `mssqlenv.dat` file contains valid configuration parameter names and values and you run the **Password management configuration parameters** check with a different value for the same parameter in the name list, then ESM SQL Server Discovery module replaces the value in the `mssqlenv.dat` file with the value that you have specified in the name list.

About using parameters in the mssqlenv.dat file

This section lists the parameters that you can use in the `mssqlenv.dat` file to work with the ESM SQL Server modules.

Before you begin, you must consider the following:

- If the line begins with #, then it is treated as a comment.
- If a parameter is not defined, then the parameter's default value is considered.
- If an invalid value is specified, then the module continues with the default values.
- The password is created based on the values that you define in the ESM MS SQL environment configuration file. The default values are used if the file or its entries are not present.
- If the password change fails, the failure details are logged in the ESM error logs, and a message, **Failed to update password** is reported.

Table 1-8 lists the different parameters that you can use in the `mssqlenv.dat` file to work with the ESM SQL Server modules.

Table 1-8 Parameters and descriptions

Parameter name	Description	Parameter Values	Example
ManageSQL UserPassword	You can use this parameter to enable the password management for SQL login accounts.	By default, this parameter is set to 0. To enable, set the parameter to 1. When enabled, the ESM SQL Server modules for MS SQL database server manages the passwords for the SQL login accounts that are explicitly configured with the respective SQL server.	ManageSQL UserPassword=1
ManageSQL UserGeneric	You can use this parameter to enable the password management for generic credentials.	By default, this parameter is set 0. To enable, set the parameter to 1. During the first password change, the ESM SQL Server module overwrites the server record in the configuration file with the actual user name and password if the SQL server is configured to use generic credentials. The overwritten server record no longer uses generic credentials.	ManageSQL UserGeneric=1

Table 1-8 Parameters and descriptions *(continued)*

Parameter name	Description	Parameter Values	Example
ManageSQL UserPassNetwork	You can use this parameter to enable the password management for the SQL login accounts that are present on a network server.	By default, this parameter is set to 0. To enable, set the parameter to 1. When enabled, the ESM SQL Server modules manage the passwords for the SQL login accounts that are configured for the Network SQL server.	ManageSQL UserPassNetwork=1
ManageSQL UserPassCluster	You can use this parameter to enable the password management of a local cluster instance. **Note:** Symantec does not recommend you to enable this parameter. For more information on the known issue, see the *Symantec™ Enterprise Security Manager Modules for MS SQL Server Databases Release Notes.*	By default, this parameter is set to 0. To enable, set the parameter to 1. When enabled, the ESM SQL Server modules manage the passwords for the SQL login accounts that are configured for the cluster SQL Server nodes.	ManageSQL UserPassCluster=1
SQLUser PassSpecString	You can use this parameter to specify the special characters that can be used while generating the password for the configured account.	NA	SQLUser PassSpecString=_+-=<>?( )* %#!

Table 1-8 Parameters and descriptions *(continued)*

Parameter name	Description	Parameter Values	Example
SQLUser PassChangePeriod	You can use this parameter to specify the period after which you want to change the password of the configured account.	If you want the password to be changed after every policy run, then you set the parameter to 0. If you do not specify any value then ESM SQL Server modules considers 35 days as the default value. The password changes on the next policy run after the specified period ends. If you specify an invalid value in the `mssqlenv.dat` file, then ESM uses the default value.	SQLUser PassChangePeriod=3
SQLUser MinPassLength	You can use this parameter to specify the minimum password length of the passwords that are generated by the ESM SQL Server module. If you specify an invalid value in the `mssqlenv.dat` file, then ESM uses the default value.	By default, the minimum password length is 12. The maximum length that you can specify is 127.	SQLUser MinPassLength=12

About parameter combinations for Password management

This section provides the parameter combinations that you require to enable the Password management on different scenarios.

Table 1-9 lists the parameter combinations for Password management.

Table 1-9 Parameter combinations for Password management

Password management scenarios	Parameter combinations
To enable password management for Network instances	Set the following parameters to 1: ■ ManageSQLUserPassword=1 ■ ManageSQLUserPassNetwork=1
To enable password management for Generic credentials	Set the following parameters to 1: ■ ManageSQLUserPassword=1 ■ ManageSQLUserGeneric=1
To enable password management for Clustered instances	Set the following parameters to 1: ■ ManageSQLUserPassword=1 ■ ManageSQLUserPassCluster=1
To enable password management for Network-clustered instances	Set the following parameters to 1: ■ ManageSQLUserPassword=1 ■ ManageSQLUserPassNetwork=1

About Generic credentials

You can use the generic credentials to configure the MS SQL Server databases. The generic credentials are the common MS SQL Server databases credentials that you can use across servers. The generic credentials can either be a “sa” account, a Windows account, or a pre-created account.

Note: If you want to manage passwords of your generic credentials, then you must ensure that you use a pre-created account. Password management for generic credentials does not work with a “sa” account or Windows account.

Managing passwords of Generic credentials

You can configure the login accounts for the SQL servers in the following ways:

- User name and password
- Generic credentials

The configuration records are saved in the configuration file of the module. If you configure the SQL servers with generic credentials, then a separate record for the generic credential is also present in the configuration file. The SQL Server configuration record is marked by an identifier to use generic credentials. The

ESM SQL Server module uses the generic credentials when it finds the marked identifier in the configuration record.

Examples of managing passwords of Generic credentials

This section contains two scenario-specific examples. In the first example, the password management is disabled and in the second example, it is enabled. Both the examples relate to the SQL servers that are directly configured with pre-created accounts or with generic credentials.

Example 1: Before you enable the Password management for SQL servers.

user= generic_user	password= generic_password	generic= 1
server= sql_server_1	user= user_1	password= password_1
server= sql_server_2	user= use_generic	password= use_generic
server= sql_server_3	user= user_3	Password=password_3

The SQL servers 1 and 3 are configured to use custom credentials where as sql_server_2 is configured to use generic credential. Every time, SQL server module scans sql_server_2, it uses the generic credentials when it finds the marked identifier in the configuration file. If you update the generic credentials with a new user name or password, or both, then sql_server_2 uses the updated credentials.

Example 2: After enable the Password management and the generic credentials for the SQL server and perform at least one policy run.

user= generic_user	password= generic_password	generic= 1
server= sql_server_1	user= user_1	password=random_password_1
server= sql_server_2	user= use_generic	password= random_password_2
server= sql_server_3	user= user_3	Password=random_password_3

The SQL servers 1 and 3 are configured to use custom credentials where as sql_server_2 is configured to use generic credential. After you enable the Password management for all the servers, the module scans sql_server 1, updates the password for user_1 with a random password, and saves the password in the configuration file. The module scans sql_server 2 and detects the marked identifier that is used to identify generic credentials. The module updates the password for use_generic with a random password. In the configuration file, the module overwrites the server record with generic_user and random_password. On the

next policy run, the sql_server 2 is no longer configured to use generic credential. The module scans sql_server 3, updates the password for user_3 with a random password, and saves the password in the configuration file.

Chapter 2

Uninstalling ESM application modules

This chapter includes the following topics:

Uninstall ESM application module

You can uninstall all the components of the ESM application module for MS SQL that are installed on the ESM agent computer and unregister the module from the manager. You can uninstall the ESM application module for MS SQL using the uninstaller program.

The `esmmssqluninstall` executable uninstalls the following components:

- Application executables
- Configuration files
  - Environment configuration files
  - Configuration file with server records
- Property file
- MS SQL application module version file
- Application-specific log file

Running the uninstallation program

You can uninstall the application modules for MS SQL on the ESM agent computer by using the esmmssqluninstall executable.

To uninstall the application module for MS SQL

1. On UNIX, at the command prompt, type cd <path> to open the directory that corresponds to <Install_Dir>/esm/bin/<platform>/esmmssqluninstall.
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 MS SQL 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.

Uninstallation logs

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

Silent uninstallation

You can use the esmmssqluninstall.exe to uninstall the ESM MS SQL module silently, by using the following command:

```
esmmssqluninstall -S -m <manager> -N <agent> [-p <port>] [-mfile
<mgrfile>] -U <user> -P <password>
```
or

```
esmmssqluninstall -S -F <mgrfile>
```
or

```
esmmssqluninstall -S
```

Table 2-1 lists the command-line options for uninstalling the ESM MS SQL module silently

Table 2-1 Options for silent uninstallation

Option	Description
-F	Enters the interactive mode and invokes the uninstall operation.
-mfile	Enters the interactive mode and creates a data file with details of the ESM manager and user credentials.

Table 2-1 Options for silent uninstallation *(continued)*

Option	Description
-S	Invokes the uninstallation in a Silent Mode . **Note:** If -S is specified without any other option then the re-registration is not performed. The uninstall program enters the interactive mode and invokes the uninstall operation.
-m	Specify the ESM manager name.
-N	Specify the agent name as registered with the ESM manager.
-p	Specify the TCP port to connect to the ESM manager.
-U	Specify the ESM manager login ID.
-P	Specify the ESM manager password.