Symantec Enterprise Security Manager Modules for MS SQL Server Databases User Guide

Release 4.1 for Symantec ESM 9.0.x and 10.0 For Windows 2000/2008 and Windows Server 2003 SQL 2005, SQL 2008, and SQL 2008 R2

Symantec

Symantec™ Enterprise Security Manager Modules for MS SQL Server Databases User Guide

Documentation version: 4.1

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

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

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing Symantec ESM Modules for MS SQL Server Databases

This chapter includes the following topics:

About Symantec ESM Modules for MS SQL Server Databases

Symantec Enterprise Security Manager (ESM) Modules for MS SQL Server Databases extends Symantec ESM beyond securing the operating system to securing mission-critical e-business components. These modules protect MS SQL databases from known security vulnerabilities. The modules introduce new, database-specific executables and content, including modules to check auditing levels, server and database configuration, password strength, and unnecessary services.

Working within the framework of Symantec ESM, the industry's most comprehensive solution for discovering security vulnerabilities, Symantec ESM

SQL Server modules for MS SQL Server Databases eases the administrative burden of measuring the effectiveness of enterprise security policies and enforcing compliance. This product installs on Windows 2000/2008 and Windows Server 2003.

With these network-based modules, Symantec ESM's centralized security scanning and integrated reporting capabilities can be used to automate security evaluations and policy enforcement for any MS SQL 2005, 2008 and 2008 R2 database that runs on your network.

Components of Symantec ESM Modules for MS SQL server Databases

When you install Symantec ESM Modules for MS SQL Server Databases, seven new modules and seven new template files are added to your Symantec ESM installation.

Modules

A module is an executable file that examines a server or operating system where a Symantec ESM agent is installed. Each module contains security checks and options that relate to different areas of security.

For example, the SQL Server Password Strength module includes checks that report use of an unauthorized authentication mode, logins with empty passwords, and easily guessed passwords. Each check examines a specific area of concern such as inactive accounts or password length.

Symantec ESM SQL Server modulesfor MS SQL Server Databases installs the modules that are described in the following topics.

SQL Server Accounts

The checks in this module report SQL servers that have logon accounts, logon accounts that were added to the database after the last snapshot update, logon accounts that were deleted from the database after the last snapshot update, and logon accounts with administrator access.

SQL Server Auditing

The checks in this module report SQL Servers that fail to audit at C2 level, that have inadequate login audit level settings, that have inadequate numbers of error log files, and that have inadequate database recovery modes.

SQL Server Configuration

The checks in this module report SQL Server version information, servers that can process ad hoc queries, servers where MSDTC and SQL Agent services start automatically, accounts that are running SQL Server, SQL Agent, and SQL Mail services without authorization, and violations of configuration parameters that are specified in a template.

SQL Server Discovery

The checks in this module automate the process of detection and configuration of new server instances that were not configured earlier on the local ESM agent computers. The checks also discover all unreachable and deleted server instances that are still configured on the ESM agent computers. The checks let you delete the unreachable server instances from the ESM agent computers.

SQL Server Objects

The checks in this module report the violations of database configuration parameter values, databases that the guest user can access, the location of sample databases, database users or roles that can execute job-related stored procedures, role and user permissions, and unauthorized stored procedure, statement, and object permissions.

SQL Server Password Strength

The checks in this module report use of an unauthorized authentication mode, logins with empty passwords, and easily guessed passwords.

SQL Server Roles

The checks in this module report unauthorized members of fixed-server roles, unauthorized members of database roles, and unauthorized application roles.

Templates

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

For example, the SQL Server Roles module uses templates to define database users and roles as either prohibited or authorized. The SQL Server Objects module uses templates to define stored procedures that are prohibited or allowed.

Table 1-1 Template name

Module	Check name	Template name	Predefined template
SQL Server Auditing	SQL Server Trace events	SQL Server Trace Events	mssqtraceevents.mse
SQL Server Configuration	Configuration parameters	SQL Server Configuration Parameters	mssqlconfig.scp
	Registry Configuration Parameters	SQL Server Registry Configuration Parameters	mssqlregconfig.rgx
SQL Server Objects	Database configuration	SQL Server Database Configuration Parameters	mssqldatabase.mdp
	Stored procedure permissions	SQL Server Database Stored Procedure Permissions	mssqlstored procedure.mpp
	Statement permissions	SQL Server Statement Permissions	mssqlstatement permission.msp
	Object permissions	SQL Server Object Permissions	mssqlobject permission.mop
SQL Server Roles	Fixed-server role members	SQL Server Fixed-Server Role Member	none
	Database role members	SQL Server Database Role Member	none

Note: For more information on the template, see the *Symantec™ Enterprise Security Manager Checks and Templates Reference 10.0*.

How Symantec ESM SQL Server modules work

Symantec ESM uses policies, templates, and modules to identify and evaluate the vulnerabilities of network resources. Policies form the standard by which Symantec ESM measures the security agent computers. Templates serve as baselines to determine what conditions should exist on agent computers. Modules perform the actual security checks.

Policies specify the settings, authorizations, and permissions that network resources must have to comply with your company's security policy. Symantec ESM compares the current state of each assessed computer to standards defined in the policy and reports each discrepancy with its severity rating.

Policies contain the modules that evaluate the security of network resources. Modules, in turn, contain the security checks that assess specific aspects of computer security.

What you can do with MS SQL Server Databases

You can use the ESM Application modules to scan the MS SQL Server Databases for reporting vulnerabilities.

You can perform the following tasks using the ESM console:

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

Where you can get more information

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

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

About the Logging functionality on the SQL Server modules

A Logging feature has been enabled on the SQL Server modules. Only those queries that are executed on the SQL server and their execution status are logged. The

logging feature enables ESM to log the information, such as errors and exceptions that a module generates at the runtime.

About the log levels of the message

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 thequalifying messages in the log file.

See "Creating the configuration file" on page 18.

You can specify the following levels:

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. Enabling this level may affect the performance of the module since all the information messages get logged
ESMTRACE	All debug ESMTRACE information is logged.
ESMMAXIMUM	Includes all log levels except ESMNOLOG.

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

[<module>_LogLevel]= ESMINFORMATION

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

[<module>_LogLevel]= ESMINFORMATION | ESMMAXIMUM

You can generate detailed logs for policy failure as follows:

ESMTRACE and ESMINFORMATION

Creating the configuration file

You can 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] = c:\program files\symantec\esm\system\agentname\logs

[mssqlobjects_LogLevel] = ESMINFORMATION|ESMTRACE

[mssqlroles_LogLevel] = ESMINFORMATION|ESMTRACE

Note: For more information on the logging feature, refer to the Security Updates 2008.09.01 (SU 36) Release Notes.

Chapter 2

Installing Symantec ESM Modules for 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.

Required account privileges

You must grant certain minimum privileges to the SQL user who is configured with the ESM SQL Server modules.

You must add the user to each database and assign the required privileges that are specified in Table 2-1. The user must have additional privileges along with the specified required privileges, for the checks that are listed in Table 2-2.

Table 2-1 lists the required privileges.

Table 2-1 Required privileges

Privilege	Object
VIEW ANY DEFINITION	Server
VIEW SERVER STATE	Server

Table 2-1 Required privileges *(continued)*

Privilege	Object
SELECT	■ master..syscurconfigs ■ master..sysservers ■ master..sysdatabases ■ master.sys.server_principals ■ master.sys.server_permissions ■ master.sys.configurations ■ master.sys.linked_logins ■ master.sys.servers ■ master.sys.endpoints ■ master.sys.sql_logins ■ master.sys.traces ■ master.sys.trace_events ■ master.sys.dm_exec_connections
	You must also grant the user the SELECT privileges on the following objects in every database: ■ sys.objects ■ sys.database_principals ■ sys.database_permissions ■ sys.sql_modules
EXECUTE	■ master..xp_startmail ■ master..xp_stopmail ■ master..xp_instance_regenumkeys ■ master..sp_configure ■ master..sp_helpsrvrolemember ■ master..sp_helpsrvrole ■ master..xp_regread ■ master..xp_instance_regread ■ master..sp_helpdb ■ master..sp_helpuser ■ master..sp_helprole ■ master..sp_helprotect ■ master..sp_helprolemember ■ master..xp_loginconfig

Table 2-2 lists the additional privileges othe than the required privileges.

Table 2-2 Additional privileges

Modules	Checks	Privileges
SQL Server Audit	SQL Server trace events	ALTER TRACE
SQL Server Password Strength	All Password cracking checks	CONTROL SERVER
SQL Server Configuration	All Replication related checks	■ The user should be a member of the sysadmin fixed server role at the Publisher. ■ The user must have the specified required privileges and must be a member of the db_owner fixed database role on the publication database. ■ The user must have the specified required privileges and must be listed in the Publication Access List (PAL) of the publication. **Note:** You must grant at least one of the specified privileges.

If you do not want to grant the specified privileges to the user, then you can make the user a member of the 'sysadmin' fixed-server role to access all the security-related settings.

Warning: If you use less than the required privileges for the accounts that the ESM SQL Server module uses for reporting, then a few checks may not function correctly. As a result the module may not report on a few conditions that you want to be reported on.

System requirements

Table 2-3 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 2-3 Supported MS SQL versions and operating systems

Supported operating systems	Supported OS versions	Architecture	Supported MS SQL versions
Windows	2000 SP4	x86	2005
Windows	2003	x86 and x64	2005, 2008, 2008 R2
Windows	2003 R2	x86 and x64	2005, 2008, 2008 R2
Windows	2008	x86 and x64	2005, 2008, 2008 R2
Windows	2008 R2	x64	2005, 2008, 2008 R2

Table 2-4 lists the cluster support on Windows.

Table 2-4 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 2-5 lists the disk space requirements for Symantec ESM SQL Server modules for MS SQL Server Databases.

Table 2-5 Disk space requirements

Operating system	Hard disk space
Windows 2000 (32-bit)	165 MB
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 27.

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.

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 2-6 lists the command line options for silently installing the ESM modules for MS SQL Server Databases.

Table 2-6 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.

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 2-7 lists the options that you can use when running the MSSQLSetup.exe program in the interactive mode.

Table 2-7 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

Table 2-7 Editing configuration records *(continued)*

To do this	Type
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

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 2-8 lists the command line options for silently configuring the ESM SQL Server modules for MS SQL Server Databases.

Table 2-8 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

Table 2-8 Options for silently configuring the MS SQL Server Databases *(continued)*

To do this	Type
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
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 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 33.

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 2-9 lists the different parameters that you can use in the `mssqlenv.dat` file to work with the ESM SQL Server modules.

Table 2-9 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 2-9 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 2-9 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 2-10 lists the parameter combinations for Password management.

Table 2-10 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 3

SQL Server Modules

This chapter includes the following topics:

SQL Server Accounts

The checks in the SQL Server Accounts module reports the SQL servers that:

- Have logon accounts.
- Have the logon accounts that were added to the database after the last snapshot update.
- Have the logon accounts that were deleted from the database after the last snapshot update.
- Have logon accounts with sysadmin access.
- Have logon accounts with securityadmin access.
- Have logon accounts with serveradmin access.
- Have logon accounts with processadmin access.
- Have logon accounts with setupadmin access.

- Have logon accounts with dbcreator access.
- Have a sa account that has not been renamed.

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-1 SQL Server Accounts module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

Servers to check

Use the name list to specify the servers that are to be excluded or included for all SQL Server Account checks. By default, all servers that are selected during installation are included.

Logon accounts

This check reports enabled server logon accounts and their status. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-2 Message for Logon accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_LOGON_ ACCOUNT Category: Policy Compliance	■ Windows 2000 (220631) ■ Windows 2003 (224631) ■ Windows 2008 (253631)	Title: Logon account Description: The SQL Server logon account.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New logon accounts

This check reports the logon accounts that were added to the database after the last snapshot update. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-3 Message for New logon accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_LOGON_ACCOUNT Category: Change Notification	■ Windows 2000 (220632) ■ Windows 2003 (224632) ■ Windows 2008 (253632)	Title: New logon account Description: The MSSQL Server logon account was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted logon accounts

This check reports the logon accounts that were deleted from the database after the last snapshot update. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-4 Message for Deleted logon accounts

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ DELETED_LOGON_ ACCOUNT Category: Change Notification	■ Windows 2000 (220633) ■ Windows 2003 (224633) ■ Windows 2008 (253633)	Title: Deleted logon account Description: The MSSQL Server logon account was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Logon account with sysadmin access

This check reports logon accounts with sysadmin access. Use the name list to specify the logon names that should be included or excluded from this check

The following table lists the message for the check.

Table 3-5 Message for Logon account with sysadmin access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ SYSADMIN_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220634) ■ Windows 2003 (224634) ■ Windows 2008 (253634)	Title: Logon account with sysadmin access Description: The SQL Server logon account has sysadmin access. Members of the sysadmin fixed server role can perform any activity in the server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Logon account with securityadmin access

This check reports logon accounts with securityadmin access. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-6 Message for Logon account with securityadmin access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SECURITYADMIN_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220635) ■ Windows 2003 (224635) ■ Windows 2008 (253635)	Title: Logon account with securityadmin access Description: The SQL Server logon account has securityadmin access. Members of the securityadmin fixed server role manage logins and their properties. They can GRANT, DENY, and REVOKE server-level permissions. They can also GRANT, DENY, and REVOKE database-level permissions. Additionally, they can reset passwords for SQL Server logins.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Logon account with serveradmin access

This check reports logon accounts with serveradmin access. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-7 Message for Logon account with serveradmin access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVERADMIN_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220636) ■ Windows 2003 (224636) ■ Windows 2008 (253636)	Title: Logon account with serveradmin access Description: The SQL Server logon account has serveradmin access. Members of the serveradmin fixed server role can change server-wide configuration options and shut down the server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Logon account with processadmin access

This check reports logon accounts with processadmin access. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-8 Message for Logon account with processadmin access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_PROCESSADMIN_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220637) ■ Windows 2003 (224637) ■ Windows 2008 (253637)	Title: Logon account with processadmin access Description: The SQL Server logon account has processadmin access. Members of the processadmin fixed server role can terminate processes that are running in an instance of SQL Server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Logon account with setupadmin access

This check reports logon accounts with setupadmin access. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-9 Message for Logon account with setupadmin access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SETUPADMIN_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220638) ■ Windows 2003 (224638) ■ Windows 2008 (253638)	Title: Logon account with setupadmin access Description: The SQL Server logon account has setupadmin access. Members of the setupadmin fixed server role can add and remove linked servers, and also execute some system stored procedures.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Logon account with dbcreator access

This check reports logon accounts with dbcreator access. Use the name list to specify the logon names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-10 Message for Logon account with dbcreator access

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DBCREATOR_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220639) ■ Windows 2003 (224639) ■ Windows 2008 (253639)	Title: Logon account with dbcreator access Description: The SQL Server logon account has dbcreator access. Members of the dbcreator fixed server role can create, alter, drop, and restore any database.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Rename sa account

This check reports whether the sa account has been renamed. This check reports only on SQL Server 2005 and later.

The following table lists the message for the check.

Table 3-11 Message for Rename sa account

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SA_EXISTS Category: Policy Compliance	■ Windows 2000 (220640) ■ Windows 2003 (224640) ■ Windows 2008 (253640)	Title: The sa account has not been renamed Description: Rename the sa account to a name that does not reveal its identity. It is difficult to script attacks against a sa account when the user name is unknown.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Database users

This check reports database users. Use the name list to specify the database names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-12 Message for Database users

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ DATABASE_USER Category: System Information	■ Windows 2000 (220641) ■ Windows 2003 (224641) ■ Windows 2008 (253641)	Title: Database user Description: The SQL Server database user.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Automatically update snapshots

Enable this check to automatically update snapshots with current information.

SQL Server Discovery

The checks in the SQL Server Discovery module report the following information:

- Detects new SQL server instances.
- Reports unreachable or deleted SQL server instances.
- Provides an option to automatically configure the newly discovered SQL server instances.
- Provides an option to automatically remove the unreachable and the deleted SQL server instances that are configured.
- Reports all the local and cluster SQL server instances.
- Configures the password management configuration parameters on the ESM agent

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance

and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-13 SQL Server Discovery module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

Detect New Instance

This check reports all the instances that are newly detected on the local computer and do not have respective credentials in the configuration file.

The following table lists the messages for the check.

Table 3-14 Messages for Detect New Instance

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_INSTANCE_DETECTED Category: ESM Administrative Information	■ Windows 2000 (220731) ■ Windows 2003 (224731) ■ Windows 2008 (253731)	Title: New Instance Description: A new server instance has been detected on the local computer. The module cannot find the respective logon credentials in the configuration file for the newly detected server. To configure the newly detected server, either use the Update option to configure with generic credentials or use the Correct option to provide the appropriate logon credentials. You can also use the Correct option even when the update fails.	Severity: yellow-1 Correctable: true Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_NEW_INSTANCE_ADDED Category: ESM Administrative Information	■ Windows 2000 (220732) ■ Windows 2003 (224732) ■ Windows 2008 (253732)	Title: Added New Instance Description: A new server instance has been detected. The configuration record for the newly detected server has been successfully added to the configuration file by using the generic credentials.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-14 Messages for Detect New Instance *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ADD_INSTANCE_FAILED Category: ESM Administrative Information	■ Windows 2000 (220733) ■ Windows 2003 (224733) ■ Windows 2008 (253733)	Title: Failed to Add New Instance Description: The module failed to add a record in the configuration file for the new instance that was detected by using the generic credentials. Either invalid logon credentials were used to connect to the server or the server itself is not running. Try using the correct option to enter the custom credentials for configuring the newly detected server.	Severity: yellow-1 Correctable: true Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Detect Deleted/Unreachable Instance

This check report all the database server instances that cannot be contacted.

The following table lists the messages for the check.

Table 3-15 Messages for Detect Deleted/Unreachable Instance

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DEL_INSTANCE_DETECTED Category: ESM Administrative Information	■ Windows 2000 (220734) ■ Windows 2003 (224734) ■ Windows 2008 (253734)	Title: Unreachable Instance Description: An unreachable server instance has been detected on the local computer. The server cannot be connected to either because it was not running or because an attempt to connect to the server failed due to an invalid login credentials. The configuration file contains the configuration information for the unreachable server instance. Use the Update option to delete the configuration information from the configuration file.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Table 3-15 Messages for Detect Deleted/Unreachable Instance *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_INSTANCE_DELETED Category: ESM Administrative Information	■ Windows 2000 (220735) ■ Windows 2003 (224735) ■ Windows 2008 (253735)	Title: Deleted Unreachable Instance Description: The configuration record for the server has been deleted from the configuration file since it cannot be connected to. Either because the server itself was not running or because an attempt to connect to the server failed due to an invalid login credentials.	Severity: yellow-1 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Automatically Add New Instance

This check works in collaboration with the 'Detect New Instance' check. Enable this check to automatically configure all newly detected server instances. The module uses the generic credentials to connect to the server instance and adds the configuration record in the configuration file after each successful connection.

Automatically Delete Unreachable Instance

This check works in collaboration with the 'Detect Deleted/Unreachable Instance' check. Enable this check to automatically delete the corresponding server records from the configuration file, in case the server is not reachable.

Password management configuration parameters

Enable this check to configure the password management configuration parameters on the ESM agents. Use the name list to specify the values for the supported configuration parameters.

The following table lists the messages for the check.

Table 3-16 Messages for Password management configuration parameters

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_INVALID_PASSWD_PARA Category: ESM Administrative Information	■ Windows 2000 (220736) ■ Windows 2003 (224736) ■ Windows 2008 (253736)	Title: Invalid password management parameter Description: Either the password management parameter that was provided in the namelist is an invalid parameter or it has an invalid value.	Severity: yellow-1 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_CONFIGRD_PASSWD_PARAM Category: ESM Administrative Information	■ Windows 2000 (220737) ■ Windows 2003 (224737) ■ Windows 2008 (253737)	Title: Password management parameters configured Description: The password management parameters were successfully configured.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server Objects

The checks in the SQL Server Objects module reports the following information:

- Violations of the database configuration parameter values.
- Databases that the guest user can access.
- The location of the sample databases.
- Database users or roles that can execute job-related stored procedures.
- Role and user permissions.
- Unauthorized stored procedure, statement, and object permissions.
- Modules that have an EXECUTE AS clause set to a value other than default.
- Created databases.

- Created databases that were added to the SQL server after the last snapshot update.
- Created databases that were deleted from the SQL server after the last snapshot update.
- Roles and users with granted statement permissions that were added to the SQL server after the last snapshot update.
- Roles and users with granted statement permissions that were deleted from the SQL server after the last snapshot update.
- Roles and users with granted object permissions that were added to the SQL server after the last snapshot update.
- Roles and users with granted object permissions that were deleted from the SQL server after the last snapshot update.
- User defined stored procedures present in the database that are not encrypted.
- User defined extended stored procedures present in the database.

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-17 SQL Server Objects module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

Servers to check

Use the name list to specify the servers that are to be excluded or included for all SQL Server Objects security checks.

By default, all SQL servers that are selected during installation are included.

Database configuration

This check reports unauthorized database configuration values as specified in enabled SQL Server Database Configuration Parameters templates.

Symantec ESM Modules for MS SQL Server Databases ships with one sample SQL Server Database Configuration Parameters template (mssqldatabase.mdp), which

is enabled by default. At least one template file must be enabled for this check to work successfully. Use the name lists to enable and disable template files.

The following table lists the message for the check.

Table 3-18 Message for Database configuration

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MDP Category: Policy Compliance	■ Windows 2000 (220336) ■ Windows 2003 (224336) ■ Windows 2008 (253336)	Title: Unauthorized database configuration parameter Description: The database configuration parameter value does not match the value specified in the template files. Modify the configuration option value or change the template file entry to match the existing configuration if it is authorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Guest access to databases

This check reports the SQL Server databases that allow guest user access. Use the Databases name list to include or exclude databases for this check.

By default, master and tempdb databases are excluded. They must have guest access.

To protect your computers, deny guest access to the msdb database, and drop guest users from all other databases where guest access is not required.

The following table lists the message for the check.

Table 3-19 Message for Guest access to databases

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_GUEST_ACCESS Category: Policy Compliance	■ Windows 2000 (220335) ■ Windows 2003 (224335) ■ Windows 2008 (253335)	Title: Guest access to database Description: Guest user access is allowed for the specified database. This allows any authenticated user of the server to access the database with the permissions granted to the guest user. Remove the guest user from the database if it is not required.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Sample databases

This check reports the SQL Servers that have the Northwind and pubs sample databases. These databases are created by default at installation and should be removed from the production servers. Use the name list to include or exclude the names of other databases.

To protect your computers, remove sample Northwind and pubs databases from production servers.

The following table lists the message for the check.

Table 3-20 Message for Sample databases

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SAMPLE_DATABASE Category: Policy Compliance	■ Windows 2000 (220333) ■ Windows 2003 (224333) ■ Windows 2008 (253333)	Title: Sample database Description: The SQL Server has the named sample database. Sample databases provide known targets for attackers and should be removed from production servers.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Job permissions

This check reports the database users and roles that are allowed to execute the following job-related stored procedures: sp_add_job, sp_add_jobstep, sp_add_jobserver, sp_start_job. Use the name list to include or exclude users or roles for this check. Use the name list to include or exclude users or roles for this check.

These stored procedures may be used to create jobs to be executed at a later time, or on a recurring basis, from the SQL Agent service. A malicious user or intruder can create a procedure to continually submit an unlimited number of jobs and execute them at any time.

To protect your computers, revoke the execute permission from unauthorized users or roles for the job-related stored procedures.

The following table lists the message for the check.

Table 3-21 Message for Job permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_JOB_PERMISSION Category: Policy Compliance	■ Windows 2000 (220334) ■ Windows 2003 (224334) ■ Windows 2008 (253334)	Title: Unauthorized job permission Description: The named user or role has the execute permission on the specified job-related stored procedure. Revoke this permission from unauthorized users or roles to prevent hostile use of job-related stored procedures.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Schema permissions

This check reports schema permissions for different users/roles. Use the name list to include or exclude users or roles for this check.

The following table lists the message for the check.

Table 3-22 Message for Schema permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SCHEMA_PERMISSION Category: Policy Compliance	■ Windows 2000 (220357) ■ Windows 2003 (224357) ■ Windows 2008 (253357)	Title: Schema permissions Description: A schema is a database-level securable contained by the database that is its parent in the permissions hierarchy. The list of permissions on the detected schema for the users/roles are listed in the information field.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Stored procedure permissions

This check reports unauthorized stored procedure permissions as specified in enabled SQL Server Database Stored Procedure Permissions templates. Use the name lists to enable and disable template files.

You can use SQL Server Database Stored Procedure Permissions templates to report the permissions of stored procedures, extended stored procedures, and scalar functions.

Symantec ESM Modules for MS SQL Server Databases ships with one sample SQL Server Database Stored Procedure Permissions template (mssqlstoredprocedure.mpp), which is enabled by default. At least one template file must be enabled for this check to work successfully.

To protect your computers, periodically review granted stored procedure and extended stored procedure permissions and revoke excessive permissions. Monitor permissions for extended stored procedures that allow access to the registry, a command shell, or the file system.

The following table lists the messages for the check.

Table 3-23 Messages for Stored procedure permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MPP Category: Policy Compliance	■ Windows 2000 (220338) ■ Windows 2003 (224338) ■ Windows 2008 (253338)	Title: Unauthorized stored procedure permission Description: The stored procedure permission does not match the permissions specified in the template files. Modify the permissions for this stored procedures or change the template file entry to match the existing permissions if they are authorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_MPP_MANDATORY Category: Policy Compliance	■ Windows 2000 (220340) ■ Windows 2003 (224340) ■ Windows 2008 (253340)	Title: Mandatory stored procedure permission Description: The mandatory stored procedure permission specified in the template files does not exist. Modify the stored procedure permissions or change the template file entry to match the existing permissions if they are authorized.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Statement permissions

This check reports unauthorized statement permissions as specified in enabled SQL Server Statement Permissions templates. Use the name lists to enable and disable template files.

Symantec ESM Modules for MS SQL Server Databases ships with one sample SQL Server Statement Permissions template (mssqlstatementpermission.msp), which is enabled by default. At least one template file must be enabled for this check to work successfully.

To protect your computers, periodically review granted statement permissions and revoke unauthorized permissions.

The following table lists the messages for the check.

Table 3-24 Messages for Statement permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MSP Category: Policy Compliance	■ Windows 2000 (220337) ■ Windows 2003 (224337) ■ Windows 2008 (253337)	Title: Unauthorized statement permission Description: The statement permission does not match the permissions specified in the template files. Modify the statement permissions or change the template file entry to match the existing permissions if they are authorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-24 Messages for Statement permissions *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MSP_MANDATORY Category: Policy Compliance	■ Windows 2000 (220342) ■ Windows 2003 (224342) ■ Windows 2008 (253342)	Title: Mandatory statement permission Description: The mandatory statement permission specified in the template files does not exist. Modify the statement permissions or change the template file entry to match the existing permissions if they are authorized.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Object permissions

This check reports the unauthorized object permissions as specified in the enabled SQL Server Object Permissions templates. Use the name lists to enable and disable the template files.

You can use SQL Server Object Permissions templates to report on the permissions of system tables, user tables, views, table functions, and inline table-values functions.

Symantec ESM Modules for MS SQL Server Databases ships with one sample SQL Server Object Permissions template (mssqlobjectpermission.mop), which is enabled by default. At least one example file must be enabled for this check to work successfully.

The following table lists the messages for the check.

Table 3-25 Messages for Object permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MOP Category: Policy Compliance	■ Windows 2000 (220339) ■ Windows 2003 (224339) ■ Windows 2008 (253339)	Title: Unauthorized object permission Description: The object permission does not match the permissions specified in the template files. Modify the object permissions or change the template file entry to match the existing permissions if they are authorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_MOP_MANDATORY Category: Policy Compliance	■ Windows 2000 (220341) ■ Windows 2003 (224341) ■ Windows 2008 (253341)	Title: Mandatory object permission Description: The mandatory object permission specified in the template files does not exist. Modify the object permissions or change the template file entry to match the existing permissions if they are authorized.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Object permission names

Use the name list to specify the permissions that are to be included or excluded for the grant with grant object permissions, the directly granted object permissions, the new granted object permissions, and the deleted granted object permissions checks. Valid entries include Select, Insert, Update, Delete, and Execute.

Object names

Use the name list to specify the object names that are to be included or excluded for the grant with grant object permissions, the directly granted object permissions, the new granted object permissions, and the deleted granted object permissions checks.

Object permission grantors

Use the name list to specify the grantors that are to be included or excluded for the grant with grant object permissions, the directly granted object permissions, the new granted object permission, and the deleted granted object permissions checks.

Directly granted object permissions

This check reports the roles and users that have the directly granted object permissions. Use the name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

To protect your computers, verify that the user or role is authorized to have the permission. Periodically review directly granted object permissions and tighten when possible.

The following table lists the message for the check.

Table 3-26 Message for Directly granted object permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_OBJ_DIR_GRANT Category: Policy Compliance	■ Windows 2000 (220330) ■ Windows 2003 (224330) ■ Windows 2008 (253330)	Title: Directly granted object permission Description: The object permission has been granted to the specified user or role in the named database. Verify that the user or role is authorized to have the permission.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Grant with grant object permissions

This check reports the roles and users that have the grant with grant object permissions. Use the name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

To protect your computers, verify that the user or role is authorized to have the permission. Periodically review directly granted object permissions and tighten when possible.

The following table lists the message for the check.

Table 3-27 Message for Grant with grant object permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_OBJ_GRANT_GRANT Category: Policy Compliance	■ Windows 2000 (220331) ■ Windows 2003 (224331) ■ Windows 2008 (253331)	Title: Grant with grant object permission Description: The grantable object permission has been granted to the specified user or role in the named database. Verify that the user or role is authorized to have and grant the permission.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Statement permission names

Use the name list to specify the statement permissions that are to be included or excluded for the directly granted statement permission, the new granted statement permission, and the deleted granted statement permission checks. Valid checks include Backup Database, Backup Log, Create Database, Create Default, Create Function, Create Procedure, Create Rule, Create Table, or Create View.

Statement permission grantors

Use the name list to specify the grantors that are to be included or excluded for the directly granted statement permission, the new granted statement permission, and the deleted granted statement permission checks.

Directly granted statement permissions

This check reports the roles and users that have the directly granted statement permissions. Use the check's name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

The following table lists the message for the check.

Table 3-28 Message for Directly granted statement permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_STA_DIR_GRANT Category: Policy Compliance	■ Windows 2000 (220332) ■ Windows 2003 (224332) ■ Windows 2008 (253332)	Title: Directly granted statement permission Description: The statement permission has been directly granted to the named user or role for the database. Verify that the user or role is authorized to have the permission.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Module EXECUTE AS clause

This check reports the SQL Server modules that have an associated EXECUTE AS clause set to a value other than the default setting of CALLER. The EXECUTE AS clause lets you set the execution context of user-defined modules such as functions, procedures, queues, and triggers. The execution context determines which user account is used to evaluate permissions that are required by objects that are referenced by the running module. This check reports modules that are assigned

to execute as a user other than the user calling the module. Use the name list to specify EXECUTE AS names that are to be included or excluded for the check.

The following table lists the message for the check.

Table 3-29 Message for Module EXECUTE AS clause

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MODULE_EXECUTE_AS Category: Policy Compliance	■ Windows 2000 (220343) ■ Windows 2003 (224343) ■ Windows 2008 (253343)	Title: Module EXECUTE AS clause Description: The module has an associated EXECUTE AS clause set to a value other than the default setting of CALLER.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Database status

This check reports information about the created databases. Use the name list to specify the database names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-30 Message for Database status

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DATABASE Category: Policy Compliance	■ Windows 2000 (220344) ■ Windows 2003 (224344) ■ Windows 2008 (253344)	Title: Database status Description: The SQL Server database status.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New databases

This check reports information about the created databases that were added to the server after the last snapshot update. Use the name list to specify the database names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-31 Message for New databases

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_DATABASE Category: Change Notification	■ Windows 2000 (220345) ■ Windows 2003 (224345) ■ Windows 2008 (253345)	Title: New database Description: The MSSQL Server database was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted databases

This check reports information about the created databases that were deleted from the server after the last snapshot update. Use the name list to specify the database names that should be included or excluded from this check.

The following table lists the message for the check.

Table 3-32 Message for Deleted databases

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DELETED_DATABASE Category: Change Notification	■ Windows 2000 (220346) ■ Windows 2003 (224346) ■ Windows 2008 (253346)	Title: Deleted database Description: The MSSQL Server database was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Non-encrypted stored procedures

This check reports the list of user defined stored procedures available in the database and are not encrypted.

The following table lists the message for the check.

Table 3-33 Message for Non-encrypted stored procedures

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_USER_DEFINED_PROC Category: Policy Compliance	■ Windows 2000 (220355) ■ Windows 2003 (224355) ■ Windows 2008 (253355)	Title: User defined stored procedures are not encrypted Description: The user defined stored procedures should be in an encrypted format.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Extended stored procedures

This check reports the list of user defined extended stored procedures available within the database.

The following table lists the message for the check.

Table 3-34 Message for Extended stored procedures

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_EXT_USER_DEFINED_PROC Category: Policy Compliance	■ Windows 2000 (220356) ■ Windows 2003 (224356) ■ Windows 2008 (253356)	Title: User defined extended stored procedures Description: Using of user-defined extended stored procedures should be avoided. If extended functionality is required, use Common Language Runtime (CLR) assemblies instead.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New granted statement permissions

This check reports the roles and users with the granted statement permissions that were added to the server after the last snapshot update. Use the check's name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

The following table lists the message for the check.

Table 3-35 Message for New granted statement permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_STATEMENT_PERM Category: Change Notification	■ Windows 2000 (220347) ■ Windows 2003 (224347) ■ Windows 2008 (253347)	Title: New statement permission Description: The MSSQL Server statement permission was granted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

New granted object permissions

This check reports the roles and users with the granted object permissions that were added to the server after the last snapshot update. Use the check's name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

The following table lists the messages for the check.

Table 3-36 Messages for New granted object permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_OBJECT Category: Change Notification	■ Windows 2000 (220349) ■ Windows 2003 (224349) ■ Windows 2008 (253349)	Title: New object Description: The MSSQL Server object was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_NEW_OBJECT_PERM Category: Change Notification	■ Windows 2000 (220350) ■ Windows 2003 (224350) ■ Windows 2008 (253350)	Title: New granted object permission Description: The MSSQL Server object permission was granted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_NEW_OBJECT_PERM_COL Category: Change Notification	■ Windows 2000 (220351) ■ Windows 2003 (224351) ■ Windows 2008 (253351)	Title: New granted object column permission Description: The MSSQL Server object column permission was granted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted granted statement permissions

This check reports the roles and users with the granted statement permissions that were deleted from the server after the last snapshot update. Use the check's name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

The following table lists the message for the check.

Table 3-37 Message for Deleted granted statement permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DELETED_STATEMENT_PERM Category: Change Notification	■ Windows 2000 (220348) ■ Windows 2003 (224348) ■ Windows 2008 (253348)	Title: Deleted statement permission Description: The MSSQL Server statement permission was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Directly granted object permissions

This check reports the roles and users that have the directly granted object permissions. Use the name list to specify the grantees that are to be included or excluded for the check. Use the keyword %users% to specify all the users in the database. Use the keyword %roles% to specify all the roles in the database.

To protect your computers, verify that the user or role is authorized to have the permission. Periodically review directly granted object permissions and tighten when possible.

The following table lists the message for the check.

Table 3-38 Message for Directly granted object permissions

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_OBJ_DIR_GRANT Category: Policy Compliance	■ Windows 2000 (220330) ■ Windows 2003 (224330) ■ Windows 2008 (253330)	Title: Directly granted object permission Description: The object permission has been granted to the specified user or role in the named database. Verify that the user or role is authorized to have the permission.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Automatically update snapshots

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

SQL Server Password Strength

The checks in the SQL Server Password Strength module reports the following information:

- Use of an unauthorized authentication mode.
- Logins and application roles with empty passwords.
- Easily guessed login and application role passwords.
- Login and application role passwords that have not been changed.
- SQL Server 2005 logins that do not have the password policy enforced.
- SQL Server 2005 logins that do not have the password expiration enforced.

Note: SQL Server Password Strength module checks examine only SQL Server passwords. To test the password strength for Windows authentication, use the operating system Password Strength modules that ship with Symantec ESM.

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance

and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-39 SQL Server Password Strength module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

About secure passwords

Secure passwords meet the following criteria:

- They have at least eight characters, including one or more non-alphabetic characters.
- They do not match an account or host computer name.
- They cannot be found in any dictionary.
  See "Password = wordlist word" on page 86.

Servers to check

Use the name list to specify the servers that are to be excluded or included for all SQL Server Password Strength checks.

By default, all servers that are selected during installation are included.

Authentication mode

This check reports the servers that do not use the specified authentication modes. In the Authentication mode text box, type 1 for Windows only mode, and 2 for SQL Server and Windows modes.

The following table lists the message for the check.

Table 3-40 Message for Authentication mode

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_AUTH_MODE Category: Policy Compliance	■ Windows 2000 (220230) ■ Windows 2003 (224230) ■ Windows 2008 (253230)	Title: Authentication mode Description: The SQL Server authentication mode does not match the mode specified in the check's value field. Use Windows Authentication Mode whenever possible to provide the most secure method to connect to the server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Empty password

This check reports the SQL Server logons with empty or NULL passwords.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

The following table lists the message for the check.

Table 3-41 Messages for Empty password

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NULL_PASSWORD Category: Policy Compliance	■ Windows 2000 (220231) ■ Windows 2003 (224231) ■ Windows 2008 (253231)	Title: Empty password Description: The reported SQL Server login has an empty or NULL password. Assign a password to it now, then instruct the user to log on with the assigned password and change the password again.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Hide guessed password details

When you enable this check, the security checks no longer display the details of the guessed password. This check works with the following checks:

- Password = login name
- Password = any login name
- Password = wordlist word
- Reverse order
- Double occurrences
- Plural
- Prefix
- Suffix

Application role password

This check reports the unauthorized application role passwords in each database. When you enable this check, any other SQL Server Password Strength check that is also enabled in the policy is applied to the application role passwords. The application role password checks are not applicable for SQL Server 2005 and above.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password..

The following table lists the message for the check.

Table 3-42 Message for Application role password

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_GUESSED_PASSWORD Category: Policy Compliance	■ Windows 2000 (220232) ■ Windows 2003 (224232) ■ Windows 2008 (253232)	Title: Guessed password Description: Symantec ESM guessed the passwords of the SQL Server logins listed below. Assign more secure passwords to these logins or remove them. A secure password should have six to eight characters, should not be found in any dictionary, and should have at least one non-alphabetic character. A secure password should also not match login or host name.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password = login name

This check reports the SQL Server logins with the matching login names and passwords. To apply this check to the application role passwords, enable this check and the Application role password check in the same policy.

The check is provided for systems with a large number of logins. It is not as thorough as Password = any login name. However, if the Password = any login name check takes too much time or consumes too much CPU, you can use Password = login name daily and Password = any login name on weekends.

Intruders frequently substitute login names for passwords in an attempt to break in.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

The following table lists the message for the check.

Table 3-43 Message for Password = login name

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_GUESSED_PASSWORD Category: Policy Compliance	■ Windows 2000 (220232) ■ Windows 2003 (224232) ■ Windows 2008 (253232)	Title: Guessed password Description: Symantec ESM guessed the passwords of the SQL Server logins listed below. Assign more secure passwords to these logins or remove them. A secure password should have six to eight characters, should not be found in any dictionary, and should have at least one non-alphabetic character. A secure password should also not match login or host name.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password = wordlist word

This check tries to match the SQL Server logon passwords with words in the enabled word files and reports matches. Use the name lists to enable or disable word files for the check. To apply this check to the application role passwords, enable this check and the Application role password check in the same policy.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

The following table lists the message for the check.

Table 3-44 Message for Password = wordlist word

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_GUESSED_PASSWORD Category: Policy Compliance	■ Windows 2000 (220232) ■ Windows 2003 (224232) ■ Windows 2008 (253232)	Title: Guessed password Description: Symantec ESM guessed the passwords of the SQL Server logins listed below. Assign more secure passwords to these logins or remove them. A secure password should have six to eight characters, should not be found in any dictionary, and should have at least one non-alphabetic character. A secure password should also not match login or host name.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Reverse order

When this option is enabled, module checks that guess passwords report logins with passwords that match the reverse of login names or entries in enabled word files; for example, golf spelled in reverse matches the password flog.

Note: When you enable this option, you must also enable Password = login name or Password = any login name, and the Password = wordlist word checks.

Intruders often add prefixes to user names or common words in an attempt to break in.

To apply this option to application role passwords, enable this option and the Application role password check in the same policy.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

Double occurrences

This option causes password checks to report logins with passwords that match doubled versions of login names or entries in enabled word files; for example, golf doubled matches the password golfgolf.

Note: When you enable this option, you must also enable Password = login name or Password = any login name, and the Password = wordlist word checks. Intruders often use doubled versions of user names or common words as passwords in an attempt to break in.

To apply this option to application role passwords, enable this option and the Application role password check in the same policy.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

Plural

This option causes password checks to report logins with passwords that match plural forms of login names or entries in enabled word files; for example, golf in plural form matches the password golfs.

Note: When you enable this option, you must also enable Password = login name or Password = any login name, and the Password = wordlist word checks.

Intruders often use plural forms of login names or common words as passwords in an attempt to break in.

To apply this option to application role passwords, enable this option and the Application role password check in the same policy.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

Prefix

This option causes password checks to report logins with passwords that match forms of login names or entries in enabled word files with a prefix; for example., golf with the prefix pro matches the password progolf. Use the name list to specify prefixes for the check.

Note: When you enable this option, you must also enable Password = login name or Password = any login name, and the Password = wordlist word checks.

Intruders often add prefixes to user names or common words in an attempt to break in.

To apply this option to application role passwords, enable this option and the Application role password check in the same policy.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

Suffix

This option affects the behavior of the enabled Password = user name, Password = any user name, and Password = wordlist word security checks. When this option is enabled, the specified suffixes are added to the user names and the wordlist words that are used to guess passwords, such as golf -> golfball). Use the option's name list to specify the suffixes that are to be used.

Note: When you enable this option, you must also enable Password = login name or Password = any login name, and the Password = wordlist word checks.

Intruders often add prefixes to user names or common words in an attempt to break in.

To apply this option to application role passwords, enable this option and the Application role password check in the same policy.

To protect your computers, if an empty or weak password is found, assign a more secure temporary password to the login. Inform the login user of the change and provide instructions on setting a secure password.

Monitor password age

This check reports the SQL Server logon and the application role passwords that have not been changed within the period that is specified in the Maximum days text box.Use the name list to specify the logon names that should be included or excluded from this check.This check compares the CRC and MD5 signatures of password hashes since the last snapshot.

To establish a baseline for this security check, create a new SQL Server Password Strength policy with this check enabled. Running this policy creates a snapshot of current password information. The snapshot file is automatically updated when passwords are changed.

To protect your computers, require users to change login and application role passwords at least every sixty days.

The following table lists the message for the check.

Table 3-45 Message for Monitor password age

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_PASSWORD_NOT_CHANGED Category: Policy Compliance	■ Windows 2000 (220234) ■ Windows 2003 (224234) ■ Windows 2008 (253234)	Title: Password not changed Description: The reported SQL Server login or application role in the specified database has not changed its password in the specified period.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password policy enforcement

This check reports the SQL Server logons with the password policy that is not enforced. Use the name list to specify the logon names that should be included or excluded from this check. This check is not supported on SQL Server 2000.

The following table lists the message for the check.

Table 3-46 Message for Password policy enforcement

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ PASSWORD_POLICY Category: Policy Compliance	■ Windows 2000 (220235) ■ Windows 2003 (224235) ■ Windows 2008 (253235)	Title: Password policy not enforced Description: The reported SQL Server 2005 login is not enforced with password policy.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Password expiration enforcement

This check reports the SQL Server logons with the password expirations that are not enforced. Use the name list to specify the logon names that should be included or excluded from this check. This check is not supported on SQL Server 2000.

The following table lists the message for the check.

Table 3-47 Message for Password expiration enforcement

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ PASSWORD_ EXPIRATION Category: Policy Compliance	■ Windows 2000 (220236) ■ Windows 2003 (224236) ■ Windows 2008 (253236)	Title: Password expiration not enforced Description: The reported SQL Server 2005 login is not enforced with password expiration.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server Auditing

The checks in the SQL Server Auditing module report the SQL servers that:

- Fail to audit at C2 level.

- Have inadequate logon audit level settings.
- Have inadequate numbers of error log files.
- Have inadequate database recovery modes.
- Reports the events that are either not being captured by any active SQL trace or any active SQL traces that are specified within the template.

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-48 SQL Server Auditing module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

C2-level auditing

This check reports the SQL Servers that do not audit at a C2 level.

The C2 audit mode is an Advanced Server configuration option that you can enable with sp_configure parameter.

To protect your computers, enable this check if your company policy requires C2-level security.

The following table lists the message for the check.

Table 3-49 Message for C2-level auditing

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_C2_LEVEL_AUDITING Category: Policy Compliance	■ Windows 2000 (220531) ■ Windows 2003 (224531) ■ Windows 2008 (253531)	Title: C2-level auditing not enabled Description: The SQL Server C2 audit mode is not enabled. This audit mode should be enabled for security policies that require C2 evaluation level auditing.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server trace events

This check reports the events specified in the template, that are either not being captured by any active SQL trace or any active SQL traces that are specified within the template.

This check uses the **SQL Server Trace Events** template to report the events specified in the template.

The following table lists the message for the check.

Table 3-50 Message for SQL Server trace events

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_TRACE_EVENT	■ Windows 2000 (220500) ■ Windows 2003 (224500) ■ Windows 2008 (253500)	Title: SQL Server trace event Description: The SQL server trace event is not configured as per user given trace and event information.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information field format: %s

Database recovery mode

This check reports the SQL Server databases that are not configured to use the specified recovery mode. In the **Recovery mode** text box, type 1 for Simple, 2 for Bulk_logged, or 3 for Full. Use the name list to include or exclude databases from this check. The default value is 1.

To protect your computers, select an adequate recovery mode to restore data to an acceptable level in the event of data loss.

The following table lists the message for the check.

Table 3-51 Message for Database recovery mode

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ RECOVERY_MODE Category: Policy Compliance	■ Windows 2000 (220533) ■ Windows 2003 (224533) ■ Windows 2008 (253533)	Title: Database recovery mode Description: The reported database is not configured to use the specified database recovery mode.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Login audit level

This check reports the SQL Servers that do not comply with the minimum login audit level that you specify in the check. In the **Audit level** text box, type 0 (None - no information about logins is desired in the audit log), 1 (Success - log only successful login attempts), 2 (Failure - log only failed login attempts), or 3 (All - log both successful and failed login attempts). The default value is 2.

To protect your computers, set the **Audit level** value of the check to 2 or greater and then monitor the login logs for suspicious login patterns.

The following table lists the message for the check.

Table 3-52 Message for Login audit level

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_LOGIN_AUDIT_LEVEL Category: Policy Compliance	■ Windows 2000 (220530) ■ Windows 2003 (224530) ■ Windows 2008 (253530)	Title: Inadequate login audit level Description: The SQL Server login audit level does not match the specified minimum audit level specified for this check. When auditing is enabled, SQL Server will write login information to both the SQL Server error log and the Windows NT Application Event Log. Check these logs often to monitor who is accessing or trying to access your server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Server error log maximum

This check reports the SQL Servers that are configured to save fewer error log files than the check specifies. A configuration parameter in SQL Server logs determines the number of error log files that are written before they are recycled.

To configure this check, in the **Number of error log files** text box, specify the required minimum number of error log files that each of your SQL servers should maintain before recycling. The default value is 6.

To protect your computers, store enough error information to meet the perceived risk. You can increase the number of saved error logs on your SQL Server through the SQL Server Enterprise Manager.

The following table lists the message for the check.

Table 3-53 Message for Server error log maximum

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MAX_ERROR_LOG_FILES Category: Policy Compliance	■ Windows 2000 (220532) ■ Windows 2003 (224532) ■ Windows 2008 (253532)	Title: Error log maximum too low Description: The SQL Server is configured to store fewer error logs than the specified value. Each time SQL Server starts, a new log file is created, and the old is saved. Once the maximum number of log files has been reached, the oldest files are replaced with new log files. To keep a log history for a longer amount of time, this maximum should be increased.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Servers to check

Use the name list to specify the servers that are to be excluded or included for all SQL Server Auditing checks. By default, all servers that are selected during installation are included.

SQL Server Configuration

The checks in the SQL Server Configuration module reports the following information:

- SQL Server version information.
- Servers that can process ad hoc queries
- Servers where MSDTC and SQL Agent services start automatically.
- Accounts that are running SQL Server, SQL Agent, and SQL Mail services without authorization.

- Violations of configuration the parameters that are specified in a template.
- SQL servers that broadcast on the network.
- SQL servers that are installed on a domain controller, are installed on an unauthorized path, or permit server access.
- Started the SQL server endpoints that the SQL Server Database Engine communicates with an application.
- Reports the remote servers that are being used through the local server.
- Unauthorized registry configuration parameter values that are specified in a template.
- Reports the publications that do not use filters to protect data.
- Verifies whether the Replication Agent uses a Windows account.
- Reports on the surface area configuration (SAC) features of Analysis Services that are detected on the host system.
- Reports on the surface area configuration (SAC) features of Reporting Services that are detected on the host system.
- Reports the SQL server publication access list accounts for the published databases.
- Verifies whether the ForceEncryption setting is enabled.
- Verifies whether the Friendly name property of the SSL certificate contains the FQDN name of the server.
- Verifies if the linked and the local servers are configured to use Windows authentication mode.
- Reports all the nodes within the SQL Server cluster setup if the SQL Server is a clustered server.
- Reports the server properties that are specified in the template.

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-54 SQL Server Configuration module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

SQL Server property

This check reports the server properties that are specified in the template.

The following table lists the message for the check.

Table 3-55 Message for SQL Server property

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ SERVER_PROPERTY Category: System Information	■ Windows 2000 (220167) ■ Windows 2003 (224167) ■ Windows 2008 (253167)	Title: SQL Server property Description: The SQL Server property is displayed in the information field.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server cluster nodes

If the SQL Server is a clustered server, then the check reports all the nodes within the SQL Server cluster setup.

The following table lists the message for the check.

Table 3-56 Message for SQL Server property

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_SQL_CLUSTER_NODES Category: System Information	■ Windows 2000 (220168) ■ Windows 2003 (224168) ■ Windows 2008 (253168)	Title: SQL Cluster Node Description: The SQL Server is a clustered server. Refer to the information field for the list of nodes that are present in the cluster.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Windows authentication for linked server

This check verifies if the linked and the local servers are configured to use Windows authentication mode.

The following table lists the message for the check.

Table 3-57 Message for Windows authentication for linked server

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NOT_WINDOWS_AUTH_MODEESM_MSSQL_NO_REPLICATION_FILTER Category: Policy Compliance	■ Windows 2000 (220164) ■ Windows 2003 (224164) ■ Windows 2008 (253164)	Title: SQL Server is running in Mixed-authentication mode Description: The SQL Server must be configured to use Windows authentication mode so that if Linked Servers are configured, then these servers automatically use the same mode. CIS recommends this as a security setting for the SQL Server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_SQL_LINKED_SRV_NO_AUTH_MODE Category: Policy Compliance	■ Windows 2000 (220165) ■ Windows 2003 (224165) ■ Windows 2008 (253165)	Title: Connections to the Linked Server do not use Windows authentication Description: The connections to the Linked Server are not configured to use the Windows authentication mode. You must enable the 'Be made using the login's current security context' property of the Linked server, if you want to configure the Linked Server to use the Windows authentication mode.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Replication Filter

This check reports the publications that do not use filters to protect data.

The following table lists the message for the check.

Table 3-58 Message for Replication Filter

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NO_REPLICATION_FILTER Category: Policy Compliance	■ Windows 2000 (220156) ■ Windows 2003 (224156) ■ Windows 2008 (253156)	Title: Replication filter not defined Description: Replication filters have not been defined for the reported publication.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Replication Agent account

This check verifies whether the Replication Agent uses a Windows account instead of a SQL server agent account.

The following table lists the message for the check.

Table 3-59 Message for Replication Agent account

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_REPLICATION_AGNT_ACCT Category: Policy Compliance	■ Windows 2000 (220157) ■ Windows 2003 (224157) ■ Windows 2008 (253157)	Title: Replication agent does not use windows account Description: Replication agents should use a windows account rather than a SQL Server Agent account.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Analysis Service SAC features

This check reports on the surface area configuration (SAC) features of Analysis Services that are detected on the host system. Use the **Keys** column to specify the expected state of the SAC feature. By default, the check verifies if all the SAC features are disabled. This check operates in the host-based mode.

Note: The check reports on the features only if it finds the Analysis service to be running. If the Analysis service is detected, but not in running state, then the module display's a note, **Analysis service was detected, but it was not in the running state**.

The following table lists the message for the check.

Table 3-60 Message for Analysis Service SAC features

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ UNAUTH_SAC_AS Category: Policy Compliance	■ Windows 2000 (220158) ■ Windows 2003 (224158) ■ Windows 2008 (253158)	Title: Unauthorized Analysis Server SAC feature Description: The state of the Analysis Server's SAC configuration parameter is unauthorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Note: The check reports an error message, **Configuration File Error** if it is unable to access the `msmdsrv.ini` file.

Reporting Service SAC features

This check reports on the surface area configuration (SAC) features of Reporting Services that are detected on the host system. Use the **Keys** column to specify the expected state of the SAC feature. This check operates in the host-based mode.

Note: The check reports on the features only if it finds the Reporting service to be running. If the Reporting service is detected, but not in running state, then the module display's a note, **Reporting service was detected, but it was not in the running state**.

The following table lists the message for the check.

Table 3-61 Message for Reporting Service SAC features

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ UNAUTH_SAC_RS Category: Policy Compliance	■ Windows 2000 (220159) ■ Windows 2003 (224159) ■ Windows 2008 (253159)	Title: Unauthorized Reporting Server SAC feature Description: The state of the Reporting Server's SAC configuration parameter is unauthorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Note: The check reports an error message, **Configuration File Error** if it is unable to access the `web.config` and `rsreportserver.config` files.

Publication Access List (PAL)

This check reports the SQL server publication access list accounts for the published databases. Use the name list to include or exclude the accounts for this check to report on.

The following table lists the message for the check.

Table 3-62 Message for Publication Access List (PAL)

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVER_PAL_ACCOUNT Category: System Information	■ Windows 2000 (220155) ■ Windows 2003 (224155) ■ Windows 2008 (253155)	Title: Publication Access List Account Description: The reported account is defined in the Publication Access List.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

ForceEncryption should be enabled

This check verifies whether the **ForceEncryption** setting is enabled for the SQL Server.

The following table lists the message for the check.

Table 3-63 Message for ForceEncryption should be enabled

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SSL_ENABLED Category: Policy Compliance	■ Windows 2000 (220166) ■ Windows 2003 (224166) ■ Windows 2008 (253166)	Title: Encryption is not forced upon the SQL Server Description: SSL encryption not enforced upon the SQL Server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server SSL certificate with FQDN name

This check verifies whether the **Friendly name** property of the SSL certificate that is configured for the SQL Server contains the FQDN name of the server. This check operates only in the host-based mode.

The following table lists the message for the check.

Table 3-64 Messages for SQL Server Certificate with FQDN name

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SSL_CERTIFICATE_FQDN Category: Policy Compliance	■ Windows 2000 (220160) ■ Windows 2003 (224160) ■ Windows 2008 (253160)	Title: SSL certificate does not contain the FQDN name Description: The 'Friendly name' property of the SSL certificate configured for the SQL Server does not contain the FQDN name of the server within it.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_SSL_CERT_NOT_FOUND Category: System Error	■ Windows 2000 (220161) ■ Windows 2003 (224161) ■ Windows 2008 (253161)	Title: SSL certificate not found Description: The SQL Server SSL certificate cannot be found.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_SSL_CERT_PROP_NOEXIST Category: System Information	■ Windows 2000 (220162) ■ Windows 2003 (224162) ■ Windows 2008 (253162)	Title:SSL certificate's property not found Description: The SSL certificate's property was not found. Please refer information field for details.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-64 Messages for SQL Server Certificate with FQDN name *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SSL_CERT_NOCONFIG Category: Policy Compliance	■ Windows 2000 (220163) ■ Windows 2003 (224163) ■ Windows 2008 (253163)	Title: SSL certificate not configured for SQL Server Description: SSL certificate has not been configured for the SQL Server.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Ad hoc queries

This check reports servers that are configured to process ad hoc queries. Malicious users can use ad hoc queries to gain unauthorized access to data. Use the name list to include or exclude data providers for the check.

To disable an ad hoc query for a provider, create a new DWORD registry value named DisallowAdhocAccess in the Windows registry under HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\MSSQLServer\Providers and set the value to 1.

To protect your computers, prohibit ad hoc access for each data provider unless required.

The following table lists the message for the check.

Table 3-65 Message for Ad hoc queries

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ADHOC_ENABLED Category: Policy Compliance	■ Windows 2000 (220135) ■ Windows 2003 (224135) ■ Windows 2008 (253135)	Title: Ad hoc queries enabled Description: Ad hoc queries should be disabled for each data access provider if not needed.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Broadcast servers

This check reports the SQL Servers that are broadcasting on the network. Use the name list to specify the servers that you want to include or exclude for this check.

The following table lists the message for the check.

Table 3-66 Message for Broadcast servers

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_BROADCAST_SERVER Category: System Information	■ Windows 2000 (220142) ■ Windows 2003 (224142) ■ Windows 2008 (253142)	Title: Broadcast server Description: The SQL Server is local or is broadcasting on the network.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Configuration parameters

This check reports the unauthorized configuration parameter values as specified in the enabled SQL Server Configuration Parameters templates. Use the name lists to enable and disable template files.

Symantec ESM Modules for MS SQL Server Databases ships with one sample SQL Server Configuration Parameters template (mssqlconfig.scp), which is enabled by default. At least one template file must be enabled for this check to work successfully.

Note: This check only reports the parameters that are accessible through the sp_configure stored procedure. To report the advanced configuration options, set **Show advanced options** to 1.

To protect your computers, make sure that SQL servers are configured in accordance with your company's security policy.

The following table lists the messages for the check.

Table 3-67 Messages for Configuration parameters

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MCP_GREEN_LEVEL Category: Policy Compliance	■ Windows 2000 (220131) ■ Windows 2003 (224131) ■ Windows 2008 (253131)	Title: Unauthorized configuration parameter (Green level) Description: The SQL Server configuration parameter matches a green level template entry.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_MCP_YELLOW_LEVEL Category: Policy Compliance	■ Windows 2000 (220132) ■ Windows 2003 (224132) ■ Windows 2008 (253132)	Title: Unauthorized configuration parameter (Yellow level) Description: The SQL Server configuration parameter matches a yellow level template entry.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-67 Messages for Configuration parameters *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MCP_RED_LEVEL Category: Policy Compliance	■ Windows 2000 (220133) ■ Windows 2003 (224133) ■ Windows 2008 (253133)	Title: Unauthorized configuration parameter (Red level) Description: The SQL Server configuration parameter matches a red level template entry.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_MCP_NOT_FOUND Category: Policy Compliance	■ Windows 2000 (220134) ■ Windows 2003 (224134) ■ Windows 2008 (253134)	Title: Configuration parameter not found Description: The SQL Server configuration parameter is not found.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Default login ID

This check reports the unauthorized default server login IDs for users of the trusted connections that do not have a matching logon name. Use the name list to specify authorized default login IDs.

SQL Server 2000 uses the default login ID setting to provide backward compatibility. It can be verified using the xp_loginconfig extended stored procedure.

To protect your computers, cChange unauthorized login IDs in the registry location HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\<instance>\DefaultLogin.

The following table lists the message for the check.

Table 3-68 Message for Default login ID

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_ DEFAULT_LOGIN Category: Policy Compliance	■ Windows 2000 (220141) ■ Windows 2003 (224141) ■ Windows 2008 (253141)	Title: Unauthorized default login Description: The default login ID does not match a login in the allowed login name list.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

MSSQL Server Agent Proxy Account

This check reports MSSQL server agent proxy accounts. An existing Windows account is configured as an SQL Server Agent proxy account with the appropriate level of rights. When the user wants to start a new Windows process with a reduced level of rights, this SQL Server Agent proxy account is used.

The following table lists the messages for the check.

Table 3-69 Messages for MSSQL Server Agent Proxy Account

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_PROXY_ACCOUNT_2000 Category: Policy Compliance	■ Windows 2000 (220147) ■ Windows 2003 (224147) ■ Windows 2008 (253147)	Title: MSSQL Server Agent Proxy Account Description: The following MSSQL Server Agent Proxy Account was detected. The proxy account is used by SQL Server Agent and the xp_cmdshell extended stored procedure when executing jobs or commands for users who are not members of the sysadmin fixed server role. The proxy account is a Microsoft Windows account in whose security context the jobs or command prompt commands are run.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-69 Messages for MSSQL Server Agent Proxy Account *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_PROXY_ACCOUNT_2005 Category: Policy Compliance	■ Windows 2000 (220148) ■ Windows 2003 (224148) ■ Windows 2008 (253148)	Title: MSSQL Server Agent Proxy Account 2005 Description: The following MSSQL Server Agent Proxy Account was detected. An existing Windows account is configured as an SQL Server Agent proxy account with the appropriate level of rights. When one wants to start a new Windows processes with a reduced level of rights, this SQL Server Agent proxy account is used.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-69 Messages for MSSQL Server Agent Proxy Account *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NO_PROXY_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220149) ■ Windows 2003 (224149) ■ Windows 2008 (253149)	Title: MSSQL Server Agent Proxy Account Not Configured Description: MSSQL Server Agent Proxy Account was not detected. This can be because no proxy account has been configured. An existing Windows account is configured as an SQL Server Agent proxy account with the appropriate level of rights. When one wants to start a new Windows processes with a reduced level of rights, this SQL Server Agent proxy account is used.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Microsoft Distributed Transaction Coordinator auto start

This check reports the SQL Servers with the Microsoft Distributed Transaction Coordinator (MSDTC) service that is enabled to start automatically at system startup.

To protect your computers, if the MSDTC service is not required to start automatically, disable it or start it manually as needed.

The following table lists the message for the check.

Table 3-70 Message for Microsoft Distributed Transaction Coordinator auto start

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_MSDTC_AUTO_START Category: Policy Compliance	■ Windows 2000 (220138) ■ Windows 2003 (224138) ■ Windows 2008 (253138)	Title: MSDTC starts automatically Description: The Microsoft Distributed Transaction Coordinator (MSDTC) service is set to start automatically at system startup. This service should be disabled or set to start manually if it is not needed.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Registry configuration parameters

This check reports the unauthorized registry configuration parameter values that are specified in the enabled SQL Server Registry Configuration Parameters templates.

The following table lists the messages for the check.

Table 3-71 Messages for Registry configuration parameters

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_RCP_GREEN_LEVEL Category: Policy Compliance	■ Windows 2000 (220150) ■ Windows 2003 (224150) ■ Windows 2008 (253150)	Title: Unauthorized registry configuration parameter (Green level) Description: The SQL Server registry configuration parameter matches a green level template entry.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Table 3-71 Messages for Registry configuration parameters *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_RCP_YELLOW_LEVEL Category: Policy Compliance	■ Windows 2000 (220151) ■ Windows 2003 (224151) ■ Windows 2008 (253151)	Title: Unauthorized registry configuration parameter (Yellow level) Description: The SQL Server registry configuration parameter matches a yellow level template entry.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_RCP_RED_LEVEL Category: Policy Compliance	■ Windows 2000 (220152) ■ Windows 2003 (224152) ■ Windows 2008 (253152)	Title: Unauthorized registry configuration parameter (Red level) Description: The SQL Server registry configuration parameter matches a red level template entry.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_RCP_NOT_FOUND Category: Policy Compliance	■ Windows 2000 (220153) ■ Windows 2003 (224153) ■ Windows 2008 (253153)	Title: Registry configuration parameter not found Description: The SQL Server registry configuration parameter is not found.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Remote servers

This check reports the remote servers that are being used through the local server.

The following table lists the message for the check.

Table 3-72 Message for Remote servers

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_REMOTE_SERVER Category: Policy Compliance	■ Windows 2000 (220154) ■ Windows 2003 (224154) ■ Windows 2008 (253154)	Title: Remote server detected Description: A remote server has been detected. A remote server is a server that you access as part of a client process without opening a separate, distinct, direct client connection.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Agent auto start

This check reports the SQL Servers with the SQL Agent service enabled to start automatically at system startup.

To protect your computers, if SQL Agent is not required to start automatically, disable it or start it manually as needed.

The following table lists the message for the check.

Table 3-73 Message for SQL Agent auto start

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SQLAGENT_AUTO_START Category: Policy Compliance	■ Windows 2000 (220139) ■ Windows 2003 (224139) ■ Windows 2008 (253139)	Title: SQL Agent starts automatically Description: The SQL Agent service is set to start automatically at system startup. This service should be disabled or set to start manually if it is not needed.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Agent service account

This check reports unauthorized SQL Agent service accounts. Use the name list to specify accounts that are authorized to run the SQL Agent service. For convenience, the %domainname% keyword can be used to represent the domain name where the SQL Server is installed. Valid entries include:

Table 3-74 Valid entries and their descriptions

Entry	Description
Account_name	The specified account is authorized.
Domain_name\Account_name	The specified domain account is authorized.
Domain_name*	Any account on the specified domain is authorized.
%domainname%\Account_name	The specified domain account is authorized.
%domainname%*	Any domain account is authorized.

To protect your computers, use a low-privilege account for the SQL Agent service instead of using LocalSystem or Administrator.

The following table lists the message for the check.

Table 3-75 Message for SQL Agent service account

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_AGENT_SERVICE_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220137) ■ Windows 2003 (224137) ■ Windows 2008 (253137)	Title: Unauthorized SQL Agent service account Description: The Microsoft Windows account assigned to run the SQL Agent service does not match an account listed in the name list. The SQL Agent service should be run as an account with the least amount of privilege needed. Avoid using high privilege accounts such as LocalSystem or administrator.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Mail enabled

This check reports the SQL servers that have a configured SQL Mail profile or an SQL Mail session running.

To protect your computers, if SQL Mail is not required, disable it by removing the configured MAPI profile.

Note: The SQL Mail enabled check is not supported on MS SQL Server 2005 (64-bit).

The following table lists the message for the check.

Table 3-76 Message for SQL Mail enabled

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SQLMAIL_ENABLED Category: Policy Compliance	■ Windows 2000 (220140) ■ Windows 2003 (224140) ■ Windows 2008 (253140)	Title: SQL Mail enabled Description: SQL Mail is configured for this server. Disable this feature if it is not needed.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server installed on domain controller

This check reports the SQL Servers that are installed on a domain controller.

If an SQL Server is installed on a domain controller, any SQL Server vulnerability could compromise the entire domain.

To protect your computers, never install MS SQL Server on a domain controller.

The following table lists the message for the check.

Table 3-77 Message for SQL Server installed on DC

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVER_ON_DC Category: Policy Compliance	■ Windows 2000 (220143) ■ Windows 2003 (224143) ■ Windows 2008 (253143)	Title: SQL Server installed on domain controller Description: The server is installed on a domain controller.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server login rights

This check reports the unauthorized SQL Server logins that permit server access. Use the name list to include or exclude SQL Server logins. For convenience, the %domainname% keyword can be used to represent the domain name where the SQL Server is installed, for example, %domainname%\username1.

To protect your computer, review logins to make sure that they are authorized and deny server access to unauthorized logins using the login properties setting in the SQL Server Enterprise Manager.

The following table lists the message for the check.

Table 3-78 Message for SQL Server login rights

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVER_LOGIN_RIGHT Category: Policy Compliance	■ Windows 2000 (220145) ■ Windows 2003 (224145) ■ Windows 2008 (253145)	Title: SQL Server login permits server access Description: The login has unauthorized login right to the named SQL server.	Severity: red-4 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server path

This check reports the SQL Servers that are not installed on an authorized path. Use the name list to specify the authorized paths. The %instancepath% keyword represents the default installation path for named instances, for example, MSSQL$Instance_name.

To protect your computer, install SQL servers in secure and authorized locations.

The following table lists the message for the check.

Table 3-79 Message for SQL Server path

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVER_PATH Category: Policy Compliance	■ Windows 2000 (220144) ■ Windows 2003 (224144) ■ Windows 2008 (253144)	Title: SQL Server on unauthorized path Description: The server is installed on an unauthorized path.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server service account

This check reports unauthorized SQL Server service accounts. Use the name list to specify the accounts that are authorized to run the SQL Server service. For convenience, the %domainname% keyword can be used to represent the domain name where the SQL Server is installed. Valid entries include:

Table 3-80 Valid entries and their descriptions

Entry	Description
Account_name	The specified account is authorized.
Domain_name\Account_name	The specified domain account is authorized.
Domain_name*	Any account on the specified domain is authorized.
%domainname%\Account_name	The specified domain account is authorized.
%domainname%*	Any domain account is authorized.

To protect your computers, use a low-privilege account for the SQL Agent service instead of using LocalSystem or Administrator.

The following table lists the message for the check.

Table 3-81 Message for SQL Server service account

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVER_SERVICE_ACCOUNT Category: Policy Compliance	■ Windows 2000 (220136) ■ Windows 2003 (224136) ■ Windows 2008 (253136)	Title: Unauthorized SQL Server service account Description: The Microsoft Windows account assigned to run the SQL Server service does not match an account listed in the name list. The SQL Server service should be run as an account with the least amount of privilege needed. Avoid using high privilege accounts such as LocalSystem or administrator.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Servers to check

Use the name list to specify the servers that are to be excluded or included for all SQL Server Configuration security checks.

By default, all servers that are selected during installation are included.

Started SQL Server endpoint

This check reports the started SQL Server endpoints that the SQL Server's Database Engine uses to communicate with the applications. This check is not supported on SQL Server 2000.

The following table lists the message for the check.

Table 3-82 Message for Started SQL Server endpoint

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_SERVER_ENDPOINT Category: Policy Compliance	■ Windows 2000 (220146) ■ Windows 2003 (224146) ■ Windows 2008 (253146)	Title: Started SQL Server endpoint Description: The started SQL Server endpoint is listening and processing requests.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Version and product level

This check reports the SQL Server version and product (service pack) level.

To protect your computers, install the latest service packs on your SQL servers.

The following table lists the message for the check.

Table 3-83 Message for Version and product level

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_VERSION_LEVEL Category: System Information	■ Windows 2000 (220130) ■ Windows 2003 (224130) ■ Windows 2008 (253130)	Title: SQL Server version and product level Description: The SQL Server version and product level.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

SQL Server Roles

The checks in the SQL Server Roles module report the following:

- Unauthorized members of fixed-server roles.

- Unauthorized members of database roles.
- Unauthorized application roles.
- Unauthorized nested roles.
- Users that are not assigned to a database role.
- Fixed-server roles and members that were added to the server after the last snapshot update.
- Fixed-server roles and members that were deleted from the server after the last snapshot update.
- Database roles and members that were added to the server after the last snapshot update.
- Database roles and members that were deleted from the server after the last snapshot update.
- Database users that were added to all the databases.
- Database roles that include or exclude the databases for the new and database role checks.

During a policy run, the module detects if the cluster node on which the ESM agent is installed, is the active node running the configured SQL Server instance and reports the check execution results of the module only from that node. For all the other nodes in the cluster, the module reports a message.

The following table lists the message for the module.

Table 3-84 SQL Server Roles module message

Message String ID	Message Title	Message Severity
ESM_CLUSTER_NOT_ ON_ACTIVENODE	Cluster instance not on active node	green-0

Application roles

This check reports the unauthorized application roles for each database. Use the name list to specify the roles to be included (accepted) or excluded (prohibited). Leave the list empty to prohibit all application roles.

To protect your computers, periodically review and drop unauthorized application roles from the database.

The following table lists the message for the check.

Table 3-85 Message for Application roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_APP_ROLE Category: Policy Compliance	■ Windows 2000 (220432) ■ Windows 2003 (224432) ■ Windows 2008 (253432)	Title: Unauthorized application role Description: The named application role is not specified as an authorized role for the database. Drop the role from the database if it is unauthorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Automatically update snapshots

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

Database role members

This check reports the unauthorized members of fixed and user-defined database roles that are specified in the enabled SQL Server Database Role Member templates. Use the name lists to enable and disable the template files.

To protect your computers, review members of fixed and user-defined roles often and drop unauthorized users from role memberships.

The following table lists the message for the check.

Table 3-86 Message for Database role members

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DATABASE_ROLE_MEM Category: Policy Compliance	■ Windows 2000 (220431) ■ Windows 2003 (224431) ■ Windows 2008 (253431)	Title: Unauthorized member of database role Description: The named user is not an authorized member of the database role as specified in the enabled template files. Drop the user from the role membership if it is not authorized, or update the membership template if the user should be an authorized member of the database role.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Database roles

This check lists databases roles.

The following table lists the message for the check.

Table 3-87 Message for Database roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DATABASE_ROLE Category: System Information	■ Windows 2000 (220443) ■ Windows 2003 (224443) ■ Windows 2008 (253443)	Title: Database role Description: The SQL Server database role.	Severity: green-0 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Databases - Application roles

Use this option's name list to specify the databases that are to be excluded or included for the Application roles check.

By default, all databases on each server that is specified in the Servers to check option are included.

Databases - Nested roles

Use this option's name list to specify the databases that are to be included or excluded by the Nested roles check.

By default, all databases on each server that is specified in the Servers to check option are included.

Databases - Roles

Use this option's name list to specify the databases that are to be excluded or included for the database roles, new and deleted database role and member checks.

Databases - Users without role

Use this option's name list to specify the databases that are to be included or excluded for the Users without roles check.

Deleted database role and member

This check reports the database roles and members that were deleted from the server after the last snapshot update. Use the name list to specify the database role names that should be included or excluded from this check.

The following table lists the messages for the check.

Table 3-88 Messages for Deleted database role and member

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DELETED_DATABASE_ROLE Category: Change Notification	■ Windows 2000 (220441) ■ Windows 2003 (224441) ■ Windows 2008 (253441)	Title: Deleted database role Description: The SQL Server database role was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_DELETED_DB_ROLE_MEMBER Category: Change Notification	■ Windows 2000 (220442) ■ Windows 2003 (224442) ■ Windows 2008 (253442)	Title: Deleted database role member Description: The SQL Server database role member was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Deleted fixed-server role and member

This check reports fixed-server roles and members that were deleted from the server after the last snapshot update. Use the name list to include or exclude fixed-server role names in the check.

The following table lists the messages for the check.

Table 3-89 Messages for Deleted server role and member

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_DELETED_SERVER_ROLE Category: Change Notification	■ Windows 2000 (220437) ■ Windows 2003 (224437) ■ Windows 2008 (253437)	Title: Deleted fixed server role Description: The SQL Server server role was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]
String ID: ESM_MSSQL_DELETED_SRV_ROLE_MEMBER Category: Change Notification	■ Windows 2000 (220438) ■ Windows 2003 (224438) ■ Windows 2008 (253438)	Title: Deleted fixed server role member Description: The SQL Server server role member was deleted after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Fixed-server role members

This check reports the unauthorized members of the fixed-server roles that are specified in the enabled SQL Server Fixed-Server Role Member templates. Use the name lists to enable and disable the template files.

To protect your computers, review members of fixed-server roles often and drop unauthorized users from role memberships.

The following table lists the message for the check.

Table 3-90 Message for Fixed-server role members

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_FIXED_SERVER_ROLE_MEM Category: Policy Compliance	■ Windows 2000 (220430) ■ Windows 2003 (224430) ■ Windows 2008 (253430)	Title: Unauthorized member of fixed-server role Description: The named user is not an authorized member of the fixed-server role as specified in the enabled template files. Drop the user from the role membership if it is not authorized, or update the membership template if the user should be an authorized member of the fixed-server role.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Nested roles

This check reports the nested roles for each database. Use the name list to specify the roles that are to be included or excluded for this check. Leave the list empty to prohibit all the application roles.

To protect your computers, periodically review and drop unauthorized nested roles from the database.

The following table lists the message for the check.

Table 3-91 Message for Nested roles

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NESTED_ROLE Category: Policy Compliance	■ Windows 2000 (220433) ■ Windows 2003 (224433) ■ Windows 2008 (253433)	Title: Unauthorized nested role Description: The named role is not specified as an authorized nested role for the database. Drop the nested role from the role member in the database if it is unauthorized.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

New database role and member

This check reports the database roles and members that were added to the server after the last snapshot update. Use the name list to specify the database role names that should be included or excluded from this check.

The following table lists the messages for the check.

Table 3-92 Messages for New database role and member

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_DATABASE_ROLE Category: Change Notification	■ Windows 2000 (220439) ■ Windows 2003 (224439) ■ Windows 2008 (253439)	Title: New database role Description: The SQL Server database role was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Table 3-92 Messages for New database role and member *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_DB_ROLE_MEMBER Category: Change Notification	■ Windows 2000 (220440) ■ Windows 2003 (224440) ■ Windows 2008 (253440)	Title: New database role member Description: The SQL Server database role member was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

New fixed-server role and member

This check reports fixed-server roles and members that were added to the server after the last snapshot update. Use the name list to include or exclude fixedserver role names from this check.

The following table lists the messages for the check.

Table 3-93 Messages for New fixed-server role and member

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_SERVER_ROLE Category: Change Notification	■ Windows 2000 (220435) ■ Windows 2003 (224435) ■ Windows 2008 (253435)	Title: New fixed server role Description: The SQL Server server role was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Table 3-93 Messages for New fixed-server role and member *(continued)*

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_NEW_SERVER_ROLE_MEMBER Category: Change Notification	■ Windows 2000 (220436) ■ Windows 2003 (224436) ■ Windows 2008 (253436)	Title: New fixed server role member Description: The SQL Server server role member was added after the last snapshot update.	Severity: yellow-2 Correctable: false Snapshot Updatable: true Template Updatable: false Information Field Format: [%s]

Servers to check

Use the name list to specify the servers that are to be excluded or included for all the SQL Server Roles security checks.

By default, all servers that are selected during installation are included.

Users without role

This check reports the users that are not assigned to a database role other than the public role. Use the name list to specify the users that are to be included or excluded for this check.

Directly granting object and statement permissions to users requires excessive management effort and does not promote the security principle of “least privilege.”

To protect your computers, do not assign object and statement permissions directly to users. Assign users to roles and then assign object and statement permissions to roles.

The following table lists the message for the check.

Table 3-94 Message for Users without role

Message String ID and Category	Platform and Message Numeric ID	Message Title and Description	Additional Information
String ID: ESM_MSSQL_USER_WITHOUT_ROLE Category: Policy Compliance	■ Windows 2000 (220434) ■ Windows 2003 (224434) ■ Windows 2008 (253434)	Title: Users not assigned to a role Description: The named user is not assigned to a role besides public role for the database.	Severity: yellow-2 Correctable: false Snapshot Updatable: false Template Updatable: false Information Field Format: [%s]

Chapter 4

Troubleshooting

This chapter includes the following topics:

Module errors

If you encounter unexpected system errors or SQL query failure errors, check if the user account, which was specified during configuration, has minimum privileges assigned to it. If not, assign the required privileges and run the policy again.

Encryption exception

An error may be reported when you run a policy.

Table 4-1 Encryption exception

Error	Solution
Encryption exception	This error may occur if you have set SSLConfigure=0 after configuring the MS SQL module. This error may also occur if you have renamed or deleted the AESConfigure.dat file. To solve this problem, you need to reconfigure the MS SQL module. If you want to generate logs for encryption, add Debugon=1 in the AESConfigMSSQLSERVER.dat file from esm\config folder. This generates MSSQLSERVERAESdebuglog in the esm\system\<platform> folder.

Account locked out

You may encounter errors while running policies that may lock the user account.

Table 4-2 Account locked out

Error	Solution
User account gets locked after running a Policy run on MSSQL module	For every check, the MS SQL module connects to the database. The user account gets locked based on the Windows Password policy. To solve this problem, make sure the credentials supplied for each database are correct.

Chapter 5

Frequently asked questions

This chapter includes the following topics:

Deploying ESM Modules for MS SQL Servers

How can I deploy Symantec ESM Modules for MS SQL Server databases?

There are two ways that you can use to deploy the ESM Modules for MS SQL Server Databases:

- Network-based deployment
- Host-based deployment

Network-based deployment

You can make the existing 32-bit or 64-bit ESM application modules for MS SQL Server report on Microsoft SQL Server 32-bit and 64-bit databases.

You can use the network-based deployments to report on the SQL Server 2005 and 2008 clusters.

Host-based deployment

You need to install 32-bit or 64-bit ESM application modules for MS SQL Server on every MS SQL Server that you want to report on.

See "Configuration of the ESM SQL Server modules for MS SQL Server Databases " on page 30.

You can use the host-based deployments to report on the SQL Server 2005 and 2008 clusters.

Changing the configuration of an MS SQL Server

How can I change the configuration of an MS SQL Server if its password has been changed?

To change the configuration of the MS SQL Server if its password has been changed, do either of the following:

- Remove the configuration record of he MS SQL Server and add it again silently.
- Modify the configuration record of tthehat MS SQL Server by using the -m option with MSSQLSetup.exe interactively.
- Run the SQL Server Discovery module.
  See "Configuring the SQL Server by using the SQL Server SQL Server Discovery module" on page 33.