Symantec Enterprise Security Manager™ Modules for Microsoft SQL Server Databases User's Guide and Reference

Release 3.0 for Symantec ESM 6.0, 6.1, and 6.5.x

For Windows 2000, Windows Server 2003, and Windows XP

SQL 2000 and SQL 2005

Symantec ESM Modules for Microsoft SQL Server User's Guide and Reference

Release 3.0

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Privacy; Data Protection:

Symantec may collect and store certain non-personally identifiable information for product administration and analysis. Symantec may disclose the collected information if asked to do so by a law enforcement official as required or permitted by law or in response to a subpoena or other legal process. In order to promote awareness, detection and prevention of Internet security risks, Symantec may share certain information with research organizations and other security software vendors. Symantec may also use statistics derived from the information to track and publish reports on security risk trends. By using the Licensed Software, You acknowledge and agree that Symantec may collect, transmit, store, disclose and analyze such information for these purposes. From time to time, the Licensed Software will collect certain information from the computer on which it is installed, which may include: (a) Information regarding installation of the WebClient Installer including username and password which should not be personally identifiable if You have chosen an alias to protect Your identity. (b) Information collected by the WebClient Profile such as mandatory user/employee information including, name, e-mail address, title, position, physical address and use ID/ employee ID as well as IP address and username. (c) Other information including username, user events and IP addresses which is used for product administration and analysis. All of the above information is collected and stored on the Your side and is not transferred to Symantec. Consult Your company’s privacy policy for further information.

Technical support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec technical support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

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

www.symantec.com/techsupp/

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

Contacting Technical Support

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

www.symantec.com/techsupp/

Select your region or language under Global Support.

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate the problem.

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

- Product release level
- Hardware information

- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/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/

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer Service

Customer service information is available at the following URL:
www.symantec.com/techsupp/

Select your country or language under Global Support.

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

- 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 insurance and maintenance contracts
- Information about Symantec Value License Program
- 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: contractsadmin@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, xpertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

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

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

http://www.symantec.com

Select your country or language from the site index.

Technical support

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

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

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

Licensing and registration

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

Contacting Technical Support

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

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

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

Contents

Chapter 1

Introducing Symantec ESM Modules for Microsoft SQL Server Databases

This chapter includes the following topics:

About Symantec ESM Modules for Microsoft SQL Server Databases

Symantec Enterprise Security Manager (ESM) Modules for Microsoft SQL (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 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, Windows XP, 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 Microsoft SQL 2000 and 2005 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, six new modules and five 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 Modules for MS SQL Server Databases installs the modules that are described in the following topics.

SQL Server Accounts

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. See "SQL Server Accounts" on page 40.

SQL Server Auditing

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. See "SQL Server Accounts" on page 40.

SQL Server Configuration

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. See "SQL Server Configuration" on page 46.

SQL Server Objects

Checks in this module report 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. See "SQL Server Objects" on page 58.

SQL Server Password Strength

Checks in this module report use of an unauthorized authentication mode, logins with empty passwords, and easily guessed passwords. See "SQL Server Password Strength" on page 78.

SQL Server Roles

Checks in this module report unauthorized members of fixed-server roles, unauthorized members of database roles, and unauthorized application roles. See "SQL Server Accounts" on page 40.

Templates

Several of the documented modules use templates to store authorized agent and object settings. Differences between current agent and object settings and template values are reported when the modules run.

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 shows the modules and checks that use template files in Symantec ESM Modules for MS SQL Server Databases.

Table 1-1 Template files

Module	Check name	Template name	Predefined template
SQL Server Configuration	Configuration parameters	SQL Server Configuration Parameters	mssqlconfig.scp
SQL Server Objects	Database configuration	SQL Server Database Configuration Parameters	mssqldatabase.mdp
	Stored procedure permissions	SQL Server Database Stored Procedure Permissions	mssqlstoredprocedure.mpp
	Statement permissions	SQL Server Statement Permissions	mssqlstatementpermission.msp
	Object permissions	SQL Server Object Permissions	mssqlobjectpermission.mop
SQL Server Roles	Fixed-server role members	SQL Server Fixed-Server Role Member	none
	Database role members	SQL Server Database Role Member	none

How Symantec ESM 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 Symantec ESM Modules for MS SQL Server Databases

You can use Symantec ESM Modules for Microsoft SQL Server Databases in the same way that you use other Symantec ESM modules.

- Create a Symantec ESM policy using one or more SQL modules
- Configure the new policy
- Configure applicable templates
- Run the policy
- Review the policy run

Where you can get more information

See "Using policies, templates, snapshots, and modules" in the latest version of your *Symantec Enterprise Security User's Guide* and "Reviewing policies, modules, and messages" in the latest version of your *Symantec ESM Security Update User's Guide* for more information about Symantec ESM modules.

For more information on Symantec ESM Security Updates see *Symantec Enterprise Security User's Guide*.

For more information on Symantec ESM, Symantec ESM Security Updates, and Symantec ESM support for database products, see the Symantec Security Response Web site at http://securityresponse.symantec.com.

2

Installing Symantec ESM Modules for MS SQL Server Databases

This chapter includes the following topics:

Symantec ESM Modules for MS SQL Server Databases can be installed on Windows 2000, Windows XP, and Windows Server 2003. Policies that are created using these network-based modules can run against any MS SQL Server 2000 and 2005 database on your network.

Before you install

Before you install Symantec ESM Modules for MS SQL Server Databases, you need to verify the following:

CD-ROM access	At least one machine on your network must have a CD-ROM drive.
Account privileges	You must have administrator rights 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	A Symantec ESM agent must be running and registered to at least one Symantec ESM manager.
ESM Security Update 17	ESM SU17 or greater must be installed on the same computer as your Symantec ESM manager.
SQL Client Tools	The following Microsoft SQL Client Tools must be installed on each Symantec ESM agent where the modules will run: ■ Management tools ■ Client connectivity You need not install any other components of the Microsoft SQL Client Tools on the agents.

Minimum account privileges

Table 2-1 lists the minimum privileges for login accounts that are needed to perform ESM security checks on MSSQL 2000 and 2005 Server.

Note: These requirements are the same as those required by the Microsoft Enterprise Manager and SQL Server Management Studio.

Table 2-1 Minimum privileges for login accounts

Modules	Database	Privileges
All	2000	select master..syscurconfigs
All	2000	select master..sysusers
All	2000	select master..sysxlogins
All	2000	select master..syslogins

Table 2-1 Minimum privileges for login accounts

Modules	Database	Privileges
All	2000	select master..sys.databases
All	2000	select master..sysobjects
All	2000	exec master..sp_configure
All	2000	exec master..sp_helpsrvrole
All	2000	exec master..sp_helpsrvrolemember
All	2000	exec master..xp_instance_regenumkeys
All	2000	exec master..xp_instance_regread
All	2000	exec master..xp_loginconfig
All	2000	exec master..xp_regread
All	2000	exec master..xp_startmail
All	2000	exec master..xp_stopmail
All	2000	exec master..xp_sqlagent_proxy_account
All	2000	exec master..sp_helprole
All	2000	exec master..sp_helprolemember
All	2000	exec master..sp_helprotect
All	2000	exec master..sp_helpuser
All	2000	exec master..sp_helpdb
All	2005	select master.sys.endpoints
All	2005	select master.sys.databases
All	2005	select master.sys.sysusers
All	2005	select master.sys.syslogins
All	2005	select master.sys.sql_modules
All	2005	select master.sys.database_principals
All	2005	select master.sys.server_principals
All	2005	select master.sys.server_permissions
All	2005	select master.sys.schemas
All	2005	select master.sys.sysobjects

Table 2-1 Minimum privileges for login accounts

Modules	Database	Privileges
All	2005	select master.sys.configurations
All	2005	exec master.sys.xp_regread
All	2005	exec master.sys.xp_instance_regread
All	2005	exec master.sys.sp_helpuser
All	2005	exec master.sys.sp_helprole
All	2005	exec master.sys.sp_helprolemember
All	2005	exec master.sys.sp_helpsrvrole
All	2005	exec master.sys.sp_helpsrvrolemember
All	2005	exec master.sys.xp_loginconfig
All	2005	exec master.sys.xp_startmail
All	2005	exec master.sys.xp_stoptmail
All	2005	exec master.sys.xp_instance_regnumkeys
All	2005	exec master.sys.sp_configure
All	2005	exec master.sys.sp_helpdb
All	2005	exec master.sys.sp_helprotect
All	2005	exec msdb.dbo.sp_help_proxy
SQL Server Password Strength	2005	Control Server permission
SQL Server Configuration	2005	Must be a member of SQLAgentOperatorRole

Note: Apart from the above permissions, you must grant the 'db_datareader' database role for every user database that you want to report on. For MS SQL Server 2005, the 'db_datareader' database role is not required if Control Server permission is granted.

System requirements

Table 2-2 lists the operating systems on which the ESM application modules for Microsoft SQL Server can be installed.

Table 2-2 Operating systems for ESM application modules

Supported operating systems	Supported OS versions
Windows x86	2000
Windows x86	XP
Windows x86, EM64T, and Opteron	2003 Server

Table 2-3 lists the Microsoft SQL Server operating systems on which the ESM application modules for Microsoft SQL Server can report.

Table 2-3 Microsoft SQL Server operating systems for ESM application modules

Supported Microsoft SQL Server operating systems	Supported OS versions	Supported Microsoft SQL Server versions
Windows (x86, Opteron, EM64T, and IA 64-bit)	2003 Server	2000, 2005
Windows (32-bit)	2000	2000, 2005
Windows (32-bit)	XP	2000, 2005

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

Table 2-4 Disk space requirements

Operating system	Hard disk space
Windows 2000 (32-bit)	15 MB
Windows XP (32-bit)	15 MB
Windows 2003 Server (32-bit)	18 MB
Windows 2003 Server (64-bit)	23 MB

Installing the modules

Symantec ESM Modules for MS SQL Server Databases are stored in an installation package, esmmssqltpi.exe, that does the following:

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

To run the installation program and register the files

1. From the CD, run \\ESM_App_Pol\Databases\MSSQL\Modules \<architecture>\esmmssqltpi.exe.
2. Select one of the following:

Option 1	Option 1 displays the contents of the package. To install the module, rerun esmmssqltpi.exe and select option 2.
Option 2	Option 2 displays the list of files that are installed and the modules or templates to which they belong.

Note: Register template and .m files only once for agents that use the same Symantec ESM manager on the same operating system.

3. Do one of the following:
   - If the files are not registered with the manager, type **Y**.
   - If the files have already been registered, type **N** and skip to "To add security checking" on page 25.
4. Type the name of the manager to which the agent is registered. Typically, this is the name of the computer on which the manager is installed.
5. Type the logon name for the Symantec ESM manager.

Note: Throughout the installation, default or discovered information is contained in brackets ([ ]). Select the default by pressing Enter.

6. Type the password that is used to log on to the manager.
7. Do one of the following:
   - Type **1** to use IPX to contact the manager.
   - Type **2** to use TCP to contact the manager.

8 Type the port that is used to contact the Symantec ESM manager. The default port is 5600.

9 Type the agent name.

10 Do one of the following:

- If the displayed information is correct, type **Y**.
  File names are displayed as they are extracted.
- If the information is not correct, type **N**.
  The command line is returned.

To add security checking

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

2 Do one of the following:

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

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

4 Type 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 Server or Windows authentication. In either case, the user must be a member of the sysadmin fixed-server role to access all security-related settings. 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 Type the SQL Server or Windows password that is used to log on to the SQL Server.

6 Type the password again for verification.

7 Do one of the following:

- If the displayed information is correct, type **Y** to create a configuration record.
- If the displayed information is not correct, type **N** to begin again.

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

9 After you have created configuration records for each server that is detected by the installation program, the program lists all of the configuration records and the following three new options:

1	Manually add a configuration record for an undetected SQL Server
2	Modify or remove an existing configuration record
3	Finish and exit the installation

10 If you selected Option 2, do one of the following:

1	Modify the selected configuration record
2	Remove the selected configuration record
3	Skip the selected configuration record without modifying or removing it
4	Finish and exit the installation

Log

The following log is a sample installation. Your log may look different, depending on how your Symantec ESM manager and agents are configured.

```
Symantec Corporation tune-up/installation package


Options:
  1) Display the description and contents of the tune-up/
installation package.
  2) Install the tune-up/installation package on your system.


Enter option number [1]: 2
Installing package: "Symantec ESM Modules for MSSQL Server" 2.1
This package includes the following templates and/or ".m" files:


File: ...\Symantec\ESM\register\win2000\mssqlconfig.m.gz
Description:     ESM mssqlconfig.m module definition file
File: ...\Symantec\ESM\register\win2000\mssqlpass.m.gz
Description:     ESM mssqlpass.m module definition file
File: ...\Symantec\ESM\register\win2000\mssqlaudit.m.gz
Description:     ESM mssqlaudit.m module definition file
File: ...\Symantec\ESM\register\win2000\mssqlobject.m.gz
Description:     ESM mssqlobject.m module definition file
File: C:\ProgramFiles\Symantec\ESM\register\win2000\mssqlroles.m.gz
Description:     ESM mssqlroles.m module definition file
File: ...\Symantec\ESM\template\win2000\mssqlconfig.scp.gz
Description:     ESM template file


Template or *.m files need to be registered only once from the same
type of agent with the same manager.


If you have already registered this package for other agents of the
same type of operating system with the same manager you can skip
this step.


Do you wish to register the template or .m files [no]? yes


ESM manager that the agent is registered to: managername
```

```
ESM access name used to logon to the ESM manager [login]: login

Enter the ESM password used to logon to the ESM manager.
Password: *******

Enter the network protocol used to contact the ESM manager.
1) IPX
2) TCP
Enter 1 or 2 [2]: 2

Enter the port used to contact the ESM manager [5600]: 5600

Enter the name of the agent as it is registered to the ESM manager
[agentname]: agentname

ESM Manager   : managername
ESM user name : login
Protocol      : TCP
Port          : 5600
ESM agent     : agentname

Is this information correct? [yes] Y
Extracting ...\Symantec\ESM\bin\w2k-ix86\mtpkreg.exe.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlconfig.exe.gz...
Extracting ...\Symantec\ESM\register\win2000\mssqlconfig.m.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlconfig.rete.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlpass.exe.gz...
Extracting ...\Symantec\ESM\register\win2000\mssqlpass.m.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlpass.rete.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlaudit.exe.gz...
Extracting ...\Symantec\ESM\register\win2000\mssqlaudit.m.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlaudit.rete.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlobject.exe.gz...
Extracting ...\Symantec\ESM\register\win2000\mssqlobject.m.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlobject.rete.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlroles.exe.gz...
Extracting ...\Symantec\ESM\register\win2000\mssqlroles.m.gz...
```

```
Extracting ...\Symantec\ESM\bin\w2k-ix86\mssqlroles.rete.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\MSSQLCollector.exe.gz...
Extracting ...\Symantec\ESM\bin\w2k-ix86\MSSQLSetup.exe.gz...
Extracting ...\Symantec\ESM\template\win2000\mssqlconfig.scp.gz...

Continue and add configuration records to enable ESM security
checking for your MSSQL Server? [yes] Y

running: "...\Symantec\ESM\bin\w2k-ix86\MSSQLSetup.exe" -c

The ESM for SQL Servers module setup program has found the following
Servers:

SQL_Server1
SQL_Server2

Would you like to continue? [yes] Y

Add a configuration record for this server "SQL_Server1"? [yes] N

Continue to the next server? [yes] Y

Add a configuration record for this server "SQL_Server2"? [yes] Y

Verify the SQL Server name [SQL_Server2]: SQL_Server2

Login ID used to log on to the SQL Server: loginID

Enter the password used to log on to the SQL Server.
Password         : ********
Re-Enter password: ********

SQL Server : SQL_Server2
SQL Server login : loginID

Is this information correct? [yes] Y

Continue to the next server? [yes] Y
```

```
running: "...\Symantec\ESM\bin\w2k-ix86\MSSQLSetup.exe" -l

   *** Configuration records   ***
SQL Server : SQL_Server2
SQL Server login : loginID
   ***   ***   ***   ***

Options:
  1) Add a new configuration record
  2) Modify/remove existing configuration records
  3) Exit

Enter option number [3]: 2

running: "...\Symantec\ESM\bin\w2k-ix86\MSSQLSetup.exe" -m

Modify/remove the following SQL Server configuration record:

SQL Server : SQL_Server2

Options:
  1) Modify record
  2) Remove record
  3) Skip Record
  4) Finished modifying/removing records

Enter option number [3]: 4

running: "...\Symantec\ESM\bin\w2k-ix86\MSSQLSetup.exe" -l

   *** Configuration records   ***
SQL Server : SQL_Server2
SQL Server login : 2d21aea9aa4cd5f9
Password           : 2aa25cca3dc8ef495e8d7981710fa0d6
   ***   ***   ***   ***

Options:
```

```
  1) Add a new configuration record
  2) Modify/remove existing configuration records
  3) Exit

Enter option number [3]: 3

Tune-up pack installation complete
Re-registering modules/template files... Please wait...
Registering to manager computername
      checking: SQL Server Configuration
      checking: SQL Server Password Strength
      checking: SQL Server Auditing
      checking: SQL Server Objects
      checking: SQL Server Roles
      loading template information
updating template exchg2k.pw5 (Patch - Windows 2000 Professional)
  no update required
updating template exchg55.pw5 (Patch - Windows 2000 Professional)
  no update required
updating template fileatt.w50 (File - Windows 2000 Professional)
  no update required
updating template ie.pw5 (Patch - Windows 2000 Professional)
  no update required
updating template iis.pw5 (Patch - Windows 2000 Professional)
  no update required
updating template mime.rw5 (Registry - Windows 2000 Professional)
  no update required
updating template mssqlconfig.scp (SQL Server Configuration
Parameters - all)
updating template nthacktl.mfw (Malicious File Watch - all)
  no update required
updating template ntnipc.mfw (Malicious File Watch - all)
  no update required
updating template patch.pw5 (Patch - Windows 2000 Professional)
  no update required

updating template registry.rw5 (Registry - Windows 2000
Professional)
```

```
  no update required
updating template sql.pw5 (Patch - Windows 2000 Professional)
  no update required
updating template verisign.rw5 (Registry - Windows 2000
Professional)
  no update required
updating template w2k.fw (File Watch - all)
  no update required
updating template w2k.mfw (Malicious File Watch - all)
  no update required
updating template windows.fkl (File Keywords - all)
  no update required
updating template windows.pkl (Patch Keywords - all)
  no update required
sync'ing policy: Test
    sync'ing policy: Dynamic Assessment
    sync'ing policy: Phase 1
    sync'ing policy: Phase 2
    sync'ing policy: Phase 3:a Relaxed
    sync'ing policy: Phase 3:b Cautious
    sync'ing policy: Phase 3:c Strict
    sync'ing policy: Queries
    sync'ing policy: Development
End of installation.

          Please press <return> to exit ESM tuneup pack
```

Silently installing the modules

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

Table 2-5 Options to silently install the ESM 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

Table 2-5 Options to silently install the ESM modules for MS SQL Server Databases

Option	Description
-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

- At the command prompt, type the following:
  esmmssqltpi.exe -it -m <manager name> -U <Username> -p <port no> -P <password> -g <agent name > -Y -n -e

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

Post-installation tasks

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

Agent registration

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

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

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

Configuring the ESM modules for MS SQL Server Databases

After installing Symantec ESM Modules for MS SQL Server Databases, you can edit the configuration records and the configuration (.m) files. A configuration record is created for each database alias when you enable security checking during installation. Module configuration (.m) files contain the message information that Symantec ESM uses to report security check results.

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 \\Program Files\Symantec\ESM\bin\<platform>\ directory.

Table 2-6 lists the options that you can use when running MSSQLSetup.exe.

Table 2-6 Editing configuration records

To do this	Type
Display help.	**MSSQLSetup -h**
Create new configuration records for detected MS SQL servers.	**MSSQLSetup -c**
Add a configuration record for undetected MS SQL servers.	**MSSQLSetup -a**
Modify existing MS SQL Server configuration records.	**MSSQLSetup -m**
List existing Microsoft SQL Server configuration records.	**MSSQLSetup -l**
Specify a new input file for MS SQL Server configuration records. The default file is \\Program Files\Symantec \ESM\config\MSSQLServerModule.dat.	**MSSQLSetup -if <filename>**
Specify a new output file for MS SQL Server configuration records. The default file is \\Program Files\Symantec \ESM\config\MSSQLServerModule.dat.	**MSSQLSetup -of <filename>**
Remove specified SQL Server instance from configuration records	**MSSQLSetup -r**
List the MS SQL Servers instances that are available in the network	**MSSQLSetup -C**
List the MSSQL server and the instance that is installed on the local machine. Prompt for configuration of the MSSQL server and instances that are installed on the local machine.	**MSSQLSetup -i**
List the MSSQL server and the instance that is installed on the local machine, from which a user runs the MSSQL setup.	**MSSQLSetup -I**

Note: For host-based deployments, use **MSSQLSetup.exe -i**. For network-based deployments, use **MSSQLSetup.exe -c**.

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

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

Editing the .m file

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

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

Silently configuring the Symantec ESM Modules for MS SQL Server Databases

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

Use the following option to configure the ESM Modules for MS SQL Server Databases silently:

Table 2-7 Options for silently configuring the MS SQL Server Databases

To do this	Type
Specify the name of the SQL Server or the instance	**MSSQLSetup -S**
Specify the name of the user to connect to the SQL Server	**MSSQLSetup -A**
Specify the ClearTextPassword	**MSSQLSetup -P**
Remove the configuration record	**MSSQLSetup -r**

To silently configure the MS SQL Server

- At the command prompt, type the following:
  Mssqlsetup.exe -S <SQL Server Name\Instance name> -A <user name to connect to SQL Server> -P < ClearTextPassword>

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

- At the command prompt, type the following:
  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 C:\Program Files\Symantec\ESM\system\<machine name>.

Chapter 3

Reference

This chapter includes the following topics:

SQL Server Accounts

Checks in this module report SQL servers that:

- Have logon accounts
- Have logon accounts that were added to the database after the last snapshot update
- Have 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

Servers to check

Use the name list to include or exclude servers for all SQL Server Account checks.

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

Logon accounts

This check reports logon accounts and their status. Use the name list to include or exclude logon names in this check.

Table 3-1 lists the Logon account message.

Table 3-1 Logon account message

Message name	Title	Severity
ESM_MSSQ_LOGON_ACCOUNT	Logon account	Yellow-2

New logon accounts

This check reports logon accounts that were added to the database after the last snapshot update. Use the name list to include or exclude logon names in this check.

Table 3-2 lists the New logon accounts message.

Table 3-2 New logon accounts message

Message name	Title	Severity
ESM_MSSQ_NEW_LOGON_ACCOUNT	New logon account	Yellow-2

Deleted logon accounts

This check reports logon accounts that were deleted from the database after the last snapshot update. Use the name list to include or exclude logon names in this check.

Table 3-3 lists the Deleted logon accounts message.

Table 3-3 Deleted logon accounts message

Message name	Title	Severity
ESM_MSSQ_DELETED_LOGON_ ACCOUNT	Deleted logon account	Yellow-2

Logon account with sysadmin access

This check reports logon accounts with sysadmin access. Use the name list to include or exclude logon names in this check.

Table 3-4 lists the Logon account with sys admin access message.

Table 3-4 Logon account with sysadmin access message

Message name	Title	Severity
ESM_MSSQL_ SYSADMIN_ACCOUNT	Logon account with sysadmin access	Yellow-2

Logon account with securityadmin access

This check reports logon accounts with securityadmin access. Use the name list to include or exclude logon names in this check.

Table 3-5 lists the Logon account with security admin access message.

Table 3-5 Logon account with security admin access message

Message name	Title	Severity
ESM_MSSQL_ SECURITYADMIN_ ACCOUNT	Logon account with security admin access	Yellow-2

Logon account with serveradmin access

This check reports logon accounts with server admin access. Use the name list to include or exclude logon names in this check.

Table 3-6 lists the Logon account with server admin access message.

Table 3-6 Logon account with serveradmin access message

Message name	Title	Severity
ESM_MSSQL_ SERVERADMIN_ ACCOUNT	Logon account with serveradmin access	Yellow-2

Logon account with processadmin access

This check reports logon accounts with processadmin access. Use the name list to include or exclude logon names in this check.

Table 3-6 lists the Logon account with processadmin access message.

Table 3-7 Logon account with processadmin access message

Message name	Title	Severity
ESM_MSSQL_ PROCESSADMIN_ ACCOUNT	Logon account with processadmin access	Yellow-2

Logon account with setupadmin access

This check reports logon accounts that with setupadmin access. Use the name list to include or exclude logon names in this check.

Table 3-6 lists the Logon account with setup admin access message.

Table 3-8 Logon account with setupadmin access message

Message name	Title	Severity
ESM_MSSQL_ SETUPADMIN_ ACCOUNT	Logon account with setupadmin access	Yellow-2

Logon account with dbcreator access

This check reports logon accounts that with dbcreator access. Use the name list to include or exclude logon names in this check.

Table 3-6 lists the Logon account with dbcreator access message.

Table 3-9 Logon account with dbcreator access message

Message name	Title	Severity
ESM_MSSQL_ DBCREATOR_ ACCOUNT	Logon account with dbcreator access	Yellow-2

Automatically update snapshots

Use this option to update snapshots automatically.

SQL Server Auditing

Checks in this module report SQL servers that:

- Fail to audit at C2 level
- Have inadequate login audit level settings
- Have inadequate numbers of error log files
- Have inadequate database recovery modes
- Have

Servers to check

Use the name list to include or exclude servers for all SQL Server Auditing checks.

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

Login audit level

This check reports SQL servers that do not comply with the minimum login audit level that you specify in the check.

To configure the Login audit level check

- In the Audit level text box, type one of the following numeric values:

  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
3	All - log both successful and failed login attempts

The default value is 2.

Table 3-10 lists the Login audit level message.

Table 3-10 Login audit level message

Message name	Title	Severity
MSSQL_LOGIN_AUDIT_LEVEL	Inadequate login audit level	Yellow

To protect your computers

- Set the check's Audit level value to 2 or greater then monitor login logs for suspicious login patterns.

C2-level auditing

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

C2 audit mode is an advanced server configuration option that you can enable using sp_configure.

Table 3-11 lists the C2-level auditing message.

Table 3-11 C2-level auditing message

Message name	Title	Severity
MSSQL_C2_LEVEL_AUDITING	C2-level auditing not enabled	Yellow

To protect your computers

- Enable this check if your company policy requires C2-level security.

Server error log maximum

This check reports 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 the Server error log maximum 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.

Table 3-12 lists the Server error log maximum message.

Table 3-12 Server error log maximum message

Message name	Title	Severity
MSSQL_MAX_ERROR_LOG_FILES	Error log maximum too low	Yellow

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.

Database recovery mode

This check reports SQL Server databases that are not configured to use the specified recovery mode.

To configure the Database recovery mode check

- In the Recovery mode text box, type one of the following numeric values:

  1 Simple - Allows database recovery to the point of the last backup.

  2 Bulk_Logged - Allows for complete database recovery while consuming less space than Full.

  3 Full - Provides the least risk of losing data but can result in large transaction log files.

  The default value is 1.

Use the name list to include or exclude databases from this check.

Table 3-13 lists the Database recovery mode message.

Table 3-13 Database recovery mode message

Message name	Title	Severity
MSSQL_RECOVERY_MODE	Database recovery mode	Yellow

To protect your computers

- Select an adequate recovery mode to restore data to an acceptable level in the event of data loss.

SQL Server Configuration

Checks in this module report 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 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 SQL server endpoints that the SQL Server Database Engine communicates with an application

Servers to check

Use the name list to include or exclude servers for all SQL Server Configuration security checks.

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

Started SQL Server endpoint (SQL Server 2005)

This check reports started SQL Server 2005 endpoints that the SQL Server Database Engine communicates with an application.

Table 3-15 lists the Started SQL Server endpoint message.

Table 3-14 Started SQL Server endpoint message

Message name	Title	Severity
ESM_MSSQL_SERVER_ENDPOINT	Started SQL Server endpoint	Green-0

Version and product level

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

Table 3-15 lists the Version and product level message.

Table 3-15 Version and product level message

Message name	Title	Severity
MSSQL_VERSION_LEVEL	SQL Server version and product level	Green-0

To protect your computers

- Install the latest service packs on your SQL servers.

Configuration parameters

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

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.

Use the name lists to enable and disable template files.

Note: Only parameters that are accessible through the sp_configure stored procedure can be reported by this check. To report advanced configuration options, set “Show advanced options” to 1.

Table 3-16 lists the Configuration parameters messages.

Table 3-16 Configuration parameters messages

Message name	Title	Severity
MSSQL_MCP_GREEN_LEVEL	Unauthorized configuration parameter (Green)	Green
MSSQL_MCP_YELLOW_LEVEL	Unauthorized configuration parameter (Yellow)	Yellow
MSSQL_MCP_RED_LEVEL	Unauthorized configuration parameter (Red)	Red
MSSQL_MCP_NOT_FOUND	Configuration parameter not found	Yellow

To protect your computers

- Make sure SQL servers are configured in accordance with your company's security policy.

Editing the SQL Server Configuration Parameters template

To ensure that Symantec can update this template in response to future security threats, do not edit mssqlconfig.scp directly. Instead, create a new SQL Server Configuration Parameters template to add unauthorized parameters that are specific to your environment.

To create a new SQL Server Configuration Parameters template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, click **SQL Server Configuration Parameters - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .scp extension.

To specify parameters for the SQL Server Configuration Parameters template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Configuration Parameters template.
2. In the Template Editor, click **Add Row**.
3. In the Parameter Name field, replace <NEW> with the name of the parameter.
4. In the Comment field, replace <NEW> with explanatory or descriptive information.
5. In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

6 In the Severity field, select one of the following severity levels (initially Green) to be reported when the parameter value is violated:
   - Green
   - Yellow
   - Red

7 Do one of the following:
   - To examine runtime values, leave the Run Value check box checked.
   - To exclude runtime values, uncheck the Run Value check box.

8 Do one of the following:
   - To examine configured values, leave the Config Value check box checked.
   - To exclude configured values, uncheck the Config Value check box.

9 In the Parameter Values field, specify parameter values.
See "To edit the Parameter Values field" on page 49.

10 Click **Save**.

11 To add another parameter, repeat steps 2 to 10.

12 Click **Close**.

To edit the Parameter Values field

1 If the Template Editor is not already open, in the console tree, double-click the SQL Server Configuration Parameters template.

2 In the Template Editor, click the Parameters Values field (initially 0).

3 In the Template Sublist Editor, click **Add Row**.

4 Do one of the following:
   - To designate the value as prohibited, leave the Prohibited check box checked.
   - To designate the value as acceptable, uncheck the Prohibited check box.

5 In the Value field, replace <NEW> with a parameter value that is expressed as a regular expression or as a numeric comparison.
If the value begins with one of the following operators, a numeric comparison is performed:

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

6 Click **Apply**.

7 To add another parameter value, repeat steps 3 to 6.

8 Click **Close**.

Ad hoc queries

This check reports servers that are configured to process ad hoc queries. Malicious users could use ad hoc queries to gain unauthorized access to data.

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.

Use the name list to include or exclude data providers for the check.

Table 3-17 lists the Ad hoc queries message.

Table 3-17 Ad hoc queries message

Message name	Title	Severity
MSSQL_ADHOC_ENABLED	Ad hoc queries enabled	Red

To protect your computers

- Prohibit ad hoc access for each data provider unless required.

SQL Server service account

This check reports unauthorized SQL Server service accounts.

Use the name list to specify 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:

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.

Table 3-18 lists the SQL Server service account message.

Table 3-18 SQL Server service account message

Message name	Title	Severity
MSSQL_SERVER_SERVICE_ACCOUNT	Unauthorized SQL Server service account	Yellow

To protect your computers

- Use a low-privilege account for the SQL Server service instead of using LocalSystem or Administrator.

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:

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.

Table 3-19 lists the SQL Agent service account message.

Table 3-19 SQL Agent service account message

Message name	Title	Severity
MSSQL_AGENT_SERVICE_ACCOUNT	Unauthorized SQL Agent service account	Yellow

To protect your computers

- Use a low-privilege account for the SQL Agent service instead of using LocalSystem or Administrator.

Microsoft Distributed Transaction Coordinator auto start

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

Table 3-20 lists the MSDTC auto start message.

Table 3-20 MSDTC auto start message

Message name	Title	Severity
MSSQL_MSDTC_AUTO_START	MSDTC starts automatically	Yellow

To protect your computers

- If the MSDTC service is not required to start automatically, disable it or start it manually as needed.

SQL Agent auto start

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

Table 3-21 lists the SQL Agent auto start message.

Table 3-21 SQL Agent auto start message

Message name	Title	Severity
MSSQL_SQLAGENT_AUTO_START	SQL Agent starts automatically	Yellow

To protect your computers

- If SQL Agent is not required to start automatically, disable it or start it manually as needed.

SQL Mail enabled

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

Table 3-22 lists the SQL Mail enabled message.

Table 3-22 SQL Mail enabled message

Message name	Title	Severity
MSSQL_SQLMAIL_ENABLED	SQL Mail enabled	Yellow

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 MSSQL Server 2005 (64-bit).

Default login ID

This check reports unauthorized default server login IDs for users of trusted connections that do not have a matching login 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.

Table 3-23 lists the Default login ID message.

Table 3-23 Default login ID message

Message name	Title	Severity
MSSQL_DEFAULT_LOGIN	Unauthorized default login	Yellow

To protect your computers

- Change unauthorized login IDs in the registry location HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\<instance>\DefaultLogin.

Broadcast servers

This check reports SQL servers broadcasting on the network.

Use the name list to include or exclude servers for this security check.

Table 3-24 lists the Broadcast servers message.

Table 3-24 Broadcast servers message

Message name	Title	Severity
MSSQL_BROADCAST_SERVER	The server is broadcasting on the network.	Green

SQL Server installed on domain controller

This check reports 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.

Table 3-25 lists the SQL Server installed on domain controller message.

Table 3-25 SQL Server installed on domain controller message

Message name	Title	Severity
MSSQL_SERVER_ON_DC	SQL Server installed on domain controller	Yellow

To protect your computers

- Never install Microsoft SQL Server on a domain controller.

SQL Sever path

This check reports SQL servers that are not installed on an authorized path.

Use the name list to specify authorized paths. The %instancepath% keyword represents the default installation path for named instances (i.e., MSSQL$Instance_name).

Table 3-26 lists the SQL Server path message.

Table 3-26 SQL Server path message

Message name	Title	Severity
MSSQL_SERVER_PATH	SQL Server on unauthorized path	Yellow

To protect your computer

- Install SQL servers in secure and authorized locations.

SQL Server login rights

This check reports 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 (e.g., %domainname%\username1).

Table 3-27 lists the SQL Server login rights message.

Table 3-27 SQL Server login rights message

Message name	Title	Severity
MSSQL_SERVER_LOGIN_RIGHT	SQL Server login permits server access	Red

To protect your computer

- Review logins to make sure they are authorized and deny server access to unauthorized logins using the login properties setting in the SQL Server Enterprise Manager.

MSSQL Server Agent Proxy Account

The MSSQL Server Agent Proxy Account check reports the MSSQL Server agent proxy accounts.

Table 3-28 lists the MSSQL Server Agent Proxy Account message.

Table 3-28 MSSQL Server Agent Proxy Account message

Message name	Title	Severity
ESM_MSSQL_NO_PROXY_ACCOUNT	MSSQL Server Agent Proxy Account not configured	Yellow
ESM_MSSQL_PROXY_ACCOUNT_2005	MSSQL Server Agent Proxy Account 2005	Green
ESM_MSSQL_PROXY_ACCOUNT_2000	MSSQL Server Agent Proxy Account 2000	Green

SQL Server Objects

Checks in this module report the following information:

- 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
- 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 server after the last snapshot update
- Created databases that were deleted from the server after the last snapshot update
- Roles and users with granted statement permissions that were added to the server after the last snapshot update.
- Roles and users with granted statement permissions that were deleted from the server after the last snapshot update.
- Roles and users with granted object permissions that were added to the server after the last snapshot update
- Roles and users with granted object permissions that were deleted from the server after the last snapshot update

Servers to check

Use the name list to include or exclude servers for all SQL Server Objects security checks.

By default, all 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.

Table 3-29 lists the Database configuration message.

Table 3-29 Database configuration message

	Title	Severity
MSSQL_MDP	Unauthorized database configuration parameter	Yellow

Editing the SQL Server Database Configuration Parameters template

To ensure that Symantec can update this template in response to future security threats, do not edit mssqldatabase.mdp directly. Instead, create a new SQL Server Database Configuration Parameters template to add unauthorized parameters that are specific to your environment.

To create a new SQL Server Database Configuration Parameters template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, click **SQL Server Database Configuration Parameters - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .mdp extension.

To specify parameters for the SQL Server Database Configuration Parameters template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Database Configuration Parameters template.
2. In the Template Editor, click **Add Row**.
3. In the Database Name field, replace <NEW> with the database name.
   If you type the + character in the Database Name field, the parameters in this row are applied to all databases except those databases that are specified in other rows of this template.
4. In the Comment field, replace <NEW> with explanatory or descriptive information.

5 In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

6 In the Permission Control List field, specify database configuration values.
See "To edit the Permission Control List field" on page 60.

7 Click **Save**.

8 To add another database, repeat steps 2 to 7.

9 Click **Close**.

To edit the Permission Control List field

1 If the Template Editor is not already open, in the console tree, double-click the SQL Server Database Configuration Parameters template.

2 In the Template Editor, click the Permission Control List field (initially **0**).

3 In the Template Sublist Editor, click **Add Row**.

4 Do one of the following:

- To designate the value as prohibited, check Prohibited.
- To designate the value as acceptable, uncheck Prohibited.

5 Click the Option or Property field, and then select one of the listed database properties.

6 In the Value field, replace <NEW> with a parameter value that is expressed as a regular expression or numeric comparison.
If the value begins with one of the following operators, a numeric comparison is performed:

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

>=	greater than or equal to

7 In the Comment field, replace <NEW> with explanatory or descriptive information.

8 Click **Apply**.

9 To add another permission entry, repeat steps 3 to 8.

10 Click **Close**.

Guest access to databases

This check reports SQL Server databases that allow guest user access.

Use the name list to include or exclude databases for the check.

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

Table 3-30 lists the Guest access to databases message.

Table 3-30 Guest access to databases message

Message name	Title	Severity
MSSQL_GUEST_ACCESS	Guest access to database	Yellow

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.

Sample databases

This check reports SQL servers that have Northwind and pubs sample databases. These databases are created by default at installation and should be removed from production servers.

Use the name list to include or exclude the names of other databases.

Table 3-31 lists the Sample databases message.

Table 3-31 Sample databases message

Message name	Title	Severity
MSSQL_SAMPLE_DATABASE	Sample database	Yellow

To protect your computers

- Remove sample Northwind and pubs databases from production servers.

Job permissions

This check reports 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

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 hostile user or intruder could create a procedure to continually submit an unlimited number of jobs and execute them at any time.

Use the name list to include or exclude users or roles for this check.

Table 3-32 lists the Job permissions message.

Table 3-32 Job permissions message

Message name	Title	Severity
MSSQL_JOB_PERMISSION	Unauthorized Job permission	Yellow

To protect your computers

- Revoke the execute permission from unauthorized users or roles for the job-related stored procedures.

Stored procedure permissions

This check reports unauthorized stored procedure permissions as specified in enabled SQL Server Database Stored Procedure Permissions templates.

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 Microsoft 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.

Use the name lists to enable and disable template files.

Table 3-33 lists the Stored procedure permissions message.

Table 3-33 Stored procedure permissions message

Message name	Title	Severity
MSSQL_MPP	Unauthorized stored procedure permission	Yellow
MSSQL_MPP_MANDATORY	Mandatory stored procedure permission	Red

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.

Editing the SQL Server Stored Procedure Permissions template

To ensure that Symantec can update this template in response to future security threats, do not edit mssqlstoredprocedure.mpp directly. Instead, create a new SQL Server Database Stored Procedure Permissions template to add unauthorized parameters that are specific to your environment.

To create a new SQL Server Stored Procedure Permissions template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, click **SQL Server Stored Procedure Permissions - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .mpp extension.

To specify parameters for the SQL Server Stored Procedure Permissions template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Stored Procedure Permissions template.
2. In the Template Editor, click **Add Row**.
3. In the Database Name field, replace <NEW> with the database name.

If you type the + character in the Database Name field, the parameters in this row are applied to all databases except those that are specified in other rows of this template.

4 In the Stored Procedure field, replace <NEW> with the stored procedure name.

5 In the Owner field, replace <NEW> with the object owner name.

6 In the Comment field, replace <NEW> with explanatory or descriptive information.

7 In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

8 In the Permission Control List field, specify the stored procedure permission values.
See "To edit the Permission Control List field" on page 64.

9 Click **Save**.

10 To add another stored procedure, repeat steps 2 to 8.

11 Click **Close**.

To edit the Permission Control List field

1 If the Template Editor is not already open, in the console tree, double-click the SQL Server Stored Procedure Permissions template.

2 In the Template Editor, click the Permission Control List field (initially 0).
When the Permission Control List field is empty (set to 0), this check reports all permissions that are associated with the stored procedure that is specified in this template entry.

3 In the Template Sublist Editor, click **Add Row**.

4 In the Required field, select one of the following options:

Prohibited	The permission defined in this template row must not exist. If it does, a Symantec ESM message is triggered.

Mandatory	The permission defined in this template row must exist. If it does not, a Symantec ESM message is triggered.
Allowed	The permission defined in this template row is allowed. All other permissions trigger a Symantec ESM message.

5 In the User or Role field, replace <NEW> with the user name or role name to which you want to grant or deny the execute permission.
Wildcard characters can be used in this field.

6 The Action field defaults to a single option, Execute, and can be left as is.

7 Click on the Protect Type field, and then select one of the following options:

- Deny
- Grant
- Grant_WGO (also known as GRANT_WITH_GRANT option)
  When given Grant_WGO, the grantee is given the ability to grant the specified permissions to another user or role.

8 In the Comment field, replace <NEW> with explanatory or descriptive information.

9 Click **Apply**.

10 To add another permissions entry, repeat steps 3 to 9.

11 Click **Close**.

Statement permissions

This check reports unauthorized statement permissions as specified in enabled SQL Server Statement Permissions templates.

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.

Use the name lists to enable and disable template files.

Table 3-34 lists the Statement permissions messages.

Table 3-34 Statement permissions messages

Message name	Title	Severity
MSSQL_MSP	Unauthorized statement permission	Yellow
MSSQL_MSP_MANDATORY	Mandatory statement permission	Red

To protect your computers

- Periodically review granted statement permissions and revoke unauthorized permissions.

Editing the SQL Server Statement Permissions template

To ensure that Symantec can update this template in response to future security threats, do not edit mssqlstatementpermission.msp directly. Instead, create a new SQL Server Statement Permissions template to add unauthorized parameters that are specific to your environment.

To create a new SQL Server Statement Permissions template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, click **SQL Server Statement Permissions - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .msp extension.

To specify parameters for the SQL Server Statement Permissions template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Statement Permissions template.
2. In the Template Editor, click **Add Row**.
3. In the Database Name field, replace <NEW> with the database name.
   If you type the + character in the Database Name field, the parameters in this row are applied to all databases except those that are specified in other rows of this template.
4. In the Comment field, replace <NEW> with explanatory or descriptive information.
5. In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

6 In the Permission Control List field, specify statement permission values.
See "To edit the Permission Control List field" on page 67.

7 Click **Save**.

8 To add another database, repeat steps 2 to 7.

9 Click **Close**.

To edit the Permission Control List field

1 If the Template Editor is not already open, in the console tree, double-click the SQL Server Statement Permissions template.

2 In the Template Editor, click the Permission Control List field (initially 0).
When the Permission Control List field is empty (set to 0), this check reports all permissions that are associated with the statement that is specified in this template entry.

3 In the Template Sublist Editor, click **Add Row**.

4 Click on the Required field, and then select one of the following options:

Prohibited	The permission defined in this template row must not exist. If it does, a Symantec ESM message is triggered.
Mandatory	The permission defined in this template row must exist. If it does not, a Symantec ESM message is triggered.
Allowed	The permission defined in this template row is allowed. All other permissions trigger a Symantec ESM message.

5 In the User or Role field, replace <NEW> with the appropriate user name or role name.
Wildcard characters can be used in this field.

6 In the Statement field, select one of the following options:

- Backup DB
- Backup Log
- Create DB
- Create Default
- Create Function

- Create SP (system procedure)
- Create Rule
- Create Table
- Create View

7 In the Protect Type field, select one of the following options:

- Deny
- Grant

8 In the Comment field, replace <NEW> with explanatory or descriptive information.

9 Click **Apply**.

10 To add another statement permission, repeat steps 3 to 9.

11 Click **Close**.

Object permissions

This check reports unauthorized object permissions as specified in enabled SQL Server Object Permissions templates.

You can use SQL Server Object Permissions templates to report on the permissions of system tables, user tables, views, table functions, and inline table-valued 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 template file must be enabled for this check to work successfully.

Use the name lists to enable and disable template files.

Table 3-35 lists the Object permissions message.

Table 3-35 Object permissions message

Message name	Title	Severity
MSSQL_MOP	Unauthorized object permission	Yellow
MSSQL_MOP_MANDATORY	Mandatory object permission	Red

To protect your computers

- Periodically review granted object permissions and revoke unauthorized permissions.

Editing the SQL Server Object Permissions template

To ensure that Symantec can update this template in response to future security threats, do not edit mssqlobjectpermission.mop directly. Instead, create a new SQL Server Object Permissions template to add unauthorized parameters that are specific to your environment.

To create a new SQL Server Object Permissions template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, select **SQL Server Object Permissions - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .mop extension.

To specify parameters for the SQL Server Object Permissions template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Object Permissions template.
2. In the Template Editor, click **Add Row**.
3. In the Database Name field, replace <NEW> with the database name.
   If you type the + character in the Database Name field, the parameters in this row are applied to all databases except those that are specified in other rows of this template.
4. In the Object field, replace <NEW> with the SQL object name.
5. In the Owner field, replace <NEW> with the object owner name.
6. In the Comment field, replace <NEW> with explanatory or descriptive information.
7. In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

8 In the Permission Control List field, specify object permission values.
See "To edit the Permission Control List field" on page 70.

9 Click **Save**.

10 To add another object, repeat steps 2 to 9.

11 Click **Close**.

To edit the Permission Control List field

1 If the Template Editor is not already open, in the console tree, double-click the SQL Server Object Permissions template.

2 In the Template Editor, click the Permission Control List field (initially 0). When the Permission Control List field is empty (i.e., set to 0), this check reports all permissions that are associated with the object that is specified in this template entry.

3 In the Template Sublist Editor, click **Add Row**.

4 In the Required field, select one of the following options:

Prohibited	The permission defined in this template row must not exist. If it does, a Symantec ESM message is triggered.
Mandatory	The permission defined in this template row must exist. If it does not, a Symantec ESM message is triggered.
Allowed	The permission defined in this template row is allowed. All other permissions trigger a Symantec ESM message.

5 In the User or Role field, replace <NEW> with the user name or role name. Wildcard characters can be used in this field.

6 In the Action field, select one of the following options:

- Select
- Insert
- Delete
- Update
- References

7 In the Protect Type field, select one of the following options:

- Deny
- Grant
- Grant_WGO (also known as GRANT_WITH_GRANT option)
  When given Grant_WGO, the grantee is given the ability to grant the specified permissions to another user or role.

8 In the Column field, replace <NEW> with one of the following values:

All	All current object columns
New	Any new columns that might be altered (by using the ALTER statement) on the object in the future
All+New	All current columns of the object and any new columns that might be altered (by using the ALTER statement) on the object in the future
any valid table column name	All specified, valid column names Separate listed column names with commas (,).
Empty	All object columns

9 In the Comment field, replace <NEW> with explanatory or descriptive information.

10 Click **Apply**.

11 To add another permission entry, repeat steps 3 to 10.

12 Click **Close**.

Database names

Use the name list to include or exclude databases for the object and statement permissions checks.

Object permission names

Use the name list to include or exclude permissions for grant and directly granted object permissions checks. Valid entries include Select, Insert, Update, Delete, and Execute.

Object names

Use the name list to include or exclude object names for grant and directly granted object permissions checks.

Object permission grantors

Use the name list to include or exclude grantors for grant with grant and directly granted object permissions checks.

Directly granted object permissions

This check reports roles and users that have directly granted object permissions.

Use the name list to include or exclude grantees for the check. Use the keyword %users% to specify all users in the database. Use the keyword %roles% to specify all roles in the database.

Table 3-36 lists the Directly granted permissions message.

Table 3-36 Directly granted permissions message

Message name	Title	Severity
MSSQL_OBJ_DIR_GRANT	Directly granted object permission	Yellow

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.

Grant with grant object permissions

This check reports roles and users that have grant with grant object permissions.

Use the name list to include or exclude grantees for the check. Use the keyword %users% to specify all users in the database. Use the keyword %roles% to specify all roles in the database.

Table 3-37 lists the Grant with grant object permissions message.

Table 3-37 Grant with grant object permissions message

Message name	Title	Severity
MSSQL_OBJ_GRANT_GRANT	Grant with grant object permission	Yellow

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.

Statement permission names

Use the name list to include or exclude statement permissions for directly granted statement permission checks.

Valid entries include the following names:

- Backup Database
- Backup Log
- Create Database
- Create Default
- Create Function
- Create Procedure
- Create Rule
- Create Table
- Create View

Statement permission grantors

Use the name list to include or exclude grantors for directly granted statement permission checks.

Directly granted statement permissions

This check reports roles and users that have directly granted statement permissions.

Use the name list to include or exclude grantees for the check. Use the keyword %users% to specify all users in the database. Use the keyword %roles% to specify all roles in the database.

Table 3-38 lists the Directly granted statement permissions message.

Table 3-38 Directly granted statement permissions message

Message name	Title	Severity
MSSQL_STA_DIR_GRANT	Directly granted statement permission	Yellow

Module EXECUTE AS clause (SQL Server 2005)

This check reports modules that have an EXECUTE AS clause set to a value other than CALLER, the default setting. 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 required by objects referenced by the running module. Use the name list to include or exclude EXECUTE AS clause names in the check. Use the Database names name list to include or exclude databases in the check.

Table 3-39 lists the Module EXECUTE AS clause message.

Table 3-39 Module EXECUTE AS clause message

Message name	Title	Severity
ESM_MSSQL_MODULE_EXECUTE_AS	Module EXECUTE AS clause	Yellow-2

Database names

Use this option's name list to include or exclude databases in the Module EXECUTE AS clause check.

Database status

This check reports information about created databases. Use the name list to include or exclude database names in this check.

Table 3-40 lists the Database status message.

Table 3-40 Database status message

Message name	Title	Severity
ESM_MSSQL_DATABASE	Database status	Yellow-2

New databases

This check reports information about created databases that were added to the server after the last snapshot update. Use the name list to include or exclude database names in this check.

Table 3-41 lists the New databases message.

Table 3-41 New databases message

Message name	Title	Severity
ESM_MSSQL_NEW_DATABASE	New database	Yellow-2

Deleted databases

This check reports information about databases that were deleted from the server after the last snapshot update. Use the name list to include or exclude database names in this check.

Table 3-42 lists the Deleted databases message.

Table 3-42 Deleted databases message

Message name	Title	Severity
ESM_MSSQL_DELETED_DATABASE	Deleted database	Yellow-2

New granted statement permissions

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

Table 3-43 lists the New granted statement permissions message.

Table 3-43 New granted statement permissions message

Message name	Title	Severity
ESM_MSSQL_NEW_ STATEMENT_PERM	New statement permission	Yellow-2

Deleted granted statement permissions

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

Table 3-44 lists the Deleted granted statement permissions message.

Table 3-44 Deleted granted statement permissions message

Message name	Title	Severity
ESM_MSSQL_DELETED_ STATEMENT_PERM	Deleted statement permission	Yellow-2

New granted object permissions

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

Table 3-44 lists the New granted object permissions messages.

Table 3-45 New granted object permissions messages

Message name	Title	Severity
ESM_MSSQL_NEW_OBJECT	New object	Yellow-2
ESM_MSSQL_NEW_OBJECT_ PERM	New granted object permission	Yellow-2
ESM_MSSQL_NEW_OBJECT_ PERM_COL	New granted object column permission	Yellow-2

Deleted granted object permissions

This check reports roles and users with granted object permissions that were deleted from the server after the last snapshot update. Use the check's name list to include or exclude grantees in the check. Use the keyword %users% to specify all users in the database. Use the keyword %roles% to specify all roles in the database.

Table 3-46 lists the Deleted granted object permissions messages.

Table 3-46 Deleted granted object permissions messages

Message name	Title	Severity
ESM_MSSQL_DELETED_OBJECT	New object	Yellow-2
ESM_MSSQL_DELETED_OBJECT_PERM	New granted object permission	Yellow-2
ESM_MSSQL_DELETED_OBJECT_PERM_COL	New granted object column permission	Yellow-2

Automatically update snapshots

Enable this option to update snapshots automatically.

SQL Server Password Strength

Checks in this module report 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.

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 "Word files" on page 83.

Servers to check

Use the name list to include or exclude servers for all SQL Server Password Strength checks.

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

Authentication mode

This check reports servers that do not use the specified authentication modes.

To configure the Authentication mode check

- In the Authentication mode text box, type one of the following values:

1	Windows only mode
2	SQL Server and Windows modes

Microsoft recommends Windows only mode for stronger security.

Table 3-47 lists the Authentication mode message.

Table 3-47 Authentication mode message

Message name	Title	Severity
MSSQL_AUTH_MODE	Authentication mode	Yellow

To protect your computers

- Use Windows only authentication mode if SQL Server native authentication is not required.

Empty password

This check reports SQL Server logins with empty or NULL passwords.

Table 3-48 lists the Empty password message.

Table 3-48 Empty password message

Message name	Title	Severity
MSSQL_NULL_PASSWORD	Empty password	Yellow

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.
  See "About secure passwords" on page 78.

Application role password

This check reports 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 application role passwords.

Table 3-49 lists the Application role password messages.

Table 3-49 Application role password messages

Message name	Title	Severity
MSSQL_APP_ROLE_NULL_PASSWORD	Application role empty password	Red
MSSQL_GUESSED_PASSWORD	Guessed password	Yellow

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.
  See "About secure passwords" on page 78.

Password = login name

This check reports logins with matching login names and passwords.

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.

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

Table 3-50 lists the Password = login name message.

Table 3-50 Password = login name message

Message name	Title	Severity
MSSQL_GUESSED_PASSWORD	Guessed password	Yellow

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.
  See "About secure passwords" on page 78.

Password = any login name

This check reports SQL Server logins with passwords that match any login name.

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

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

Table 3-51 lists the Password = any login name message.

Table 3-51 Password = any login name message

Message name	Title	Severity
MSSQL_GUESSED_PASSWORD	Guessed password	Yellow

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.
  See "About secure passwords" on page 78.

Password = wordlist word

This check tries to match passwords with words in enabled word files and reports logins with matches.

Use the name lists to enable or disable word files for the check.

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

Table 3-52 lists the Password = wordlist word message.

Table 3-52 Password = wordlist word message

Message name	Title	Severity
MSSQL_GUESSED_PASSWORD	Guessed password	Yellow

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.
  See "About secure passwords" on page 78.

Word files

The Password = wordlist word check compares passwords to words in dictionary word files (*.wrd files). Passwords that match word file words (and variations of those words) can be easily guessed by intruders and are a security threat.

The SQL Server Password Strength module provides the following word files. The letters D, FR, I, NL, P, and SP are language identifiers for German, French, Italian, Dutch, Portuguese, and Spanish.

Table 3-53 lists the word files that are installed with this product.

Table 3-53 Word files

Category	File	No. of words
First name	firstnam.wrd Fname_D.wrd Fname_FR.wrd Fname_I.wrd Fname_NL.wrd Fname_P.wrd Fname_SP.wrd	651 1602 784 952 724 449 349
Last name	lastnam.wrd Lname_D.wrd Lname_FR.wrd Lname_I.wrd Lname_NL.wrd Lname_P.wrd Lname_SP.wrd	2958 3101 3196 2848 3005 723 3027

Table 3-53 Word files

Category	File	No. of words
Dictionaries	synopsis.wrd	253
	english.wrd	3489
	lenglish.wrd	34886
	Slist_D.wrd	169
	List_D.wrd	2597
	Llist_D.wrd	19319
	Slist_FR.wrd	166
	List_FR.wrd	2517
	Llist_FR.wrd	17893
	Slist_I.wrd	227
	List_I.wrd	2490
	Llist_I.wrd	14814
	Slist_NL.wrd	399
	List_NL.wrd	3038
	Llist_NL.wrd	14232
	Slist_P.wrd	217
	List_P.wrd	2169
	Llist_P.wrd	16950
	Slist_SP.wrd	162
	List_SP.wrd	2424
	Llist_SP.wrd	19580
	yiddish.wrd	639
Computers	computer.wrd	143
	Compu_D.wrd	545
	Compu_FR.wrd	346
	Compu_I.wrd	255
	Compu_NL.wrd	184
	Compu_P.wrd	226
	Compu_SP.wrd	216
	defaults.wrd	465
	nerdnet-defaults.wrd	142
	ntccrack.wrd	16870
	Oracle.wrd	37
	wormlist.wrd	432
Specialty	cartoon.wrd	133
	college.wrd	819
	disney.wrd	433
	hpotter.wrd	715
	python.wrd	3443
	sports.wrd	247
	tolkien.wrd	471
	trek.wrd	876

To enable a word file

1 In the Disabled Word Files list, select a word file.

2 Click the left arrow.

To disable a word file

1 In the Enabled Word files list, select a word file.

2 Click the right arrow.

To edit a word file

1 Do one of the following:

- Open an existing word file in a text editor. (Windows word files are located in \Program Files\Symantec\ESM\Words.)
- Create a new ASCII plain-text word file in a text editor. Name the new file with a .wrd extension (for example, medical.wrd).

2 Type only one word per line.

3 Save the file in the \Words folder.

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 use common names or words in reverse order 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.
  See "About secure passwords" on page 78.

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.
  See "About secure passwords" on page 78.

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.
  See "About secure passwords" on page 78.

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. See "About secure passwords" on page 78.

Suffix

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

Use the name list to specify suffixes 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 suffixes 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.

See "About secure passwords" on page 78.

Monitor password age

This check reports SQL Server login and application role passwords that have not been changed within the period specified in the Maximum days text box. 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.

Table 3-54 lists the Monitor password age message.

Table 3-54 Monitor password age message

Message name	Title	Severity
MSSQL_PASSWORD_NOT_CHANGED	Password not changed	Yellow

To protect your computers

- Require users to change login and application role passwords at least every sixty days.

Password policy enforcement (SQL Server 2005)

This check reports SQL Server 2005 logins that do not have the password policy enforced. Use the name list to include or exclude login names from this check.

Table 3-55 lists the Password policy enforcement message.

Table 3-55 Password policy enforcement message

Message name	Title	Severity
MSSQL_PASSWORD_POLICY	Password policy not enforced	Yellow-2

Password expiration enforcement (SQL Server 2005)

This check reports SQL Server 2005 logins that do not have the password expiration enforced. Use the name list to include or exclude login names from this check.

Table 3-56 lists the Password expiration enforcement message.

Table 3-56 Password expiration enforcement message

Message name	Title	Severity
MSSQL_PASSWORD_EXPIRATION	Password expiration not enforced	Yellow-2

SQL Server Roles

Checks in this module report the following information:

- 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

Servers to check

Use the name list to include or exclude servers for all SQL Server Roles security checks.

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

Fixed-server role members

This check reports unauthorized members of the fixed-server roles as specified in enabled SQL Server Fixed-Server Role Member templates.

Use the name lists to enable and disable template files.

Table 3-57 lists the Fixed-server role members message.

Table 3-57 Fixed-server role members message

Message name	Title	Severity
MSSQL_FIXED_SERVER_ROLE_MEM	Unauthorized member of fixed-server role	Yellow

To protect your computers

- Review members of fixed-server roles often and drop unauthorized users from role memberships.

Editing the SQL Server Fixed-Server Role Member template

You must create at least one SQL Server Fixed-Server Role Member template and enable it, for this check to successfully report unauthorized fixed-server role members.

To create a new SQL Server Fixed-Server Role Member template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, select **SQL Server Fixed-Server Role Member - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .msr extension.

To specify roles for the SQL Server Fixed-Server Role Member template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Fixed-Server Role Member template.
2. In the Template Editor, click **Add Row**.
3. In the Role Name field, replace <NEW> with the role name.
4. In the Comment field, replace <NEW> with explanatory or descriptive information.
5. In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

6. In the Role Member List field, specify prohibited and allowed role members.
   See "To edit the Role Member List field" on page 92.
7. Click **Save**.
8. To add another role, repeat steps 2 to 7.
9. Click **Close**.

To edit the Role Member List field

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Fixed-Server Role Member template.
2. In the Template Editor, click the Role Member List field (initially 0).
   When the Role Member List field is empty (set to 0), this check reports all members that are assigned to the fixed-server role that are specified in this template entry.
3. In the Template Sublist Editor, click **Add Row**.
4. Do one of the following:
   - To designate the member as prohibited, check Prohibited.
   - To designate the member as allowed, uncheck Prohibited.
5. In the Member field, replace <NEW> with the name of an allowed or prohibited role member.
   Wildcard characters can be used in this field.
6. Click **Apply**.
7. To add another role member, repeat steps 3 to 6.
8. Click **Close**.

Note: If only prohibited members are specified in the Member field, then all other members are treated as allowed. If only allowed members are specified, then all other members are treated as prohibited. If both prohibited and allowed members are specified, all other members are treated as prohibited.

Database role members

This check reports unauthorized members of fixed and user-defined database roles as specified in enabled SQL Server Database Role Member templates.

Use the name lists to enable and disable template files.

Table 3-58 lists the Database roles message.

Table 3-58 Database roles message

Message name	Title	Severity
MSSQL_DATABASE_ROLE_MEM	Unauthorized member of database role	Yellow

To protect your computers

- Review members of fixed and user-defined roles often and drop unauthorized users from role memberships.

Editing the SQL Server Database Role Member template

You must create at least one SQL Server Database Role Member template, and enable it, for this check to report unauthorized fixed-server role members successfully.

To create a new SQL Server Database Role Member template

1. In the console tree, right-click **Templates**, and then click **New**.
2. In the Create New Template dialog box, select **SQL Server Database Role Member - all**.
3. Type a new template name without an extension.
4. Press **Enter**.
   Symantec ESM automatically adds the .mdr extension.

To specify roles for the SQL Server Database Role Member template

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Database Role Member template.
2. In the Template Editor, click **Add Row**.
3. In the Database Name field, replace <NEW> with the database name.
4. In the Role Name field, replace <NEW> with the role name.
5. In the Comment field, replace <NEW> with explanatory or descriptive information.
6. In the SQL Version field, replace <NEW> with one of the following values:

Value	Description
Empty	All version numbers
8.00	8.00.x
8	8.x
+8	8.x and later

7. In the Role Member List field, specify prohibited and allowed members of the role.
   See "To edit the Role Member List field" on page 62.
8. Click **Save**.
9. To add another role, repeat steps 2 to 8.
10. Click **Close**.

To edit the Role Member List field

1. If the Template Editor is not already open, in the console tree, double-click the SQL Server Database Role Member template.
2. In the Template Editor, click the Role Member List field (initially 0).
   When the Role Member List field is empty (set to 0), this check reports all members that are assigned with the database role that is specified in this template entry.
3. In the Template Sublist Editor, click **Add Row**.

4 Do one of the following:
   - To designate the member as prohibited, check Prohibited.
   - To designate the member as allowed, uncheck Prohibited.

5 In the Member field, replace <NEW> with the name of an allowed or prohibited role member.
   Wildcard characters can be used in this field.

6 Click **Apply**.

7 To add another role member, repeat steps 3 to 6.

8 Click **Close**.

Note: If only prohibited members are specified in the Member field, then all other members are treated as allowed. If only allowed members are specified, then all other members are treated as prohibited. If both prohibited and allowed members are specified, all other members are treated as prohibited.

Databases - Application roles

Use the name list to include or exclude databases for the Application roles check.

By default, all databases on each server that is specified in the Servers to check option are included. See "Servers to check" on page 58.

Application roles

This check reports unauthorized application roles for each database.

Use the name list to include (accept) or exclude (prohibit) roles. Leave the list empty to prohibit all application roles.

Table 3-59 lists the Application roles message.

Table 3-59 Application roles message

Message name	Title	Severity
MSSQL_APP_ROLE	Unauthorized application role	Yellow

To protect your computers

- Periodically review and drop unauthorized application roles from the database.

Databases - Nested roles

Use the name list to include or exclude databases for this check.

By default, all databases on each server that is specified in the Servers to check option are included. See "Servers to check" on page 58.

Nested roles

This check reports nested roles for each database.

Use the name list to include or exclude roles for this check. Leave the list empty to prohibit all application roles.

Table 3-60 lists the Nested roles message.

Table 3-60 Nested roles message

Message name	Title	Severity
MSSQL_NESTED_ROLE	Unauthorized nested role	Yellow

To protect your computers

- Periodically review and drop unauthorized nested roles from the database.

Databases - Users without roles

Use the name list to include or exclude databases for the Users without roles check.

Users without roles

This check reports users that are not assigned to a database role other than the public role.

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

Use the name list to include or exclude users for this check.

Table 3-61 lists the Users without roles message.

Table 3-61 Users without roles message

Message name	Title	Severity
MSSQL_USER_WITHOUT_ROLE	Users not assigned to a role	Yellow

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.

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 fixed-server role names from this check.

Table 3-62 lists the New fixed server role and member messages.

Table 3-62 New fixed server role and member messages

Message name	Title	Severity
ESM_MSSQL_NEW_SERVER_ROLE	New fixed server role	Yellow-2
ESM_MSSQL_NEW_SERVER_ROLE_MEMBER	New fixed server role member	Yellow-2

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.

Table 3-63 lists the Deleted fixed server role and member messages.

Table 3-63 Deleted fixed server role and member messages

Message name	Title	Severity
ESM_MSSQL_DELETED_SERVER_ROLE	Deleted fixed server role	Yellow-2
ESM_MSSQL_DELETED_SERVER_ROLE_MEMBER	Deleted fixed server role	Yellow-2

Database - Roles

Use the name list in this option to include or exclude the databases for the new and deleted database roles checks.

New database role and member

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

Table 3-64 lists the New database role and member messages.

Table 3-64 New database role and member messages

Message name	Title	Severity
ESM_MSSQL_NEW_DATABASE_ROLE	New database role	Yellow-2
ESM_MSSQL_NEW_DATABASE_ROLE_MEMBER	New database role member	Yellow-2

Deleted database role and member

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

Table 3-64 lists the Deleted database role and member messages.

Table 3-65 Deleted database role and member messages

Message name	Title	Severity
ESM_MSSQL_DELETED_DATABASE_ROLE	Deleted database role	Yellow-2

Table 3-65 Deleted database role and member messages

Message name	Title	Severity
ESM_MSSQL_DELETED_DATABASE_ROLE_MEMBER	Deleted database role member	Yellow-2

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.

For more information, see Minimum account privileges.

Chapter 5

Frequently asked questions

This chapter includes the following topics:

- Deploying ESM Modules for MS SQL Servers
- Changing the configuration of an MS SQL Server

This chapter lists certain frequently asked questions pertaining to Symantec ESM Modules for MS SQL Server Databases and their answers.

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 Microsoft SQL Server report on Microsoft SQL Server 32-bit and 64-bit databases.

Host-based deployment

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

See "Configuring the ESM modules for MS SQL Server Databases" on page 34.

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 a MSSQL Server whose password has been changed, do either of the following:
  - Remove the configuration record of that MSSQL Server and add it again silently.
  - Modify the configuration record of that MSSQL Server by using the -m option with MSSQLSetup.exe interactively.