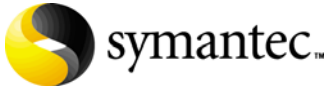
Symantec Enterprise Security Manager™ Modules for MySQL Databases User's Guide

Release 4.0 for Symantec ESM 6.0, 6.1, 6.5.x, and 9.0

For Red Hat Enterprise Linux

MySQL 4.0, 4.1, and 5.0



Symantec ESM Modules for MySQL Databases User's Guide

Release 4.0

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

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Technical support

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

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing Symantec ESM Modules for MySQL Databases

This chapter includes the following topics:

About Symantec ESM Modules for MySQL Databases

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

Working within the framework of Symantec ESM, the industry's most comprehensive solution for discovering security vulnerabilities, Symantec ESM Modules for MySQL Databases eases the administrative burden of measuring the effectiveness of enterprise security policies and enforcing compliance. This product installs on Red Hat Enterprise Linux ES 3/4/5.

Components of Symantec ESM Modules for MySQL Databases

When you install Symantec ESM Modules for MySQL Databases, five modules and one template file 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 MySQL Password module includes checks that report logons 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 MySQL Databases installs the following modules:

MySQL Accounts

Checks in this module report MySQL databases 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 "MySQL Accounts" on page 28.

MySQL Configuration

Checks in this module report MySQL version information, configuration parameters that are specified in a template, MySQL daemon owner, status of the logs, and information about the socket file. See "MySQL Configuration" on page 30.

MySQL Databases

Checks in this module report the default, sample, new, and deleted databases on the MySQL server. See "MySQL Databases" on page 32.

MySQL Passwords

Checks in this module report logons with empty passwords and easily guessed passwords. See "MySQL Passwords" on page 34.

MySQL Privileges

Checks in this module report the MySQL database accounts with privileges such as GLOBAL, SUPER, FILE, SHUTDOWN, and GRANT. The checks in this module ensure that privileges are assigned only to authorized users. The checks also report unauthorized changes in the privileges and their misuse. See "MySQL Privileges" on page 43.

Templates

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

Table 1-1 shows the modules and checks that use template files in Symantec ESM Modules for MySQL Server Databases.

Table 1-1 Template files

Module	Check name	Template name	Predefined template
MySQL Configuration	Configuration parameters	MySQL Configuration Watch	-
File Attributes	Template files	New File - Linux	mysql.li

Creating the MySQL Configuration Watch template

The MySQL Configuration Watch template needs to be created with the following fields:

Description	Describes the database parameter
Parameter	Specifies the parameter that is checked. To see the various database parameters, run the following command: `show variables`
Parameter value	Specifies the value of the parameter
Use of value	Specifies if the value is optional, required, or forbidden
Severity	Specifies if the severity of the value is green, yellow, or red
MySQL version	Specify the MySQL version to which the parameter is applicable If you specify a value of 0 (zero), the parameter is applicable to all MySQL versions.

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 the standards that are 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 MySQL Databases

You can use Symantec ESM Modules for MySQL Databases in the same way that you use other Symantec ESM Modules.

- Create a Symantec ESM policy using one or more MySQL 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.

Chapter 2

Installing Symantec ESM Modules for MySQL Server Databases

This chapter includes the following topics:

Before you install

Symantec ESM Modules for MySQL Server Databases can be installed on Red Hat Enterprise Linux ES 3/4 and Red Hat Linux 5. Policies that are created using these server-based modules can run against any MySQL 4.0/4.1/5.0 database.

Before you install Symantec ESM Modules for MySQL Databases, you need to verify the following:

CD-ROM access	At least one computer 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 (SU) 22	ESM SU22 or greater must be installed on the same computer as the Symantec ESM manager.

Minimum account privileges

The logon accounts must have the following privileges to perform ESM security checks on the MySQL databases:

- Read privileges on the MySQL database
- Privilege to execute the command, `SHOW DATABASES`

System requirements

Table 2-1 lists the supported operating systems on which you can install ESM Modules for MySQL, and the operating systems on which these modules can report.

Table 2-1 ESM Modules for MySQL system requirements

Supported operating systems	Architecture	Supported OS versions	Supported MySQL versions
Red Hat Linux	x86, Opteron, EM64T	5.x	5.0
Red Hat Enterprise Linux	x86, Opteron, EM64T	ES 4	4.0, 5.0

Table 2-1 ESM Modules for MySQL system requirements

Supported operating systems	Architecture	Supported OS versions	Supported MySQL versions
Red Hat Enterprise Linux	x86, Opteron, EM64T	ES 3	4.0, 4.1

Installing the ESM Modules for MySQL databases

Symantec ESM Modules for MySQL Databases are stored in an installation package, esmmysql.tpi.

The esmmysql.tpi package 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. Download esmmysql.tpi from the application modules section in the Symantec Security Response Web page : http://www.symantec.com/avcenter/security/Content/Product/Product_ESM.html
2. Run esmmysql.tpi.
3. Select one of the following options:

Option 1	Displays the contents of the package. To install the module, rerun esmmysql.tpi and select option 2.
Option 2	Installs the tune-up or installation package on your system.
Option 3	Quits installation.

   Register template and .m files only one time for the agents that use the same Symantec ESM manager on the same operating system.

4. 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 step .
5. Type the name of the manager to which the agent is registered. Typically, this entry is the name of the computer on which the manager is installed.
6. 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.

7. Type the password that is used to log on to the manager.

8 Type the port that the ESM manager uses. The default port is 5600.

9 Type the name of the agent that is registered to the manager.

10 Do one of the following:

- Type **Y** if the information that you have provided is correct.
  File names are displayed as they are extracted.
- Type **N** if the information is not correct.
  The command line is returned. Enter the correct information again.

11 When the extraction is complete, the setup prompts you want to add configuration records to enable ESM security checking for your MySQL database. Do one of the following:

- Type **Y** to continue the installation and configure the MySQL database for security checks.
  For configuring the MySQL database, see "Configuring the ESM Modules for MySQL databases silently" on page 24.
- Type **N** to end the installation without adding the security checks.

12 Do one of the following:

- Type **Y** to update the report content on the agent, and finish the installation.
- Type **N** to finish the installation.

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

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.

```
[root@localhost linux-x86]# ./esmmysql.tpi
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
  3) Quit
Enter option number [1]: 2
Installing package: Symantec ESM Modules for MySQL Databases 4.0.0
(2007/12/28)
Tuneup pack will overlay Symantec ESM Modules for MySQL Databases
version 3.1.0 with version 4.0.0
This package includes the following templates and/or ".m" files:
File: /esm/register/unix/mysqlacct.m.gz
Description:     ESM MySQL Accounts module. module definition file
File: /esm/register/unix/mysqlcomm.m.gz
Description:     ESM MySQL Common Configuration file. module
definition file
File: /esm/register/unix/mysqlconfig.m.gz
Description: ESM MySQL Configuration module. module definition file
File: /esm/register/unix/mysqldb.m.gz
Description: ESM MySQL Databases module. module definition file
File: /esm/register/unix/mysqlpass.m.gz
Description: ESM MySQL Passwords module. module definition file
File: /esm/register/unix/mysqlpriv.m.gz
Description: ESM MySQL Privileges module. module definition file
File: /esm/register/unix/i18n/mysqlacct.m.gz
Description: ESM MySQL Accounts module. module definition file
File: /esm/register/unix/i18n/mysqlcomm.m.gz
Description: ESM MySQl Common Configuration file. module definition
file
File: /esm/register/unix/i18n/mysqlconfig.m.gz
Description: ESM MySQl Configuration module. module definition file
File: /esm/register/unix/i18n/mysqldb.m.gz
Description: ESM MySQl Databases module . module definition file
```

```
File: /esm/register/unix/i18n/mysqlpass.m.gz

Description: ESM MySQL Passwords module. module definition file

File: /esm/register/unix/i18n/mysqlpriv.m.gz

Description: ESM MySQL Privileges module. module definition file

File: /esm/template/unix/mysql.li.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: 10.218.103.20

ESM access name to log on to the ESM manager [ESM]: esm

Enter the ESM password used to log on to the ESM manager.

Password:

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

Enter the name of the agent as it is registered to the ESM manager
[localhost.localdomain]: 10.216.213.237

ESM Manager   : 10.218.103.20

ESM user name : esm

Protocol      : TCP

Port          : 5600

ESM agent     : 10.216.213.237

Is this information correct? [yes]

Extracting /esm/bin/lnx-x86/mtpkreg.gz...

Extracting /esm/bin/lnx-x86/pushfiles.gz...

Extracting /esm/bin/lnx-x86/mergemanifest.gz...

Extracting /esm/register/unix/mysqlacct.m.gz...

Extracting /esm/register/unix/mysqlcomm.m.gz...

Extracting /esm/register/unix/mysqlconfig.m.gz...

Extracting /esm/register/unix/mysqldb.m.gz...

Extracting /esm/register/unix/mysqlpass.m.gz...

Extracting /esm/register/unix/mysqlpriv.m.gz...

Extracting /esm/register/unix/i18n/mysqlacct.m.gz...

Extracting /esm/register/unix/i18n/mysqlcomm.m.gz...

Extracting /esm/register/unix/i18n/mysqlconfig.m.gz...

Extracting /esm/register/unix/i18n/mysqldb.m.gz...
```

```
Extracting /esm/register/unix/i18n/mysqlpass.m.gz...

Extracting /esm/register/unix/i18n/mysqlpriv.m.gz...

Extracting /esm/config/esmsu-mysql.properties.gz...

Extracting /esm/bin/lnx-x86/mysqlacct.gz...

Extracting /esm/bin/lnx-x86/mysqlconfig.gz...

Extracting /esm/bin/lnx-x86/mysqldb.gz...

Extracting /esm/bin/lnx-x86/mysqlpass.gz...

Extracting /esm/bin/lnx-x86/mysqlpriv.gz...

Extracting /esm/template/unix/mysql.li.gz...

Extracting /esm/bin/lnx-x86/esmmysqlsetup.gz...

Extracting /esm/update/ble/SU_3300/en/UpdatePackage.rdl.gz...

Extracting /tmp/esmthird.gz...

Continue and add configuration records to enable ESM security
checking for your MySQL database? [Y/N] n

This esmmysqlsetup program can be run at later time.

Please note the following usage.

Usage: configure a MySQL instance into Symantec ESM MySQL Modules
Silently

esmmysqlsetup -a -Q -A {ACCOUNT} -P {PASSWORD} -t {PORT} -s {SOCKET
FILE} [-S {INSTANCE}] [-T {SSL KEY}] [-W {CA CERT}] [-V {SSL cert}]

Usage: update a MySQL configuration record from ESM MySQL module

esmmysqlsetup -U {PORT} <switch> {value} <switch> {value}...

e.g. For updating password and ssl key, options are esmmysqlsetup -U
{PORT} -P {PASSWORD} -T {SSL KEY}

Help: esmmysqlsetup [OPTIONS]

-h: Display help

-l: List all MySQL configuration record from ESM MySQL module

-a: Configure a MySQL instance into Symantec ESM MySQL Modules

-d {PORT}: Delete a MySQL configuration record from ESM MySQL module

-d all: Delete all MySQL configuration records from ESM MySQL module

-a -Q: Silent configuration of a MySQL instance into Symantec ESM
MySQL Modules

-U {PORT}: Silent Update of a MySQL instance into Symantec ESM MySQL
Modules

-A {ACCOUNT}: Account to connect to the MySQL Database

-P {PASSWORD}: Password of Account to connect to the MySQL Database

-t {PORT}: Port on which the MySQL Database service is running (Need
to specify only when host in account name is not localhost)
```

```
-s {SOCKET FILE}: Path of Socket file to connect to the MySQL
Database (Need to specify only when host in account name is
localhost)

-S {INSTANCE}: Instance name (If not given,setup will take N/A)

-T {SSL KEY}: SSL client key required to connect to the MySQL
database (If not given, setup will take N/A)

-W {CA CERT}: Ca-cert required to connect to the MySQL database (If
not given,setup will take N/A)

-V {SSL cert}: SSL client cert required to connect to the MySQL
database (If not given, setup will take N/A)

Extracting /esm/config/su/65/manifest.xml.gz...

Re-registering modules/template files... Please wait...

Running "/esm/bin/lnx-x86/mtpkreg" -v -m "10.218.103.20" -N
"10.216.213.237" -p 5600 -t -U "esm" -P "******" -L "ESM_MySQL" -T
mysqlacct.m,mysqlcomm.m,mysqlconfig.m,mysqldb.m,mysqlpass.m,mysqlpr
iv.m... Please wait...

Registering /esm/register/unix/i18n/mysqlacct.m ...

Registering /esm/register/unix/i18n/mysqlcomm.m ...

Registering /esm/register/unix/i18n/mysqlconfig.m ...

Registering /esm/register/unix/i18n/mysqldb.m ...

Registering /esm/register/unix/i18n/mysqlpass.m ...

Registering /esm/register/unix/i18n/mysqlpriv.m ...

checking: MySQL Accounts

checking: MySQL Configuration

checking: MySQL Databases

checking: MySQL Passwords

checking: MySQL Privileges

uploading property file: esm-unix.properties

skipping: file already uploaded ....

uploading property file: esmsu-unix.properties

skipping: file already uploaded ....

uploading property file: esmsu-mysql.properties

skipping: file already uploaded ....

loading template information

updating template basic.slx (Services - Linux)

no update required

updating template fileatt.li (New File - Linux)

no update required

updating template internet.li (New File - Linux)

no update required
```

```
updating template lnxadore.mfw (Malicious File Watch - all)
no update required
updating template lnxlion.mfw (Malicious File Watch - all)
no update required
updating template lnxt0rn.mfw (Malicious File Watch - all)
no update required
updating template mail.li (New File - Linux)
no update required
updating template nfs.li (New File - Linux)
no update required
updating template objects.li (New File - Linux)
no update required
updating template patch.plx (Patch - Linux)
no update required
updating template queues.li (New File - Linux)
no update required
updating template remote.slx (Services - Linux)
no update required
updating template sysstart.li (New File - Linux)
no update required
updating template unix.fw (File Watch - all)
no update required
updating template unixhide.mfw (Malicious File Watch - all)
no update required
updating template unix.mfw (Malicious File Watch - all)
no update required
updating template uucp.li (New File - Linux)
no update required
updating template mysql.li (New File - Linux)
no update required
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: mysql_1

sync'ing policy: mysql_2

Report content file: update/ble/SU_3300/en/UpdatePackage.rdl

If you have already pushed this report content for other agents of
the same type of operating system with the same manager, you can
skip this step.

Do you wish to push the report content file [no]? yes

Update ESM check message mapping file: /esm/update/ble/SU_3300/en/
UpdatePackage.rdl

... Please wait...

Running "/esm/bin/lnx-x86/pushfiles" -v -m "10.218.103.20" -p 5600 -
t -U "esm" -P "******" -d "update/ble/SU_3300/en/UpdatePackage.rdl"
-s "/esm/update/ble/SU_3300/en/UpdatePackage.rdl"

Running "/esm/bin/lnx-x86/mergemanifest"... Please wait...

Merging src file: /esm/config/manifest.xml

Merging dst file: /esm/config/su/65/manifest.xml

End of installation

[root@localhost linux-x86]#
```

Installing the ESM Modules for MySQL databases silently

You can also install the ESM modules for MySQL silently using the esmmysql.tpi package. A silent installation does not require user interaction.

To install ESM modules for MySQL silently

- At the command prompt, enter the following command:
  ./esmmysql.tpi -it -m <manager name> -U <Username> -p <port no> -P <Password> -g <agent name> -e
  If the installation succeeds, the return value is 0. If the installation fails, the return value is 1.

Table 2-2 lists all the command line options that you can use for silent installation of ESM Modules.

Table 2-2 Command line options for silent installation of ESM Modules

Command line option	Description
-h	Displays the usage help
-d	Displays the description and contents of this tune-up/ third-party package.

Table 2-2 Command line options for silent installation of ESM Modules

Command line option	Description
-i	Installs the tune-up package.
-e	Installs the tune-up package without configuration.
-f	Forces installation of the package.
-P	The ESM access record password.
-U	The ESM access record name.
-p	The TCP port to use.
-m	The ESM manager name.
-t	Connects to the ESM manager through TCP.
-x	Connects to the ESM manager through IPX (WIndows only).
-g	The ESM agent name to use for registration.
-K	Doesn't prompt or re-registers
-L	The application name.
-n	No return required to exit tune-up package.
-N	Does not update report content file to manager.
-Y	Updates report content file to manager.

After installation, you can begin using Symantec ESM Modules for MySQL Databases.

Configuring the ESM Modules for MySQL databases silently

You can configure ESM Modules for MySQL databases silently using the esmmysqlsetup.

To add configuration records silently

- At the command prompt, type the following command:
  esmmysqlsetup -a -Q -A <account> -P <password> -t <port> -s<socket file> -S <instance> -T <SSL key> -W <CA Cert> -V <SSL Cert>

If the configuration succeeds, the return value is 0. If the configuration fails, the return value is 255.

After you run the esmmysqlsetup, the log file, EsmMySQLConfig.log is created in the following location:

/esm/system/<agent name>

The OpenSSL AES algorithm encryption stores the credentials in the disk file.

Table 2-3 lists all the command line options you can use for the silent configuration of MySQL databases.

Table 2-3 Command line options for silent configuration of MySQL databases

Command line option	Description
-a -Q	Configures silently a MySQL instance to ESM MySQL modules
-U {port}	Updates silently a MySQL instance to ESM MySQL modules.
-A {account}	Account to connect to the MySQL database.
-P {password}	Account password to connect to the MySQL database.
-t {port}	The port on which the MySQL database service is running. You must specify the port only when the the host in the account name is not a local host.
-s {socket file}	The path of the socket file to connect to the MySQL database. You must specify the path only when the the host in the account name is a local host.
-S {instance}	The instance name.
-T {SSL key}	The SSL client key that is required to connect to the MySQL database. If no value is provided, the setup takes the value, N/A.
-W {CA cert}	The CA cert that is required to connect to the MySQL database. If no value is provided, the setup takes the value, N/A.
-V {SSL cert}	The SSL cert that is required to connect to the MySQL database. If no value is provided, the setup takes the value, N/A.

You can also modify the configuration records silently using the esmmysqlsetup.

To edit the configuration records silently

- At the command prompt, type the following command:
  esmmysqlsetup -U {port} <switch> {value} <switch> {value}

To update password and SSL key

- At the command prompt, type the following command:
  esmmysqlsetup -U {port} -P {password} -T{SSL key}

Editing MySQL configuration records

After installing Symantec ESM Modules for MySQL Databases, you can edit the configuration records. A configuration record is created for each MySQL server.

You can add or remove the MySQL servers that have been configured for Symantec ESM Security checks using the esmmysqlsetup.

Table 2-4 lists the options that you can use when you run the esmmysqlsetup.

Table 2-4 esmmysqlsetup options

Command line options	Description
esmmysqlsetup -a	Configures a MySQL instance to Symantec ESM MySQL modules.
esmmysqlsetup -d {port}	Deletes a MySQL configuration record in the ESM MySQL module.
esmmysqlsetup -d all	Deletes all the MySQL configuration records in the ESM MySQL module.
esmmysqlsetup -l	Lists all the MySQL configuration records in the ESM MySQL module.
esmmysqlsetup -h	Displays the help.

Chapter 3

Reference

This chapter includes the following topics:

MySQL Accounts

Checks in this module report MySQL 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 special privileges
- Have anonymous accounts

MySQL server port

The MySQL server port option specifies the port numbers of the servers that are included or excluded by all the MySQL Account security checks.

Accounts with privileges

This check reports the logon accounts that have been granted important privileges in the user table. Use the name list to enter the list of privileges that have to be checked.

Table 3-1 lists the Accounts with privileges message.

Table 3-1 Accounts with privileges message

Message name	Title	Severity
MYSQL_UNAUTHORIZED_INTERNAL	Account with privileges	Red-4

Logon accounts

This check reports the user 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 Logon accounts message.

Table 3-2 Logon accounts message

Message name	Title	Severity
MYSQL_USER_ACCT	Logon account	Green-0

New logon accounts

This check reports the user 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 3-3 lists the New logon accounts message.

Table 3-3 New logon accounts message

Message name	Title	Severity
MYSQL_USER_ACCT_ADDED	New logon account	Yellow-1

Deleted logon accounts

This check reports the user 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 3-4 lists the Deleted logon accounts message.

Table 3-4 Deleted logon accounts message

Message name	Title	Severity
MYSQL_USER_ACCT_DELETED	Deleted database account	Yellow-1

Default accounts

This check reports all the default user accounts that are available on a computer. Use the name list to include or exclude logon names in this check.

Table 3-5 lists the Default accounts message.

Table 3-5 Default accounts message

Message name	Title	Severity
MYSQL_DEFAULT_ACCOUNT	Default account	Yellow-1

Anonymous account

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

Table 3-6 lists the Anonymous account message.

Table 3-6 Anonymous account message

Message name	Title	Severity
MYSQL_ANONYMOUS_ACCOUNT	Anonymous account	Yellow-1

Admin with null password

This check reports if the administrator account does not have a password. Use the name list to include or exclude logon names in this check.

Table 3-7 lists the Admin with null password message.

Table 3-7 Admin with null password message

Message name	Title	Severity
MYSQL_ADMIN_NULL_PASS	Admin with NULL password	Red-4

Automatically update snapshots

Use this option to update snapshots automatically.

MySQL Configuration

Checks in this module report the following information:

- MySQL version information
- Configuration parameters that are specified in a template
- MySQL daemon owner
- Status of the logs
- Information about the socket file

MySQL server port

The MySQL server port option specifies the port numbers of the servers that are included or excluded by all the MySQL Configuration security checks.

Version

This check reports the version of MySQL database.

Table 3-8 lists the Version message.

Table 3-8 Version message

Message name	Title	Severity
MYSQL_DB_VERSION	Version	Green-0

Configuration parameters

This check reports unauthorized configuration parameter values as specified in the MySQL Configuration Watch template. See "Creating the MySQL Configuration Watch template" on page 10.

At least one template file must be enabled for this check to work successfully.

Use the name lists to enable and disable template files.

Daemon owner

This check reports the user account that is the owner of MySQL daemon. Make sure that the administrator is not the owner of the MySQL daemon.

Table 3-9 lists the Daemon owner messages.

Table 3-9 Daemon owner messages

Message name	Title	Severity
MYSQL_OWENR	MySQL daemon owner	Green-0
MYSQL_OWENR_ROOT	Root is owner	Red-4

Logs status

This check reports the logs that are enabled. The logs on which this check reports are as follows:

- Error log
- General Query log
- Binary log
- Slow Query log

Table 3-10 lists the Logs status messages.

Table 3-10 Logs status messages

Message name	Title	Severity
MYSQL_GENERAL_QUERY_LOG	GENERAL QUERY LOG	Yellow-1
MYSQL_ERROR_LOG	MYSQL ERROR LOG	Green-0
MYSQL_LOG_FILE_PERM	MYSQL ERROR LOG	Yellow-1
MYSQL_BIN_LOG	MYSQL BINARY LOG	Green-0
MYSQL_GENERAL_QUERY_LOG_DIS	GENERAL QUERY LOG	Green-0
MYSQL_BIN_LOG_DIS	MYSQL BINARY LOG	Yellow-1
MYSQL_ERROR_LOG_DIS	MYSQL ERROR LOG	Yellow-1

Sock file

This check reports the location of the socket file and its permissions.

Table 3-11 lists the Sock file messages.

Table 3-11 Sock file messages

Message name	Title	Severity
MYSQL_SOCK_FILE	Socket file	Green-0
MYSQL_SOCK_FILE_WRONGLOC	Socket file	Red-4

MySQL Databases

Checks in this module report the following information:

- Databases on the MySQL server
- Sample databases on the MySQL server
- New databases on the MySQL server
- Deleted databases on the MySQL server

MySQL server port

The MySQL server port option specifies the port numbers of the servers that are included or excluded by all the MySQL Databases security checks.

List databases

This check lists the databases that are installed on the MySQL server. Use the name list to include or exclude the databases in this check.

Table 3-12 lists the List databases message.

Table 3-12 List database message

Message name	Title	Severity
MYSQL_DB_LIST	Databases	Green-0

Sample databases

This check lists the databases that are installed by default when MySQL server is installed.

Table 3-13 lists the Sample databases message.

Table 3-13 Sample database message

Message name	Title	Severity
MYSQL_DB_SAMPLE	Sample databases	Yellow-1

New databases

This check lists the newly created databases that were added to the MySQL server after the last snapshot update. Use the name list to include or exclude databases in this check.

Table 3-14 lists the New databases message.

Table 3-14 New database message

Message name	Title	Severity
MYSQL_DB_NEW	New databases	Yellow-1

Deleted databases

This check lists the databases that were deleted from the MySQL server after the last snapshot update. Use the name list to include or exclude databases in this check.

Table 3-15 lists the Deleted databases message.

Table 3-15 Deleted database message

Message name	Title	Severity
MYSQL_DB_DELETED	Deleted databases	Yellow-1

Automatically update snapshots

Use this option to update snapshots automatically.

MySQL Passwords

Checks in this module report the following information:

- Logons with no passwords
- Easily guessed logon and administrator passwords

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

MySQL server port

The MySQL server port option specifies the port numbers of the servers that are included or excluded by all the MySQL Password security checks.

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 37.

Users to check

Use the name list to include or exclude users for all MySQL Password checks.

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

Password = username

This check reports the user accounts with passwords that are the same as their user names.

The check is provided for systems with a large number of user accounts. This check is not as thorough as Password = any username.

If the Password = any username check takes long time to run or consumes a significant amount of CPU, you can use Password = username daily and Password = any username on weekends.

Intruders frequently substitute user names for passwords when they try to break in.

Table 3-16 lists the Password = username message.

Table 3-16 Password = username message

Message name	Title	Severity
MYSQL_PASS_GUESSED	Weak user password	Red-4

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See "About secure passwords" on page 34.

Password = any username

This check reports the user accounts with passwords that match any user name.

Intruders frequently substitute user names for passwords when they try to break in.

Table 3-17 lists the Password = any username message.

Table 3-17 Password = any username message

Message name	Title	Severity
MYSQL_PASS_GUESSED	Weak user password	Red-4

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.

See “About secure passwords” on page 34.

Password = wordlist word

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

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

Table 3-18 lists the Password = wordlist word messages.

Table 3-18 Password = wordlist word messages

Message name	Title	Severity
MYSQL_NO_WORDS	No word files specified	Red-4
MYSQL_PASS_GUESSED	Weak user password	Red-4

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See “About secure passwords” on page 34.

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 MySQL Password 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 3-19 lists the word files that are installed with this product.

Table 3-19 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 3-19 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.

Null password

This check reports the user accounts that have NULL passwords.

User accounts with NULL passwords are subject to high security risk. Always assign passwords to user accounts.

Table 3-20 lists the Null password message.

Table 3-20 Null password message

Message name	Title	Severity
MYSQL_NULL_PASS	Null password	Red-4

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.

See "About secure passwords" on page 34.

Reverse order

This option enables the password checks report the user accounts with passwords that match the reverse of user 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 = username or Password = any username, and the Password = wordlist checks.

Intruders often use common names or words in reverse order as passwords when they try to break in.

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See "About secure passwords" on page 34.

Double occurrences

This option enables the password checks to report user accounts with passwords that match doubled versions of user 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 = username or Password = any username, and the Password = wordlist checks.

Intruders often use doubled versions of user names or common words as passwords when they try to break in.

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See "About secure passwords" on page 34.

Plural

This option enables the password checks to report user accounts with passwords that match plural forms of user 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 = username or Password = any username, and the Password = wordlist checks.

Intruders often use plural forms of login names or common words as passwords when they try to break in.

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See "About secure passwords" on page 34.

Prefix

This option enables the password checks to report user accounts with passwords that match forms of user 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 = username or Password = any username, and the Password = wordlist checks.

Intruders often add prefixes to user names or common words when they try to break in.

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See "About secure passwords" on page 34.

Suffix

This option enables the password checks to report user accounts with passwords that match forms of user 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 = username or Password = any username, and the Password = wordlist checks.

Intruders often add suffixes to user names or common words when they try to break in.

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.
  See "About secure passwords" on page 34.

Well known passwords

This check reports the user name/password combinations that are known to everyone. For example, scott/tiger, which is the default user name/password combination for MySQL databases.

Use the name list to specify such well known passwords for the check.

Intruders often use well-known passwords when they try break in.

Table 3-21 lists the Well known passwords message.

Table 3-21 Well known passwords message

Message name	Title	Severity
MYSQL_PASS_GUESSED	Weak user password	Red-4

To protect your computers

- If an empty or weak password is found, assign a more secure temporary password to the user account. Inform the user about the change and provide instructions on setting a secure password.

See "About secure passwords" on page 34.

Password display

This option, if enabled, displays the passwords reported by the Password = username, Password = any username, and Password = wordlist checks in the following format:

User <name> : Password is <first_character> * <last_character>

By default, the passwords are displayed in the following format:

<name> : <password>

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

MySQL Privileges

Checks in this module report the following information:

- Global privileges
- Schema privileges
- File privileges
- Super privileges
- Shutdown privileges
- Grant privileges
- Changes in any of the privileges

MySQL server port

The MySQL server port option specifies the port numbers of the servers that are included or excluded by all the MySQL Privilege security checks.

List global privilege

This check reports the global privileges that the MySQL server and its databases hold. For example, SHUTDOWN privilege is a global privilege. Use the name list to exclude or include the users in this check.

This check reports on the following global privileges:

- Select
- Insert
- Update
- Delete
- Create
- Drop
- Reload
- Lock_tables_priv

- Process
- Execute_priv
- References
- Index
- Alter

Table 3-22 lists the List global privilege message.

Table 3-22 List global privilege message

Message name	Title	Severity
MYSQL_GLOBAL_PRIVILEGES	Global privileges	Yellow-2

List changed global privilege

This check reports the database accounts with GLOBAL privileges that were changed after the last snapshot update. Use the name list to exclude or include the users in this check.

Table 3-23 lists the List changed global privilege message.

Table 3-23 List changed global privilege message

Message name	Title	Severity
MYSQL_CHANGED_GLOBAL_PRIVILEGES	Changed global privileges	Yellow-2

List schema privilege

This check reports the database privileges for all users. Use the name list to exclude or include the users in this check.

This check reports on the following schema privileges:

- Select
- Insert
- Update
- Delete
- Create
- Drop
- Grant

- References
- Index
- Alter

Table 3-24 lists the List schema privilege message.

Table 3-24 List schema privilege message

Message name	Title	Severity
MYSQL_DB_PRIVILEGES	Schema level privileges	Yellow-2

List changed schema privilege

This check reports the database accounts with database privileges that were changed after the last snapshot update. Use the name list to exclude or include the users in this check.

Table 3-25 lists the List changed schema privilege messages.

Table 3-25 List changed schema privilege messages

Message name	Title	Severity
MYSQL_CHANGED_DB_PRIVILEGES	Changed schema privileges	Yellow-2
MYSQL_DB_PRIV_DELETED	Deleted entry from DB table	Yellow-2
MYSQL_DB_PRIV_ADDED	Added entry to DB table	Yellow-2

List file privilege

This check reports the users with LOCAL IN FILE privilege. Use the name list to exclude or include the users in this check.

Table 3-26 lists the List file privilege message.

Table 3-26 List file privilege message

Message name	Title	Severity
MYSQL_FILE_PRIVILEGES	Users with FILE privileges	Yellow-2

List changed file privilege

This check reports the database accounts with LOCAL IN FILE privileges that were changed after the last snapshot update. Use the name list to exclude or include the users in this check.

Table 3-27 lists the List changed file privilege message.

Table 3-27 List changed file privilege message

Message name	Title	Severity
MYSQL_ENABLED_FILE_PRIVILEGES	Enabled FILE privileges	Yellow-2
MYSQL_DISABLED_FILE_PRIVILEGES	Disabled FILE privileges	Yellow-2

List super privilege

This check reports the users with SUPER privilege. Use the name list to exclude or include the users in this check.

Table 3-28 lists the List super privilege message.

Table 3-28 List super privilege message

Message name	Title	Severity
MYSQL_SUPER_PRIVILEGES	Users with SUPER privileges	Yellow-2

List changed super privilege

This check reports the database accounts with SUPER privileges that were changed after the last snapshot update. Use the name list to exclude or include the users in this check.

Intruders can misuse the SUPER privilege to terminate user accounts and change the way in which the MySQL server operates.

Table 3-29 lists the List changed super privilege message.

Table 3-29 List changed super privilege message

Message name	Title	Severity
MYSQL_ENABLED_SUPER_PRIVILEGES	Enabled SUPER privileges	Yellow-2
MYSQL_DISABLED_SUPER_PRIVILEGES	Disabled SUPER privileges	Yellow-2

List shutdown privilege

This check reports the users with SHUTDOWN privilege. Use the name list to exclude or include the users in this check.

Table 3-30 lists the List shutdown privilege message.

Table 3-30 List shutdown privilege message

Message name	Title	Severity
MYSQL_SHUTDOWN_PRIVILEGES	Users with SHUTDOWN privileges	Yellow-2

List changed shutdown privilege

This check reports the database accounts with SHUTDOWN privileges that were changed after the last snapshot update.

Intruders can misuse the SHUTDOWN privilege to terminate the MySQL server and deny access to other users.

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

Table 3-31 lists the List changed shutdown privilege message.

Table 3-31 List changed shutdown privilege message

Message name	Title	Severity
MYSQL_ENABLED_SHUTDOWN_PRIVILEGES	Enabled SHUTDOWN privileges	Yellow-2
MYSQL_DISABLED_SHUTDOWN_PRIVILEGES	Disabled SHUTDOWN privileges	Yellow-2

List grant privilege

This check reports the users with GRANT privilege.

The GRANT privilege enables the users to assign their privileges to other users. For example, if two users have different privileges, they can use the GRANT privilege to assign their privileges to each other.

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

Table 3-32 lists the List grant privilege message.

Table 3-32 List grant privilege message

Message name	Title	Severity
MYSQL_GRANT_PRIVILEGES	Users with GRANT privileges	Yellow-2

List changed grant privilege

This check reports the database accounts with GRANT privileges that were changed after the last snapshot update.

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

Table 3-33 lists the List changed grant privilege message.

Table 3-33 List changed grant privilege message

Message name	Title	Severity
MYSQL_ENABLED_GRANT_PRIVILEGES	Enabled GRANT privileges	Yellow-2
MYSQL_DISABLED_GRANT_PRIVILEGES	Disabled GRANT privileges	Yellow-2

Automatically update snapshots

Use this option to update snapshots automatically.

Note: For checks that have a name list option, the users must be specified in the following format:
username@hostname
The format, however, for the checks, List schema privileges and List changed schema privileges is as follows:
username@hostname@databasename

---

mysql.li template

Symantec ESM Modules for MySQL Databases ship with the mysql.li template in the File Attributes module. This template, when enabled, causes the Template files check in the module to check the files on the MySQL database.

The mysql.li template is enabled by default.

Chapter 4

Troubleshooting

This chapter includes the following topics:

Encryption Exception error

Encryption exception error may occur when you run a policy. The error message prompts you to reconfigure the module.

Table 4-1 lists the error message that is displayed and the solution for the error.

Table 4-1 Encryption exception error

Error	Solution
Encryption exception	This error may occur if you have manually reset SSLConfigure=0 after configuring the MySQL module. The error may also occur if you have renamed or deleted the AESConfigMYSQL.dat file. To solve this problem, you must reconfigure the MySQL module. If you want to generate logs for encryption, add Debugon=1 in the AESConfigMYSQL.dat from the esm\config folder. This change in the DAT file generates MYSQLAESdebuglog.log in the following folder: esm\system\<platform>