

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

Release 3.1.0 for Symantec ESM 6.0, 6.1, and 6.5.x

For Red Hat Enterprise Linux

MySQL 4.0, 4.1, and 5.0



# Symantec ESM Modules for MySQL Databases User's Guide

## Release 3.1.0

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.

### Legal Notice

Copyright ©2007 Symantec Corporation.

All Rights Reserved.

Symantec, the Symantec Logo, LiveUpdate, Symantec Enterprise Security Architecture, Enterprise Security Manager, and NetRecon are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this 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/](http://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/](http://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/](http://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/](http://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](mailto:contractsadmin@symantec.com)
- Europe, Middle-East, and Africa: [semea@symantec.com](mailto:semea@symantec.com)
- North America and Latin America: [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

## Additional Enterprise services

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

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each 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](http://www.symantec.com)

Select your country or language from the site index.



# Contents

Chapter 1	Introducing Symantec ESM Modules for MySQL Databases	
	About Symantec ESM Modules for MySQL Databases .....	10
	Components of Symantec ESM Modules for MySQL Databases .....	10
	Modules .....	10
	Templates .....	11
	How Symantec ESM modules work .....	12
	What you can do with Symantec ESM Modules for MySQL Databases .....	12
	Where you can get more information .....	13
Chapter 2	Installing Symantec ESM Modules for MySQL Server Databases	
	System requirements .....	16
	Installing the modules .....	17
	Log .....	20
	Post-installation tasks .....	28
	Agent registration .....	28
	Adding configuration records .....	28
Chapter 3	Reference	
	MySQL Accounts .....	30
	Accounts with privileges .....	30
	Logon accounts .....	30
	New logon accounts .....	30
	Deleted logon accounts .....	31
	Default accounts .....	31
	Anonymous account .....	31
	Admin with null password .....	32
	Automatically update snapshots .....	32
	MySQL Configuration .....	32
	Version .....	32
	Configuration parameters .....	32
	Daemon owner .....	33
	Logs status .....	33
	Sock file .....	34
	MySQL Databases .....	34

List databases .....	34
Sample databases .....	34
New databases .....	35
Deleted databases .....	35
Automatically update snapshots .....	35
MySQL Passwords .....	35
About secure passwords .....	36
Users to check .....	36
Password = username .....	36
Password = any username .....	37
Password = wordlist word .....	37
Null password .....	41
Reverse order .....	42
Double occurrences .....	42
Plural .....	42
Prefix .....	43
Suffix .....	43
Well known passwords .....	44
Password display .....	44
MySQL Privileges .....	45
List global privilege .....	45
List changed global privilege .....	45
List schema privilege .....	46
List changed schema privilege .....	46
List file privilege .....	46
List changed file privilege .....	46
List super privilege .....	47
List changed super privilege .....	47
List shutdown privilege .....	47
List changed shutdown privilege .....	48
List grant privilege .....	48
List changed grant privilege .....	48
Automatically update snapshots .....	49
mysql.li template .....	49

# Introducing Symantec ESM Modules for MySQL Databases

This chapter includes the following topics:

- [About Symantec ESM Modules for MySQL Databases](#)
- [Components of Symantec ESM Modules for MySQL Databases](#)
- [How Symantec ESM modules work](#)
- [What you can do with Symantec ESM Modules for MySQL Databases](#)
- [Where you can get more information](#)

# 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 30.

## 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 32.

## MySQL Databases

Checks in this module report the default, sample, new, and deleted databases on the MySQL server. See [“MySQL Databases”](#) on page 34.

## MySQL Passwords

Checks in this module report logons with empty passwords and easily guessed passwords. See [“MySQL Passwords”](#) on page 35.

## 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 45.

## 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: <pre>show variables</pre>
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>.



# Installing Symantec ESM Modules for MySQL Server Databases

This chapter includes the following topics:

- [Before you install](#)
- [System requirements](#)
- [Installing the modules](#)
- [Post-installation tasks](#)

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

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 read privileges on the database to perform ESM security checks on MySQL 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	Supported OS versions	Supported MySQL versions
Red Hat Linux (32-bit, 64-bit)	5	5.0
Red Hat Enterprise Linux (32-bit, 64-bit)	ES 4	4.0, 5.0
Red Hat Enterprise Linux (32-bit, 64-bit)	ES 3	4.0, 4.1

# Installing the modules

Symantec ESM Modules for MySQL Databases are stored in an installation package, `esmmysql.tpi`, 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 Symantec Security Response Web site at [http://www.symantec.com/avcenter/security/Content/Product/Product\\_ESM.html](http://www.symantec.com/avcenter/security/Content/Product/Product_ESM.html), under application modules, download `esmmysql.tpi`.
- 2 Run `esmmysql.tpi`.
- 3 Select one of the following:

- |          |   |
|----------|---|
| Option 1 | Displays the contents of the package. To install the module, rerun <code>esmmysql.tpi</code> and select option 2. |
| Option 2 | Displays the list of files that are installed and the modules or templates to which they belong.                  |
| Option 3 | Quit the installation.  |

---

**Note:** Register template and .m files only once 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 “[To add security checking](#)” on page 18.
- 5 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.
- 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:
  - 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 MySQL database. Do one of the following:
  - To continue the installation, type **Y**.
  - To end the installation without adding the security checks, type **N**.
- 2 Do one of the following:
  - To continue the installation and configure the MySQL database for security checks, type **Y**.
  - To end the installation without adding the security checks, type **N**.
- 3 Type the user name and the host name for the MySQL database in the following format:  
<user\_name>@<host\_name>
- 4 Type the password for the MySQL database.
- 5 Retype the password for verification.
- 6 Type the port that is used to contact the MySQL database.
- 7 Type the location of the socket file that is used to establish connection with the MySQL database.
- 8 Do one of the following:
  - If you want to use SSL to communicate with the MySQL database, type **Y**.
  - If you do not want to use SSL to communicate with the MySQL database, type **N**.
- 9 If you want to use SSL to communicate with the MySQL database, type the following:
  - Location of the SSL Client Key file
  - Location of the SSL Client Certificate file
  - Location of the SSL Client CA Certificate file

The MySQL object is initiated and the connection with MySQL database is established.

**10** 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.

## 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@esm-linux 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 3.0.0  
(2007/05/28)
```

```
Tuneup pack will overlay Symantec ESM Modules for MySQL Databases  
version 3.0.0 with version 3.0.0
```

```
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/mysqlpdb.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/mysqlldb.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  
[esm-linux]: 10.218.148.102

ESM Manager : 10.218.103.20

ESM user name : esm

Protocol : TCP

Port : 5600

ESM agent : 10.218.148.102

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/mysqlldb.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/mysqlldb.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/mysqlldb.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_3000/en/UpdatePackage.rdl.gz...
Extracting /tmp/esmthird.gz...
```

Continue and add configuration records to enable ESM security checking

for your MySQL database? [Y/N] y

```
running /esm/bin/lnx-x86/esmmysqlsetup -a -all
```

Configure MySQL for ESM security checks? [Y/N] y

Connecting to MySQL

The privilege MySQL logon account is  
to perform the ESM Modules for MySQL Database security checks.  
Database security checks will be validated for CONNECT and SELECT  
privileges.

Enter [userName@Hostname] : root@localhost

Enter [root@localhost] account password :

Verify password :

Enter the port number [root@localhost]: 3306

Enter the Socket file location [/var/lib/mysql/mysql.sock]:

Use SSL for establishing connection with the server? [Y/N] y

```
Enter the SSL client key file location [../../client-key]: /newcerts/  
client-key.pem
```

```
Enter the SSL client certificate file location [../../client-cert]: /  
newcerts/client-cert.pem
```

```
Enter the SSL client ca certificate file location [../../ca-cert]: /  
newcerts/ca-cert.pem
```

```
Connecting ...
```

```
MySQL Object initiated
```

```
Connected
```

```
config.c 188 ssl_key = / newcerts/client-key.pem ssl_cert = /  
newcerts/client-cert.pem ssl_ca = /newcerts/ca-cert.pemp-> = 3306 p->  
> username = root p-> host name = localhost
```

```
Succeeded Establishing MySQL connection
```

```
Tune-up pack installation complete
```

```
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  
"10.218.148.102" -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: esmsu-mysql.properties
    skipping: file already uploaded ...
uploading property file: esmsu-unix.properties
    skipping: file already uploaded ...
uploading property file: esm-unix.properties
    skipping: file already uploaded ...
loading template information
updating template unixhide.mfw (Malicious File Watch - all)

no update required
    updating template internet.li (New File - Linux)

no update required
    updating template basic.slx (Services - Linux)

no update required
    updating template nfs.li (New File - Linux)

no update required
    updating template patch.plx (Patch - Linux)

no update required
    updating template fileatt.li (New File - 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 lnxt0rn.mfw (Malicious File Watch - all)

no update required
    updating template objects.li (New File - Linux)

no update required
```

```
        updating template lnxlion.mfw (Malicious File Watch - all)

no update required
        updating template lnxadore.mfw (Malicious File Watch - all)

no update required
        updating template mysql.li (New File - Linux)

no update required
        updating template uucp.li (New File - Linux)

no update required
        updating template unix.fw (File Watch - all)

no update required
        updating template mail.li (New File - Linux)

no update required
        updating template unix.mfw (Malicious File Watch - all)

no update required
        updating template sysstart.li (New File - Linux)

no update required
        sync'ing policy: Dynamic Assessment
        sync'ing policy: MySQL-Linux-17799-base
        sync'ing policy: Oracle-Linux-17799-base
        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
        sync'ing policy: new
Report content file: update/ble/SU_3000/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\_3000/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_3000/en/UpdatePackage.rdl"  
-s "/esm/update/ble/SU_3000/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

## Post-installation tasks

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

### Agent registration

Each Symantec ESM agent must reregister with a Symantec ESM manager. The `esmmysql.tpi` 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.

### Adding configuration records

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

[Table 2-2](#) lists the options that you can use when running `esmmysqlsetup`.

**Table 2-2** Adding configuration records

To do this	Type
Add a new configuration record for undetected MySQL servers.	<code>esmmysqlsetup -a -all</code>

# Reference

This chapter includes the following topics:

- [MySQL Accounts](#)
- [MySQL Configuration](#)
- [MySQL Databases](#)
- [MySQL Passwords](#)
- [MySQL Privileges](#)
- [mysql.li template](#)

# 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

## Accounts with privileges

This check reports the logon accounts that have been granted important privileges in the user table.

[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 database 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

## 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 12.

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 ERROR 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

## Socket file

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

[Table 3-11](#) lists the Socket file messages.

**Table 3-11** Socket file messages

Message name	Title	Severity
MYSQL_SOCKET_FILE	Socket file	Green-0
MYSQL_SOCKET_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

## List databases

This check lists the databases that are installed on the MySQL server.

[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.

---

## 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 39.

## 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 36.

## 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 36.

## 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 36.

## 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	651
	Fname_D.wrd	1602
	Fname_FR.wrd	784
	Fname_I.wrd	952
	Fname_NL.wrd	724
	Fname_Pwrd	449
	Fname_SP.wrd	349
Last name	lastnam.wrd	2958
	Lname_D.wrd	3101
	Lname_FR.wrd	3196
	Lname_I.wrd	2848
	Lname_NL.wrd	3005
	Lname_Pwrd	723
	Lname_SP.wrd	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 .wrд 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 36.

## 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 36.

## 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 36.

## 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 36.

## 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 36.

## 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 36.

## 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 36.

## 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

### 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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

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.

[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.

[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.

[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.

[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.

## 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.

