

Symantec Enterprise Security Manager™ Modules for IBM DB2 Universal Databases User's Guide v2.0.1

Release for Symantec ESM 5.5, 6.x, and 6.5.x

For Windows, AIX, Solaris, Red Hat Linux



Symantec Enterprise Security Manager Modules for IBM DB2 Universal Databases User's Guide

Release 2.0.1

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 ©2008 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/

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, 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

Select your country or language from the site index.

Chapter 1 Introducing ESM Modules for IBM DB2 Universal Databases

| | |
|--|----|
| Preparing for IBM DB2 module installation | 6 |
| Minimum account privileges | 6 |
| System requirements | 7 |
| Installing the IBM DB2 module on Windows | 9 |
| Windows installation log | 11 |
| Silently installing the IBM DB2 module on Windows | 16 |
| Installing the IBM DB2 module on Linux, Solaris, or AIX | 17 |
| Linux, AIX, and Solaris installation log | 19 |
| Silently installing the IBM DB2 module on Linux, Solaris, or AIX | 24 |
| Configuring the IBM DB2 Remote module on Windows, Linux, Solaris, and AIX 25 | |
| Editing the configuration records | 25 |
| Silently configuring the IBM DB2 Remote module | 26 |
| Configuring the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules on Linux, Solaris, and AIX | 27 |
| Editing the configuration records | 27 |
| Silently configuring the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules 28 | |
| Creating a baseline snapshot | 28 |

Chapter 2 Understanding the DB2 Audit Configuration module

| | |
|--|----|
| About the DB2 Audit Configuration module | 32 |
| Auditing Enabled | 32 |
| Event Types | 32 |
| Audit Failure Events | 32 |
| Audit Success Events | 33 |
| Audit Database Events | 33 |
| Auditing Related Events | 33 |
| Checking Events | 33 |
| Object Maintenance Events | 34 |
| Security Maintenance Events | 34 |
| System Administrator Events | 34 |
| Validate Events | 34 |
| Context Events | 35 |
| Error Handling Facility | 35 |
| Audit Miscellaneous Events | 35 |
| Instance Startup and Shutdown | 36 |
| Changes To Configuration Parameters | 36 |
| Database Activation and Deactivation | 36 |
| Use of SYSADM, DBADM, SYSCTRL, and SYSMANT | 37 |
| Attempted Access To Restricted Objects | 37 |
| Access To Sensitive Objects and/or Tables | 37 |
| Unsuccessful Connection Attempts | 38 |

| | |
|--|----|
| Administrative Functions Performed | 38 |
|--|----|

Chapter 3 Understanding the IBM DB2 Fix Packs module

| | |
|--|----|
| About the IBM DB2 Fix Packs module | 39 |
| Template files | 39 |
| Installed Fix Packs | 40 |

Chapter 4 Understanding the IBM DB2 Remote module

| | |
|---|----|
| About the IBM DB2 Remote module | 41 |
| IBM DB2 Database Aliases | 41 |
| Authentication from the Server | 43 |
| DB2 Version and OS | 43 |
| Discovery mode | 43 |
| Server Discovery Mode | 43 |
| Instance Discovery Mode | 44 |
| Database Discovery Mode | 44 |
| System authorities | 45 |
| Unauthorized Group Set in System Administrator Authority | 45 |
| Unauthorized Group Set in System Control Authority | 45 |
| Unauthorized Group Set in System Maintenance Authority | 46 |
| Unauthorized Group/User in Database Administrator Authority | 46 |
| New Group/User in Database Administrator Authority | 47 |
| Deleted Group/User in Database Administrator Authority | 47 |
| Modified Group/User in Database Administrator Authority | 48 |
| Unauthorized Group/User in LOAD Authority | 48 |
| New Group/User in LOAD Authority | 49 |
| Deleted Group/User in LOAD Authority | 49 |
| Modified Group/User in LOAD Authority | 50 |
| Database privileges | 51 |
| Unauthorized Group/User in BINDADD Database Privilege | 51 |
| New Group/User in BINDADD Database Privilege | 51 |
| Deleted Group/User in BINDADD Database Privilege | 52 |
| Modified Group/User in BINDADD Database Privilege | 52 |
| Unauthorized Group/User in CONNECT Database Privilege | 53 |
| New Group/User in CONNECT Database Privilege | 53 |
| Deleted Group/User in CONNECT Database Privilege | 54 |
| Modified Group/User in CONNECT Database Privilege | 54 |
| Unauthorized Group/User in CREATETAB Database Privilege | 55 |
| New Group/User in CREATETAB Database Privilege | 55 |
| Deleted Group/User in CREATETAB Database Privilege | 56 |
| Modified Group/User in CREATETAB Database Privilege | 56 |
| Unauthorized Group/User in CREATE_NOT_FENCED Database Privilege | 57 |

| | |
|---|----|
| New Group/User in CREATE_NOT_FENCED Database Privilege | 57 |
| Deleted Group/User in CREATE_NOT_FENCED Database Privilege .. | 58 |
| Modified Group/User in CREATE_NOT_FENCED Database Privilege | 58 |
| Unauthorized Group/User in IMPLICIT_SCHEMA Database Privilege | 59 |
| New Group/User in IMPLICIT_SCHEMA Database Privilege | 59 |
| Deleted Group/User in IMPLICIT_SCHEMA Database Privilege | 60 |
| Modified Group/User in IMPLICIT_SCHEMA Database Privilege | 60 |

Chapter 5 Troubleshooting

| | |
|--------------------------------|----|
| Encryption exception | 61 |
| DB2 Remote module errors | 61 |

Introducing ESM Modules for IBM DB2 Universal Databases

This chapter includes the following topics:

- [Preparing for IBM DB2 module installation](#)
- [System requirements](#)
- [Installing the IBM DB2 module on Windows](#)
- [Silently installing the IBM DB2 module on Windows](#)
- [Installing the IBM DB2 module on Linux, Solaris, or AIX](#)
- [Silently installing the IBM DB2 module on Linux, Solaris, or AIX](#)
- [Configuring the IBM DB2 Remote module on Windows, Linux, Solaris, and AIX](#)
- [Silently configuring the IBM DB2 Remote module](#)
- [Configuring the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules on Linux, Solaris, and AIX](#)
- [Silently configuring the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules](#)
- [Creating a baseline snapshot](#)

Preparing for IBM DB2 module installation

To install the IBM DB2 module, you need the following:

- CD-ROM access: At least one machine on your network must have a CD-ROM drive.
- Account privileges: You must have Administrator rights on each computer where you plan to install the module.
- Connection to the manager: Verify that the ESM Enterprise Console can connect to the ESM manager.
- Agent and manager: You must have an ESM agent running and registered to at least one ESM manager.
- ESM Security Update 12: You must have ESM SU12 installed on the same computer as your ESM manager.
- IBM DB2 client and server: You must have a IBM DB2 client application and IBM DB2 server installed on the same computer where you plan to install the ESM DB2 module.

Note: Symantec ESM Modules for IBM DB2 Universal Databases supports v8.1, v8.2, and v9.1 databases.

Minimum account privileges

For the IBM DB2 Remote module, the login accounts need minimum privileges to execute the following commands for performing ESM security checks on IBM DB2 Server:

- `select syscat.dbauth`
- `get database manager configuration`
- `get database configuration for <db>`

For the IBM DB2 Audit Configuration module that is installed on Linux, Solaris, or AIX, the login account that you specify during configuration must have the following authority:

- `sysadm`

Note: No specific privileges are required for the IBM DB2 Audit Configuration module to work on Windows.

System requirements

[Table 1-1](#) lists the IBM DB2 operating systems on which the ESM application modules for IBM DB2 can be installed.

Table 1-1 Operating systems for installing ESM application modules for IBM DB2

| Supported IBM DB2 operating systems | Supported OS versions |
|-------------------------------------|-----------------------------|
| Red Hat Enterprise Linux (32-bit) | 4 and 5 |
| Windows (32-bit) | 2000 Server and 2003 Server |
| Sun Solaris Sparc | 9 and 10 |
| AIX (32-bit, 64-bit) | 5.2 |
| AIX (64-bit) | 5.3 |

[Table 1-2](#) lists the IBM DB2 operating systems on which the IBM DB2 Remote module for Windows can report remotely.

Table 1-2 Supported IBM DB2 operating systems for IBM DB2 Remote module

| Supported IBM DB2 operating systems | Supported OS versions | Supported IBM DB2 versions |
|---|-----------------------|----------------------------|
| Red Hat Enterprise Linux (32-bit, 64-bit, and IA64-bit) | 4 and 5 | 8.1, 8.2, and 9.1 |
| AIX (64-bit) | 5.2 | 8.1 and 8.2 |
| AIX (64-bit) | 5.3 | 9.1 |
| Sun Solaris Sparc | 9 and 10 | 9.1 |
| Windows (32-bit) | Windows 2000 Server | 8.1, 8.2, and 9.1 |
| Windows (32-bit, 64-bit, and IA64-bit) | Windows 2003 Server | 8.1, 8.2, and 9.1 |

[Table 1-3](#) lists the IBM DB2 operating systems on which the IBM DB2 Host based modules can report.

Table 1-3 Supported IBM DB2 operating systems for Host based modules

| Supported IBM DB2 operating systems | Supported OS versions | Supported IBM DB2 versions |
|-------------------------------------|------------------------------|----------------------------|
| Red Hat Enterprise Linux (32-bit) | 4 and 5 | 8.1, 8.2, and 9.1 |
| AIX (32-bit, 64-bit) | 5.2 | 8.1, 8.2, and 9.1 |
| AIX (64-bit) | 5.3 | 8.1, 8.2, and 9.1 |
| Sun Solaris Sparc | 9 and 10 | 8.1, 8.2, and 9.1 |
| Windows (32-bit) | Windows 2000 and 2003 Server | 8.1, 8.2, and 9.1 |

Installing the IBM DB2 module on Windows

You can install the IBM DB2 module using `esmdb2tpi.exe`.

The installation program does the following:

- Extracts and installs module executables and configuration (.m) files.
- Registers the .m and template files using the `register.exe` program on the agent.

To run the installation program and register the files

- 1 From the CD, run
`\\DATABASES\DB2\Modules\<<architecture>\esmdb2tpi.exe`.
- 2 Choose an option:
 - Option 1: to display the contents of the package.
To install the module, rerun `esmdb2tpi.exe` and select option 2.
 - Option 2: to begin the installation.
- 3 Do you wish to register the template or .m files?
 - If the files are not registered with the manager, type Y.
 - If the files have already been registered, type N and skip to “To enable security checking for your IBM DB2 databases” on page 9.

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

- 4 Enter the ESM manager that the agent is registered to. Typically, this is the name of the computer that the manager is installed on.
- 5 Enter the ESM access name (logon name) for the manager.
- 6 Enter the ESM password that is used to log on to the ESM manager.
- 7 Enter the network protocol that is used to contact the ESM manager.
- 8 Enter the port that is used to contact the ESM Manager. The default port is 5600.

- 9 Enter the name of the agent as it is registered to the ESM manager. Typically, this is the name of the computer that the agent is installed on.
- 10 Is this information correct?
 - If the displayed information is correct, type Y.
The installation program lists files as they are extracted.
 - If the information is not correct, type N.
The installation program begins again, allowing you to enter the correct information.

To enable security checking for your IBM DB2 databases

- 1 When the extraction is complete, you will be asked if you want to add configuration records to enable ESM security checking for your IBM DB2 databases.
 - To continue the installation and enable security checking for your databases, type Y.
When you install the IBM DB2 module on Windows, the installation program automatically detects the existing IBM DB2 databases and displays them one at a time.
 - To end the installation without adding security checking, type N.
- 2 Would you like to add a configuration record for this database?
 - Type Y to add a configuration record for the database.
 - Type N to skip this database and go to the next database.
- 3 Enter the IBM DB2 database alias. Press Enter if you are satisfied with the detected alias.
- 4 Enter the IBM DB2 instance name.

Note: Specify the node name if the node name is different from the attached instance name. Open the IBM DB2 Command Center to find the node name.

- 5 Enter the User ID that is used to log on to the IBM DB2 database.
- 6 Enter the password that is used to log on to the IBM DB2 database.

- 7 Is this information correct?
- Type Y to save the configuration record and continue with the next detected database.
 - Type N to begin again with this database.

Note: The IBM DB2 User ID and password are encrypted when they are displayed for your approval.

- 8 Repeat steps 2-8 for each database that is detected.
- After you have created configuration records for each database, the program lists all of the configuration records and the following options:
- Option 1: to manually create a new configuration record for an undetected database.
 - Option 2: to modify or remove an existing configuration record.
 - Option 3: to finish the installation and exit the program.

Note: The encryption that is used to store the credentials in disk file is OpenSSL AES algorithm.

Windows installation log

The following log is an example of an ESM Modules for IBM DB2 Universal Databases installed on Windows. Your log may look different, depending on how your manager and agents are configured.

```
Symantec Corporation tune-up/installation package
```

```
Options:
```

```
  1) Display the description and contents of the tune-up/  
installation package  
  2) Install the tune-up/installation package on your system  
  3) Quit
```

```
Enter option number [1]: 2
```

```
Installing package: "ESM modules for DB2" 2.0
```

```
Tuneup pack will overlay ESM modules for DB2 version 1.0 with  
version 2.0
```

```
This package includes the following templates and/or ".m" files:
```

```
File: C:\Program  
Files\Symantec\ESM\register\win2003\db2module_w.m.gz
```

Description: ESM db2module_w.m module definition file

File: C:\Program
Files\Symantec\ESM\register\win2003\i18n\db2module_w.m.gz

Description: ESM i18n/db2module_w.m module definition file

File: C:\Program
Files\Symantec\ESM\register\win2003\db2auditconfig_w.m.gz

Description: ESM db2auditconfig_w.m module definition file

File: C:\Program
Files\Symantec\ESM\register\win2003\i18n\db2auditconfig_w.m.gz

Description: ESM i18n/db2auditconfig_w.m module definition
file

File: C:\Program
Files\Symantec\ESM\register\win2003\db2patch_w.m.gz

Description: ESM db2patch_w.m module definition file

File: C:\Program
Files\Symantec\ESM\register\win2003\i18n\db2patch_w.m.gz

Description: ESM i18n/db2patch_w.m module definition file

File: C:\Program
Files\Symantec\ESM\template\win2003\patchdb2.wdb.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: esmmanager

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

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

Password: *****

Enter the network protocol used to contact the ESM manager.

1) IPX

2) TCP

Enter 1 or 2 [2]:

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

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

ESM Manager : esmmanager

ESM user name : ESM

Protocol : TCP

Port : 5600

ESM agent : esmagent

Is this information correct? [yes]

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\mtpkreg.exe.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\db2module.exe.gz...

Extracting C:\Program
Files\Symantec\ESM\register\win2003\db2module_w.m.gz...

Extracting C:\Program
Files\Symantec\ESM\register\win2003\i18n\db2module_w.m.gz.

..

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\db2auditconfig.exe.gz...

Extracting C:\Program
Files\Symantec\ESM\register\win2003\db2auditconfig_w.m.gz.

..

Extracting C:\Program
Files\Symantec\ESM\register\win2003\i18n\db2auditconfig_w.
m.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\db2patch.exe.gz...

```
Extracting C:\Program
Files\Symantec\ESM\register\win2003\db2patch_w.m.gz...

Extracting C:\Program
Files\Symantec\ESM\register\win2003\i18n\db2patch_w.m.gz..
.

Extracting C:\Program
Files\Symantec\ESM\template\win2003\patchdb2.wdb.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\DB2Collector.exe.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\SnapshotCollector.exe.gz..
.

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\db2module.rete.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w3s-
ix86\DB2Setup.exe.gz...

Continue and add configuration records to enable ESM security
checking
for your DB2 database? [yes]
The ESM DB2 Module setup program has found the following database:

DB2 database alias : DB1

Would you like to add a configuration record for this database?
[yes]

DB2 database alias [DB1]:

DB2 instance name : inst1

User ID used to log on to the DB2 database: user

Enter the password used to log on to the DB2 database.
Password          : *****

Re-Enter password: *****

DB2 database alias : DB1
DB2 instance name  : inst1
DB2 database login : 18CD49D37CF43C5722D02BE1
```

Password : 7F664B1ADB0459D1AD652385

Is this information correct? [yes]

The ESM DB2 Module setup program has found the following database:

DB2 database alias : DB2

Would you like to add a configuration record for this database?
[yes]

DB2 database alias [DB2]:

DB2 instance name : inst2

User ID used to log on to the DB2 database: user

Enter the password used to log on to the DB2 database.

Password : *****

Re-Enter password: *****

DB2 database alias : DB2

DB2 instance name : inst2

DB2 database login : 65FF4C60A30CE6DF316E5450

Password : 4C974DA71E66F68220199855

Is this information correct? [yes]

The ESM DB2 Module setup program has found the following database:

DB2 database alias : DB3

Would you like to add a configuration record for this database?
[yes] no

*** Configuration records ***

DB2 database alias : DB1

DB2 instance name : inst1

DB2 database login : 5AE34D628B2715587FC993AE

Password : 417B4EA968EA0DB6403E9669

```
===   ===  
DB2 database alias : DB2  
DB2 instance name  : inst1  
DB2 database login : 28144FEF79CA248768F1373D  
Password           : 0EAD5136753B80A1673B7254  
    ***   ***   ***   ***  
  
Options:  
    1) Add a new configuration record  
    2) Modify/remove existing configuration records  
    3) Exit  
  
Enter option number [3]:  
  
Tune-up pack installation complete  
Re-registering modules/template files... Please wait...  
End of installation  
    Press <return> to exit ESM tuneup pack
```

Silently installing the IBM DB2 module on Windows

You can silently install the IBM DB2 module on Windows operating systems by using `esmdb2tpi.exe`.

[Table 1-4](#) lists the command line options for silently installing the IBM DB2 module on Windows operating systems:

Table 1-4 Options to silently install the IBM DB2 module on Windows

| Option | Description |
|--------|--|
| -i | Install this tune-up/third-party package. |
| -d | Display the description and contents of this tune-up/third-party package. |
| -U | Specify the ESM access record name. |
| -e | Don't execute the before and after executables (installation without configuration). |
| -P | Specify the ESM access record password. |
| -p | Specify the TCP port to use. |

Table 1-4 Options to silently install the IBM DB2 module on Windows

| Option | Description |
|--------|---|
| -m | Specify the ESM manager name. |
| -t | Connect to the ESM manager by using TCP. |
| -x | Connect to the ESM manager by using IPX (Windows only). |
| -g | Specify the ESM agent name to use for registration. |
| -K | Do not prompt for and do the re-registration of the agents. |
| -n | No return is required to exit the tune-up package (Windows only). |
| -N | Do not update the report content file on the manager. |
| -Y | Update the report content file on the manager. |

For example,

```
esmdb2tpi.exe -it -m <Manager Name> -U <Username> -p <5600> -P
<password> -g <Agent Name> -e
```

Installing the IBM DB2 module on Linux, Solaris, or AIX

Perform step 1 to 10 mentioned in the [Installing the IBM DB2 module on Windows](#) section. When the configuration is complete, you will be asked if you want to add configuration records to enable ESM security checking for your IBM DB2 instances.

To enable security checking for your IBM DB2 instances

- When the extraction is complete, you will be asked if you want to add configuration records to enable ESM security checking for your IBM DB2.
 - Type Y to continue the installation and enable security checking for your instances.
 - Type N to end the installation without configuring any module. If you type Y, you can configure the IBM DB2 Remote module.

To configure the IBM DB2 Remote module

- You will be asked if you want to Configure DB2 Remote module.
 - To continue configuration of IBM DB2 Remote module, type Y.
- Enter the IBM DB2 database alias.

- 3 Enter the IBM DB2 instance name.
- 4 Enter the User ID to log on to the IBM DB2 database.
- 5 Enter the password to log on to the IBM DB2 database.
- 6 Is this information correct?
 - Type Y to save the configuration record and continue with the next database.
 - Type N to begin again with the same instance.The IBM DB2 User ID and password are encrypted when they are displayed for your approval.
- 7 Repeat steps 1 - 6 to configure another database.

After you have created configuration records for each database, the program lists all of the configuration records and the following options:

 - Option 1: to create a new configuration record database.
 - Option 2: to modify or remove an existing configuration record.
 - Option 3: to finish the installation and exit the program.

Note: The encryption that is used to store the credentials in disk file is OpenSSL AES algorithm.

To configure the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules

- 1 You will be asked if you want to Configure IBM DB2 Audit Configuration and the IBM DB2 Fix Packs module.
 - Type Y to continue the IBM DB2 Audit Configuration and IBM DB2 Fix Packs modules configuration.
 - Type N to end the installation without configuration.
- 2 Enter the IBM DB2 instance name.
- 3 Enter the user with SYSADM authority.
- 4 Is this information correct?
 - Type Y to save the configuration record and continue with the next instance.
 - Type N to begin again with the same instance.
- 5 Repeat steps 1- 4 for each IBM DB2 instance.
- 6 After you have created configuration records for each instance, the program lists all of the configuration records and the following options:
 - Option 1: to create a new configuration record for an instance.

- Option 2: to modify or remove an existing configuration record.
- Option 3: to finish the installation and exit the program.

Linux, AIX, and Solaris installation log

The following log is an example of an ESM Modules for IBM DB2 Universal Databases installed on Linux, Solaris, or AIX. Your log may look different, depending on how your manager and agents are configured.

Symantec Corporation tune-up/installation package

Options:

- 1) Display the description and contents of the tune-up/installation package
- 2) Install the tune-up/installation package on your system
- 3) Quit

Enter option number [1]: 2

Installing package: ESM modules for DB2 2.0.1

Tuneup pack will overlay ESM modules for DB2 version 2.0 with version 2.0.1

This package includes the following templates and/or ".m" files:

File: /esm/register/unix/db2auditconfig.m.gz
Description: ESM DB2 Audit Configuration module definition file

File: /esm/register/unix/db2patch.m.gz
Description: ESM DB2 Patch module definition file

File: /esm/register/unix/db2module.m.gz
Description: ESM DB2 Remote module definition file

File: /esm/register/unix/i18n/db2auditconfig.m.gz
Description: ESM DB2 Audit Configuration module definition file

File: /esm/register/unix/i18n/db2patch.m.gz
Description: ESM DB2 Patch module definition file

```
File: /esm/register/unix/i18n/db2module.m.gz
Description:      ESM DB2 Remote module definition file
```

```
File: /esm/template/unix/patchdb2.wdb.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: esmmanager

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 [esmagent]: esmagent

```
ESM Manager      : esmmanager
ESM user name    : ESM
Protocol         : TCP
Port             : 5600
ESM agent        : esmagent
```

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/bin/lnx-x86/db2auditconfig.gz...
Extracting /esm/bin/lnx-x86/db2patch.gz...
Extracting /esm/bin/lnx-x86/db2module.gz...
Extracting /esm/register/unix/db2auditconfig.m.gz...
Extracting /esm/register/unix/db2patch.m.gz...
Extracting /esm/register/unix/db2module.m.gz...
Extracting /esm/register/unix/i18n/db2auditconfig.m.gz...
Extracting /esm/register/unix/i18n/db2patch.m.gz...
Extracting /esm/register/unix/i18n/db2module.m.gz...
Extracting /esm/template/unix/patchdb2.wdb.gz...
Extracting /esm/bin/lnx-x86/db2setup.gz...
Extracting /esm/bin/lnx-x86/DB2Collector.gz...
Extracting /esm/bin/lnx-x86/SnapshotCollector.gz...
Extracting /esm/bin/lnx-x86/db2module.rete.gz...
Continue and add configuration records to enable ESM security
checking
for your DB2? [yes]
```

Configure DB2 Remote module? [yes] yes

DB2 database alias: DB1

DB2 instance name : inst1

User ID used to log on to the DB2 database: user

Enter the password used to log on to the DB2 database.

Password :

Re-Enter password:

DB2 database alias : DB1

DB2 instance name : inst1

DB2 database login : 7F225B1C17EB1E5E49984EC6

Password : 6606C4D31E215F4120668B7A

Is this information correct? [yes]

Would you like to add configuration record for another database?
[yes]

DB2 database alias: DB2

DB2 instance name : inst2

User ID used to log on to the DB2 database: user

Enter the password used to log on to the DB2 database.

Password :

Re-Enter password:

DB2 database alias : DB2

DB2 instance name : inst2

DB2 database login : D95A39B167D552376D18408B

Password : 350CDFE52D0559AF74256E9D

Is this information correct? [yes]

Would you like to add configuration record for another database?
[yes] no

*** Configuration records ***

DB2 database alias : DB1

DB2 instance name : inst1

DB2 database login : 12B363D54275F2B66814D52B

Password : 396CFC330C75B24EB3E160D3

=== ===

DB2 database alias : DB2

DB2 instance name : inst2

DB2 database login : 21CC565F98DDA8CC28929D64

Password : 48B6C8EC9FE0FACE85327CAF

*** **

Options:

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

Enter option number [3]:

Configure DB2 Audit Configuration and DB2 Fix Packs modules? [yes] yes

Enter the instance name: inst1

Enter the user with SYSADM privileges: user

Instance Name : inst1

User with SYSADM privilege : user

Is this information correct? [yes]

Would you like to configure another instance? [yes] yes

Enter the instance name: inst2

Enter the user with SYSADM privileges: user

Instance Name : inst2

User with SYSADM privilege : user

Is this information correct? [yes]

Would you like to configure another instance? [yes] no

Configured Instance:

Instance Name : inst1

User with SYSADM privilege : user

Instance Name : inst2

User with SYSADM privilege : user

Options:

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

```
Enter option number [3]:
```

```
Tune-up pack installation complete  
Extracting /esm/config/su/65/manifest.xml.gz...  
Re-registering modules/template files... Please wait...  
  
End of installation.
```

Silently installing the IBM DB2 module on Linux, Solaris, or AIX

You can silently install the IBM DB2 module on Linux, Solaris, or AIX operating systems by using `esmdb2.tpi`.

[Table 1-5](#) lists the command line options for silently installing the IBM DB2 module on Linux, Solaris, or AIX operating systems:

Table 1-5 Options to silently install the IBM DB2 module on Linux, Solaris, or AIX

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

Table 1-5 Options to silently install the IBM DB2 module on Linux, Solaris, or AIX

| Option | Description |
|--------|--|
| -Y | Update the report content file on the manager. |

For example,

```
esmdb2.tpi -it -m <Manager Name> -U <Username> -p <5600> -P <password> -g <Agent Name> -e
```

Configuring the IBM DB2 Remote module on Windows, Linux, Solaris, and AIX

After installing the IBM DB2 module on Windows, Linux, Solaris, and AIX, you can edit the configuration records using the DB2Setup.exe. A configuration record is created for each database alias when you enable security checking during installation.

Editing the configuration records

You can add, modify, or remove the IBM DB2 database instances that ESM includes in security checks by using the DB2Setup.exe program. By default, DB2Setup.exe is located in the \\<InstallDir>\ESM\bin\<platform>\ directory.

Run DB2Setup.exe on the IBM DB2 Remote modules that are installed on Windows, Linux, Solaris, or AIX with the following options:

Table 1-6 Options for silently configuring the IBM DB2 Remote modules that are installed on Windows, Linux, Solaris, or AIX

| To do this | Type |
|---|----------------------------|
| Display Help | DB2Setup -h |
| Create configuration records for detected DB2 databases. | DB2Setup -c |
| Add new configuration records for undetected DB2 databases. | DB2Setup -a |
| Modify or remove existing DB2 database configuration records. | DB2Setup -m |
| List existing DB2 database configuration records. | DB2Setup -l |
| Setup overwrites the default file with configuration records and writes it into -of file. | DB2Setup -c -of <filename> |

Table 1-6 Options for silently configuring the IBM DB2 Remote modules that are installed on Windows, Linux, Solaris, or AIX

| To do this | Type |
|--|--|
| Setup reads from -if file and add a new record in the default file. The default file is \\Install directory\Symantec\ESM\config\DB2Module.dat. | DB2Setup -a -if <filename> |
| Setup reads from the default file and adds a new record in -of file. The default file is \\InstallDirectory\ESM\config\DB2Module.dat. | DB2Setup -a -of <filename> |
| Setup reads from -if file and add a new record in the -of file. | DB2Setup -a -if <filename>-of <filename> |
| Setup reads from -if file and add the modified records in the default file. | DB2Setup -m -if <filename> |
| Setup reads from the default file and add the modified records in the -of file. | DB2Setup -m -of <filename> |
| Setup reads from -if file and add the modified records in the -of file. | DB2Setup -m -if <filename>-of <filename> |

Silently configuring the IBM DB2 Remote module

You can silently configure the IBM DB2 Remote module by using the DB2Setup.exe.

Use the following option to configure the IBM DB2 Remote module silently on Linux, Solaris, or AIX:

Table 1-7 Options for silent installation of the IBM DB2 Remote module

| Options | Description |
|---------|---|
| -q | Silently configure the DB2 Remote module. |
| -D | Specify the database name. |
| -I | Specify the instance name. |
| -U | Specify the username. |
| -P | Specify the password. |

For example,

```
db2setup -q -D <database name> -I <instance name> -U <username> -P <password>
```

Configuring the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules on Linux, Solaris, and AIX

After installing the IBM DB2 Audit Configuration and Fix Packs modules on Linux, Solaris, and AIX, you can edit the configuration records using the DB2Setup.exe. A configuration record is created for each database alias when you enable security checking during installation.

Editing the configuration records

You can add, modify, or remove the IBM DB2 database instances that ESM includes in security checks by using the DB2Setup.exe program. By default, DB2Setup.exe is located in the \\<InstallDir>\ESM\bin\<platform>\ directory.

Run DB2Setup.exe on the IBM DB2 Audit Configuration and the Fix Pack modules that are installed on Linux, Solaris, or AIX with the following options:

Table 1-8 Editing configuration records for the Audit Configuration and Fix Packs modules

| To do this | Type |
|--|----------------------------|
| Create configuration records for DB instance. | DB2Setup -H -c |
| Add new configuration record for DB2 instance. | DB2Setup -H -a |
| Modify existing DB2 instance configuration records. | DB2Setup -H -m |
| List existing DB2 instance configuration records. | DB2Setup -H -l |
| Specify a new input file for DB2 instance configuration records. The default file is \\ProgramFiles\Symantec\ESM\config\DB2ModulePath.dat. | DB2Setup -H -if <filename> |
| Specify a new output file for DB2 database configuration records. The default file is \\ProgramFiles\Symantec\ESM\config\DB2ModulePath.dat. | DB2Setup -H -of <filename> |
| Setup reads from -if file and add a new record in the default file. The default file is \\ProgramFiles\Symantec\ESM\config\DB2ModulePath.dat. | DB2Setup -a -if <filename> |
| Setup reads from the default file and adds a new record in -of file. The default file is \\ProgramFiles\Symantec\ESM\config\DB2ModulePath.dat. | DB2Setup -a -of <filename> |

Table 1-8 Editing configuration records for the Audit Configuration and Fix Packs modules

| To do this | Type |
|---|--|
| Setup reads from -if file and add a new record in the -of file. | DB2Setup -a -if <filename>-of <filename> |
| Setup reads from -if file and add the modified records in the default file. | DB2Setup -m -if <filename> |
| Setup reads from the default file and add the modified records in the -of file. | DB2Setup -m -of <filename> |
| Setup reads from -if file and add the modified records in the -of file. | DB2Setup -m -if <filename>-of <filename> |

Silently configuring the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules

You can silently configure the IBM DB2 Audit Configuration and the IBM DB2 Fix Packs modules by using the DB2Setup.exe.

Use the following option to configure the IBM DB2 module silently for the DB2 Audit Configuration and Fix Packs modules that are installed on Linux, Solaris, or AIX:

Table 1-9 Options for silently configuring the IBM DB2 module for Audit Configuration and Fix Packs modules

| -q -H | Silently configure the DB2 Audit Configuration module and the DB2 Fix Packs modules. |
|-------|--|
| -N | Specify the host instance name. |
| -A | Specify the user having SYSADM authority. |

For example,

db2setup -q -H -N <instance name> -A <username>

Creating a baseline snapshot

To establish a baseline for IBM DB2 module security checks, create a new IBM DB2 remote policy with snapshot-related checks enabled. Running this policy creates

snapshots of current account information that you can update when you run checks for new, deleted, or modified information.

Run the module one time to create the snapshots, then rerun the module to detect changes between policy runs.

After running a policy, you can update the snapshots directly from messages in the Policy Run report by right-clicking on a modified, deleted, or new report message.

Understanding the DB2 Audit Configuration module

This chapter includes the following topics:

- [About the DB2 Audit Configuration module](#)
- [Event Types](#)
- [Audit Database Events](#)
- [Audit Miscellaneous Events](#)

About the DB2 Audit Configuration module

The DB2 Audit Configuration module reports the current audit configuration information and its status on the computer where the DB2 server is configured.

The DB2 Audit Configuration module is a host-based module. This module does not report on the DB2 remote servers.

The DB2 Audit Configuration module reports on DB2 instance in case of Red Hat Linux, AIX, or Solaris, and on DB2 Copy for Windows.

Note: If the ESM agent has only the DB2 Administration client installed, the module reports on the audit settings of the client.

DB2 Audit Configuration module lets you generate reports based on various events and event types.

Auditing Enabled

The Auditing Enabled check reports whether auditing is enabled on the DB2 server.

Table 2-1 Auditing Enabled message

| Message Name | Title | Class |
|------------------|------------------|-------|
| ESM_AUDIT_ACTIVE | DB2 Audit Status | 4 |

Event Types

The checks included in the Events Types group let you specify which types of events you want to audit. You can also specify whether only successful or failed events, or both, should be logged.

Audit Failure Events

The Audit Failure Events check reports whether DB2 databases logs error events.

Table 2-2 Audit Failure messages

| Message Name | Title | Class |
|-----------------------|-------------------------|-------|
| ESM_LOG_ERROR | Auditing Failure Events | 4 |
| ESM_LOG_ERROR_WARNING | Auditing Failure Events | 4 |

Audit Success Events

The Audit Success Events check reports whether DB2 databases logs success events.

Table 2-3 Audit Success Events messages

| Message Name | Title | Class |
|---------------------------------|-------------------------|-------|
| ESM_LOG_SUCCESS | Auditing Success Events | 4 |
| ESM_LOG_SUCCESS_WARNING | Audit Success events | 4 |
| ESM_LOG_SUCCESS_ENABLED_WARNING | Audit Success events | 1 |

Audit Database Events

The checks included in the Audit Database Events group verify which DB2 database events are audited.

Auditing Related Events

The Auditing Related Events check reports whether DB2 databases logs audit events.

Table 2-4 Audit Auditing Related Events messages

| Message Name | Title | Class |
|-----------------------|-------------------------------|-------|
| ESM_LOG_AUDIT | Audit auditing related events | 4 |
| ESM_LOG_AUDIT_WARNING | Audit auditing related events | 4 |

Checking Events

The Checking Events check reports whether DB2 databases logs checking events.

Table 2-5 Audit Checking Events messages

| Message Name | Title | Class |
|--------------------------|-----------------------|-------|
| ESM_LOG_CHECKING | Audit Checking events | 4 |
| ESM_LOG_CHECKING_WARNING | Audit Checking Events | 4 |

Object Maintenance Events

The Object Maintenance Events check reports whether DB2 databases logs Object Maintenance events.

Table 2-6 Audit Object Maintenance Events messages

| Message Name | Title | Class |
|--------------------------|---------------------------------|-------|
| ESM_LOG_OBJMAINT | Audit Object Maintenance events | 4 |
| ESM_LOG_OBJMAINT_WARNING | Audit Object Maintenance events | 4 |

Security Maintenance Events

The Security Maintenance Events check reports whether DB2 databases logs Security Maintenance events.

Table 2-7 Audit Security Maintenance Events messages

| Message Name | Title | Class |
|--------------------------|-----------------------------------|-------|
| ESM_LOG_SECMAINT | Audit Security Maintenance events | 4 |
| ESM_LOG_SECMAINT_WARNING | Audit Security Maintenance events | 4 |

System Administrator Events

The System Administrator Events check reports whether DB2 databases logs System Administrator events.

Table 2-8 Audit System Administrator Events messages

| Message Name | Title | Class |
|------------------------|-----------------------------------|-------|
| ESM_LOG_SYSADM | Audit System Administrator events | 4 |
| ESM_LOG_SYSADM_WARNING | Audit System Administrator events | 4 |

Validate Events

The Validate Events check reports whether DB2 databases logs Validate events.

Table 2-9 Audit Validate Events messages

| Message Name | Title | Class |
|--------------------------|-----------------------|-------|
| ESM_LOG_VALIDATE | Audit Validate events | 4 |
| ESM_LOG_VALIDATE_WARNING | Audit Validate events | 4 |

Context Events

The Context Events check reports whether DB2 databases logs Context events.

Table 2-10 Audit Context Events messages

| Message Name | Title | Class |
|-------------------------|----------------------|-------|
| ESM_LOG_CONTEXT | Audit context events | 4 |
| ESM_LOG_CONTEXT_WARNING | Audit Context events | 4 |

Error Handling Facility

The Error Handling Facility check reports whether DB2 databases have the audit facility parameter set to Audit. You have the option to specify whether audit facility errors are returned to the user (AUDIT) or ignored (NORMAL).

The Errortype parameter defines errors that either are returned to the user or are ignored. The following options are defined for the ERRORTYPE option:

Audit - Transactions succeed only if the appropriate audit record is written to the audit log.

Normal - Transactions succeed regardless of the audit status. The application continues with normal processing and programmatically defined termination.

Table 2-11 Audit Facility For Error Handling message

| Message Name | Title | Class |
|-------------------|-----------------------------------|-------|
| ESM_LOG_ERRORTYPE | Audit Facility For Error Handling | 4 |

Audit Miscellaneous Events

The checks included in the Audit Miscellaneous Events group verify which DB2 database miscellaneous events are audited.

Instance Startup and Shutdown

The Instance Startup and Shutdown check reports whether DB2 databases log the startup and shutdown events of instances.

Table 2-12 Audit Instance startup and shutdown messages

| Message Name | Title | Class |
|----------------------------------|-------------------------------------|-------|
| ESM_LOG_INSTANCE_UP_DOWN | Audit Instance startup and shutdown | 4 |
| ESM_LOG_INSTANCE_UP_DOWN_WARNING | Audit Instance startup and shutdown | 4 |

Changes To Configuration Parameters

The Changes To Configuration Parameters check reports whether DB2 databases log the changes made to instance and database configuration parameters.

Table 2-13 Audit changes to configuration parameters messages

| Message Name | Title | Class |
|----------------------------|--|-------|
| ESM_LOG_DB_DBM_CFG | Audit changes made to instance and database configuration parameters | 4 |
| ESM_LOG_DB_DBM_CFG_WARNING | Audit changes made to instance and database configuration parameters | 4 |

Database Activation and Deactivation

The Database Activation and Deactivation check reports whether DB2 databases log database activation and deactivation.

Table 2-14 Audit database activation and deactivation messages

| Message Name | Title | Class |
|------------------------------|--|-------|
| ESM_LOG_DB_ACT_DEACT | Audit database activation and deactivation | 4 |
| ESM_LOG_DB_ACT_DEACT_WARNING | Audit database activation and deactivation | 4 |

Use of SYSADM, DBADM, SYSCTRL, and SYSMANT

The Use of SYSADM, DBADM, SYSCTRL, and SYSMANT check reports whether DB2 databases log the use of SYSADM, DBADM, SYSCTRL, and SYSMANT.

Table 2-15 Audit use of SYSADM,DBADM,SYSCTRL,SYSMANT messages

| Message Name | Title | Class |
|------------------------|---|-------|
| ESM_LOG_ADMINS | Audit Use of SYSADM,DBADM,SYSCTRL,SYSMANT | 4 |
| ESM_LOG_ADMINS_WARNING | Audit Use of SYSADM,DBADM,SYSCTRL,SYSMANT | 4 |

Attempted Access To Restricted Objects

The Attempted Access To Restricted Objects check reports whether DB2 databases log the attempted access to restricted objects defined by information owner.

Table 2-16 Audit attempted access to restricted objects messages

| Message Name | Title | Class |
|--------------------------------|---|-------|
| ESM_LOG_RESTRICTED_OBJ | Audit attempted access to restricted objects defined by Information owner | 4 |
| ESM_LOG_RESTRICTED_OBJ_WARNING | Audit attempted access to restricted objects defined by Information owner | 4 |

Access To Sensitive Objects and/or Tables

The Access To Sensitive Objects and/or Tables check reports whether DB2 databases log the access to sensitive Objects and/or Tables defined by Information owner.

Table 2-17 Audit access to sensitive Objects and/or Tables messages

| Message Name | Title | Class |
|-----------------------|--|-------|
| ESM_LOG_SENSITIVE_OBJ | Audit access to sensitive Objects and/or Tables defined by Information owner | 4 |

Table 2-17 Audit access to sensitive Objects and/or Tables messages

| Message Name | Title | Class |
|-------------------------------|--|-------|
| ESM_LOG_SENSITIVE_OBJ_WARNING | Audit access to sensitive Objects and/or Tables defined by Information owner | 4 |

Unsuccessful Connection Attempts

The Unsuccessful Connection Attempts check reports whether DB2 databases log the non-successful connection attempts from all users.

Table 2-18 Audit non-successful connection attempts messages

| Message Name | Title | Class |
|-----------------------------|---|-------|
| ESM_LOG_FAILED_CONN | Audit non-successful connection attempts from all users | 4 |
| ESM_LOG_FAILED_CONN_WARNING | Audit non-successful connection attempts from all users | 4 |

Administrative Functions Performed

The Administrative Functions Performed check reports whether DB2 databases log the administrative functions performed by all users against database permissions granted to accounts or groups.

Table 2-19 Audit administrative functions performed messages

| Message Name | Title | Class |
|---------------------------|--|-------|
| ESM_LOG_ADMIN_FNS | Audit administrative functions performed by all users against database permissions granted to accounts or groups | 4 |
| ESM_LOG_ADMIN_FNS_WARNING | Audit administrative functions performed by all users against database permissions granted to accounts or groups | 4 |

Understanding the IBM DB2 Fix Packs module

This chapter includes the following topics:

- [About the IBM DB2 Fix Packs module](#)

About the IBM DB2 Fix Packs module

This module reports if the current IBM DB2 level on the IBM DB2 server needs to be upgraded to the latest IBM DB2 fix pack.

The IBM DB2 Fix Packs module is a host-based module. The Fix Packs module does not report on the IBM DB2 remote servers.

The DB2 Audit Configuration module reports on DB2 instance in case of Red Hat Linux, AIX, or Solaris, and on DB2 Copy for Windows.

Note: If the ESM agent has only the DB2 Administration client installed, the module reports on the client.

Template files

This check reports the information on the specific template files that are to be included for the checks. This check compares the existing IBM DB2 level on the

IBM DB2 server with the latest fix pack available in the template file and reports the difference.

Table 3-1 Template files messages

| Message | Name | Title Class |
|--------------------------|---|-------------|
| DB2_TEMPLATEFILE_MISSING | No template files specified | 4 |
| DB2_REQUIRED_FIXPACK | Required DB2 Fix Pack for your computer | 4 |
| DB2_CONFIG_ERR | Configuration Error | 4 |

Installed Fix Packs

This check reports the fix packs that are installed on the IBM DB2 server. This check also reports the details of the IBM DB2 level on the IBM DB2 server.

Table 3-2 Installed Fix Pack messages

| Message | Name | Title Class |
|-----------------------|---|-------------|
| DB2_INSTALLED_FIXPACK | Installed DB2 Fix Pack on your computer | 0 |
| DB2_CONFIG_ERR | Configuration Error | 4 |

Understanding the IBM DB2 Remote module

This chapter includes the following topics:

- [About the IBM DB2 Remote module](#)
- [Discovery mode](#)
- [System authorities](#)
- [Database privileges](#)

About the IBM DB2 Remote module

The IBM DB2 Remote module includes checks that specify database aliases to be checked, examine authentication methods, and list the current DB2 version and operating system.

The IBM DB2 Remote module works as host-based on Linux, Solaris, and AIX, and network-based on Windows machines.

IBM DB2 Database Aliases

Configuration records are created during the IBM DB2 Remote module installation to enable security checking for each of your databases. Also, you may have added new configuration records after installation using DB2Setup.exe. See [“Installing the IBM DB2 module on Windows”](#) on page 9.

By default, ESM examines every IBM DB2 database alias for which there exists a configuration record. Use the IBM DB2 Database Aliases option to specify included or excluded database aliases that you want to check. If the name list is empty, all databases are checked.

To include one or more database aliases:

- 1 Enter names in the name list.
- 2 Select Include.

To exclude one or more database aliases:

- 1 Enter names in the name list.
- 2 Select Exclude.

Note: ESM stores IBM DB2 database configuration records in the
\\Program Files\Symantec\ESM\config\DB2Module.dat file.

Authentication from the Server

This check examines the way users are authenticated. Your database is most secure if users are authenticated from the server side rather than the client side.

Use the Authorized Setting name list to specify the authorized authentication methods. The Authorized Setting name list includes by default the recommended authentication methods SERVER and SERVER_ENCRYPT.

Table 4-1 Authentication from the Server message

| Message Name | Title | Class |
|--------------------------------|------------------------------------|-------|
| INVALID_AUTHENTICATION_SETTING | Invalid DB2 Authentication setting | 4 |

DB2 Version and OS

This check reports the DB2 database version and operating system.

Table 4-2 DB2 Version and OS message

| Message Name | Title | Class |
|----------------|--------------------|-------|
| DB2_VERSION_OS | DB2 Version and OS | 0 |

Discovery mode

Discovery mode is a IBM DB2 feature that is used to gather information from IBM DB2 servers located on a network. The ESM Modules for IBM DB2 Universal Databases includes checks that verify if a server, instance, or database is running in discovery mode.

Server Discovery Mode

This check examines the discovery mode setting for the IBM DB2 server.

Use the Server Discovery Mode name list to specify allowed the discovery mode action parameters. By default, the Server Discovery Mode name list contains DISABLE and KNOWN.

After running this check, the Policy Run report lists all discovery mode action parameters that are not in the name list.

Table 4-3 Server Discovery Mode message

| Message Name | Title | Class |
|-----------------|---------------------------|-------|
| SERVER_DIS_MODE | DB2 Server Discovery Mode | 1 |

Instance Discovery Mode

This check examines the discovery mode setting for IBM DB2 instances.

Use the Instance Discovery Mode name list to specify the allowed discovery mode action parameters. By default, the Instance Discovery Mode name list contains DISABLE.

After running this check, the Policy Run report lists all discovery mode action parameters that are not in the name list.

Table 4-4 Instance Discovery Mode message

| Message Name | Title | Class |
|-------------------|-----------------------------|-------|
| INSTANCE_DIS_MODE | DB2 Instance Discovery Mode | 1 |

Database Discovery Mode

This check examines the discovery mode setting for IBM DB2 databases.

Use the Database Discovery Mode name list to specify the allowed discovery mode action parameters. By default, the Database Discovery Mode name list contains DISABLE.

After running this check, the Policy Run report lists all discovery mode action parameters that are not in the name list.

Table 4-5 Database Discovery Mode message

| Message Name | Title | Class |
|-------------------|-----------------------------|-------|
| DATABASE_DIS_MODE | DB2 Database Discovery Mode | 1 |

System authorities

The IBM DB2 Remote module lets you to maintain lists of groups and users that have been granted IBM DB2 authorities. The checks create reports of unauthorized groups and users. The module also includes checks that report new, modified, and deleted groups and users that have been granted authorities.

Unauthorized Group Set in System Administrator Authority

This check reports groups that have been granted the System Administrator Authority but that are not authorized to have it.

Use the Authorized Groups name list to exclude all groups that are authorized to have the System Administrator Authority.

After running this check, the Policy Run report lists groups that have the System Administrator Authority and that are not in the Authorized Groups name list.

Table 4-6 Unauthorized System Administrator Authority message

| Message Name | Title | Class |
|---------------------|---|-------|
| UNAUTH_SYSADM_GROUP | Unauthorized group set for System Administrator Authority | 3 |

Unauthorized Group Set in System Control Authority

This check reports groups that have been granted the System Control Authority but that are not authorized to have it.

Use the Authorized Groups name list to exclude all groups that are authorized to have the System Control Authority.

After running this check, the Policy Run report lists groups that have the System Control Authority and that are not in the Authorized Groups name list.

Table 4-7 Unauthorized System Control Authority message

| Message Name | Title | Class |
|---------------------|---|-------|
| UNAUTH_SYCTRL_GROUP | Unauthorized group set for System Control Authority | 3 |

Unauthorized Group Set in System Maintenance Authority

This check reports groups that have been granted the System Maintenance Authority but that are not authorized to have it.

Use the Authorized Groups name list to exclude all groups that are authorized to have the System Maintenance Authority.

After running this check, the Policy Run report lists groups that have the System Maintenance Authority and that are not in the Authorized Groups name list.

Table 4-8 Unauthorized System Maintenance Authority message

| Message Name | Title | Class |
|------------------------|---|-------|
| UNAUTH_SYSMMAINT_GROUP | Unauthorized group set for System Maintenance Authority | 3 |

Unauthorized Group/User in Database Administrator Authority

This check reports groups and users that have been granted the Database Administrator Authority but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the Database Administrator Authority.

After running this check, the Policy Run report lists groups and users that have the Database Administrator Authority and that are not in the Authorized Groups/Users name list.

Table 4-9 Unauthorized Database Administrator Authority message

| Message Name | Title | Class |
|----------------------------|--|-------|
| UNAUTH_GROUPUSER_DBADMAUTH | Unauthorized group/user set for Database Administrator Authority | 3 |

New Group/User in Database Administrator Authority

This check reports groups and users that were granted the Database Administrator Authority since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-10 New Group/User in Database Administrator Authority message

| Message Name | Title | Class |
|-------------------------|---|-------|
| NEW_GROUPUSER_DBADMAUTH | New group/user set for Database Administrator Authority | 2 |

If the detected user \or group is authorized to have this authority, update the snapshot. Revoke the authority if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in Database Administrator Authority

This check reports groups and users that had the Database Administrator Authority and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-11 Deleted Group/User in Database Administrator Authority message

| Message Name | Title | Class |
|-------------------------|---|-------|
| DEL_GROUPUSER_DBADMAUTH | Deleted group/user set for Database Administrator Authority | 2 |

If the deletion is authorized, update the snapshot. Restore the authority if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in Database Administrator Authority

This check reports groups and users with Database Administrator Authority “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

```
grantor changed to gwashington from fdouglas
```

Or a message might read:

```
granteetype changed to user from group
```

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-12 Modified Group/User in Database Administrator Authority message

| Message Name | Title | Class |
|-------------------------|--|-------|
| MOD_GROUPUSER_DBADMAUTH | Modified group/user set for Database Administrator Authority | 2 |

If the modification is authorized, update the snapshot. Restore the authority if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Unauthorized Group/User in LOAD Authority

This check reports groups and users that were granted the LOAD Authority but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the LOAD Authority.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-13 Unauthorized LOAD Authority message

| Message Name | Title | Class |
|---------------------------|--|-------|
| UNAUTH_GROUPUSER_LOADAUTH | Unauthorized group/user set for LOAD Authority | 3 |

New Group/User in LOAD Authority

This check reports groups and users that were granted the LOAD Authority since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-14 New Group/User in LOAD Authority message

| Message name | Title | Class |
|-----------------------|---------------------------------------|-------|
| NEW_GROUPUER_LOADAUTH | New group/user set for LOAD Authority | 2 |

If the detected user or group is authorized to have this authority, update the snapshot. Revoke the authority if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in LOAD Authority

This check reports groups and users that had the LOAD Authority and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-15 Deleted Group/User in LOAD Authority message

| Message Name | Title | Class |
|------------------------|---|-------|
| DEL_GROUPUSER_LOADAUTH | Deleted group/user set for LOAD Authority | 2 |

If the deletion is authorized, update the snapshot. Restore the authority if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in LOAD Authority

This check reports groups and users with LOAD Authority “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

```
grantor changed to gwashington from fdouglas
```

Or a message might read:

```
granteetype changed to user from group
```

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-16 Modified Group/User in LOAD Authority message

| Message Name | Title | Class |
|------------------------|--|-------|
| MOD_GROUPUSER_LOADAUTH | Modified group/user set for LOAD Authority | 2 |

If the modification is authorized, update the snapshot. Restore the authority if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Database privileges

The IBM DB2 Remote module lets you maintain lists of groups and users that have IBM DB2 database privileges. The checks create reports of groups and users that are unauthorized to have these privileges. The module also includes checks that report groups and users that have newly been granted database privileges, that have privileges modified, that have privileges revoked, or that have been deleted since the last snapshot updates.

Unauthorized Group/User in BINDADD Database Privilege

This check reports groups and users that have been granted the BINDADD Database Privilege but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the BINDADD Database Privilege.

After running this check, the Policy Run report lists groups and users that have the BINDADD Database Privilege and that are not in the Authorized Groups/Users name list.

Table 4-17 Unauthorized BINDADD Database Privilege message

| Message Name | Title | Class |
|------------------------------|--|-------|
| UNAUTH_GROUPUSER_BINDADDAUTH | Unauthorized group/user set for BINDADD Database Privilege | 3 |

New Group/User in BINDADD Database Privilege

This check reports groups and users that were granted the BINDADD Database Privilege since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-18 New Group/User in BINDADD Database Privilege message

| Message Name | Title | Class |
|---------------------------|---|-------|
| NEW_GROUPUSER_BINDADDAUTH | New group/user set for BINDADD Database Privilege | 2 |

If the detected user or group is authorized to have this privilege, update the snapshot. Revoke the privilege if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in BINDADD Database Privilege

This check reports groups and users that had the BINDADD Privilege and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-19 Deleted Group/User in BINDADD Privilege message

| Message Name | Title | Class |
|---------------------------|---|-------|
| DEL_GROUPUSER_BINDADDAUTH | Deleted group/user set for BINDADD Database Privilege | 2 |

If the deletion is authorized, update the snapshot. Restore the privilege if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in BINDADD Database Privilege

This check reports groups and users with BINDADD Database Privilege “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

```
grantor changed to gwashington from fdouglas
```

Or a message might read:

```
granteetype changed to user from group
```

Table 4-20 Modified Group/User in BINDADD Database Privilege message

| Message Name | Title | Class |
|---------------------------|--|-------|
| MOD_GROUPUSER_BINDADDAUTH | Modified group/user set for BINDADD Database Privilege | 2 |

If the modification is authorized, update the snapshot. Restore the privilege if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Unauthorized Group/User in CONNECT Database Privilege

This check reports groups and users that have been granted the CONNECT Database Privilege but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the CONNECT Database Privilege.

After running this check, the Policy Run report lists groups and users that have the CONNECT Database Privilege and that are not in the Authorized Groups/Users name list.

Table 4-21 Unauthorized CONNECT Database Privilege message

| Message Name | Title | Class |
|------------------------------|--|-------|
| UNAUTH_GROUPUSER_CONNECTAUTH | Unauthorized group/user set for CONNECT Database Privilege | 3 |

New Group/User in CONNECT Database Privilege

This check reports groups and users that were granted the CONNECT Database Privilege since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-22 New Group/User in CONNECT Privilege message

| Message Name | Title | Class |
|---------------------------|---|-------|
| NEW_GROUPUSER_CONNECTAUTH | New group/user set for CONNECT Database Privilege | 2 |

If the detected user or group is authorized to have this privilege, update the snapshot. Revoke the privilege if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in CONNECT Database Privilege

This check reports groups and users that had the CONNECT Database Privilege and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-23 Deleted Group/User in CONNECT Database Privilege message

| Message Name | Title | Class |
|---------------------------|---|-------|
| DEL_GROUPUSER_CONNECTAUTH | Deleted group/user set for CONNECT Database Privilege | 2 |

If the deletion is authorized, update the snapshot. Restore the privilege if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in CONNECT Database Privilege

This check reports groups and users with CONNECT Database Privilege “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

`grantor changed to gwashington from fdouglas`

Or a message might read:

`granteetype changed to user from group`

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-24 Modified Group/User in CONNECT Database Privilege message

| Message Name | Title | Class |
|---------------------------|--|-------|
| MOD_GROUPUSER_CONNECTAUTH | Modified group/user set for CONNECT Database Privilege | 2 |

If the modification is authorized, update the snapshot. Restore the privilege if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Unauthorized Group/User in CREATETAB Database Privilege

This check reports groups and users that have been granted the CREATETAB Database Privilege but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the CREATETAB Database Privilege.

After running this check, the Policy Run report lists groups and users that have the CREATETAB Database Privilege and that are not in the Authorized Groups/Users name list.

Table 4-25 Unauthorized CREATETAB Database Privilege message

| Message Name | Title | Class |
|--------------------------------|--|-------|
| UNAUTH_GROUPUSER_CREATETABAUTH | Unauthorized group/user set for CREATETAB Database Privilege | 3 |

New Group/User in CREATETAB Database Privilege

This check reports groups and users that were granted the CREATETAB Database Privilege since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-26 New CREATETAB Database Privilege message

| Message Name | Title | Class |
|-----------------------------|---|-------|
| NEW_GROUPUSER_CREATETABAUTH | New group/user set for CREATETAB Database Privilege | 2 |

If the detected user or group is authorized to have this privilege, update the snapshot. Revoke the privilege if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in CREATETAB Database Privilege

This check reports groups and users that had the CREATETAB Database Privilege and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-27 Deleted Group/User in CREATETAB Database Privilege message

| Message Name | Title | Class |
|-----------------------------|---|-------|
| DEL_GROUPUSER_CREATETABAUTH | Deleted group/user set for CREATETAB Database Privilege | 2 |

If the deletion is authorized, update the snapshot. Restore the privilege if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in CREATETAB Database Privilege

This check reports groups and users with CREATETAB Database Privilege “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

`grantor changed to gwashington from fdouglas`

Or a message might read:

`granteetype changed to user from group`

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-28 Modified Group/User in CREATETAB Database Privilege message

| Message Name | Title | Class |
|-----------------------------|--|-------|
| MOD_GROUPUSER_CREATETABAUTH | Modified group/user set for CREATETAB Database Privilege | 2 |

If the modification is authorized, update the snapshot. Restore the privilege if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Unauthorized Group/User in CREATE_NOT_FENCED Database Privilege

This check reports groups and users that have been granted the CREATE_NOT_FENCED Database Privilege but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the CREATE_NOT_FENCED Database Privilege.

After running this check, the Policy Run report lists groups and users that have the CREATE_NOT_FENCED Database Privilege and that are not in the Authorized Groups/Users name list.

Table 4-29 Unauthorized CREATE_NOT_FENCED Privilege message

| Message Name | Title | Class |
|------------------------------|--|-------|
| UNAUTH_GROUPUSER_NOFENCEAUTH | Unauthorized group/user set for CREATE_NOT_FENCED Database Privilege | 3 |

New Group/User in CREATE_NOT_FENCED Database Privilege

This check reports groups and users that were granted the CREATE_NOT_FENCED Database Privilege since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-30 New CREATE_NOT_FENCED Database Privilege message

| Message Name | Title | Class |
|---------------------------|---|-------|
| NEW_GROUPUSER_NOFENCEAUTH | New group/user set for CREATE_NOT_FENCED Database Privilege | 2 |

If the detected user or group is authorized to have this privilege, update the snapshot. Revoke the privilege if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in CREATE_NOT_FENCED Database Privilege

This check reports groups and users that had the CREATE_NOT_FENCED Database Privilege and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-31 Deleted CREATE_NOT_FENCED Database Privilege message

| Message Name | Title | Class |
|---------------------------|---|-------|
| DEL_GROUPUSER_NOFENCEAUTH | Deleted group/user set for CREATE_NOT_FENCED Database Privilege | 2 |

If the deletion is authorized, update the snapshot. Restore the privilege if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in CREATE_NOT_FENCED Database Privilege

This check reports groups and users with CREATE_NOT_FENCED Database Privilege “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

```
grantor changed to gwashington from fdouglas
```

Or a message might read:

```
granteetype changed to user from group
```

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-32 Modified CREATE_NOT_FENCED Database Privilege message

| Message Name | Title | Class |
|---------------------------|--|-------|
| MOD_GROUPUSER_NOFENCEAUTH | Modified group/user set for CREATE_NOT_FENCED Database Privilege | 2 |

If the modification is authorized, update the snapshot. Restore the privilege if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Unauthorized Group/User in IMPLICIT_SCHEMA Database Privilege

This check reports groups and users that have been granted the IMPLICIT_SCHEMA Database Privilege but that are not authorized to have it.

Use the Authorized Groups/Users name list to exclude all groups and users that are authorized to have the IMPLICIT_SCHEMA Database Privilege.

After running this check, the Policy Run report lists groups and users that have the IMPLICIT_SCHEMA Database Privilege and that are not in the Authorized Groups/Users name list.

Table 4-33 Unauthorized IMPLICIT_SCHEMA Database Privilege message

| Message Name | Title | Class |
|---------------------------------|--|-------|
| UNAUTH_GROUPUSER_IMPLSCHEMAAUTH | Unauthorized group/user set for IMPLICIT_SCHEMA Database Privilege | 3 |

New Group/User in IMPLICIT_SCHEMA Database Privilege

This check reports groups and users that were granted the IMPLICIT_SCHEMA Database Privilege since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-34 New IMPLICIT_SCHEMA Database Privilege message

| Message Name | Title | Class |
|------------------------------|---|-------|
| NEW_GROUPUSER_IMPLSCHEMAAUTH | New group/user set for IMPLICIT_SCHEMA Database Privilege | 2 |

If the detected user or group is authorized to have this privilege, update the snapshot. Revoke the privilege if the detected user or group is not authorized.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Deleted Group/User in IMPLICIT_SCHEMA Database Privilege

This check reports groups and users that had the IMPLICIT_SCHEMA Database Privilege and had it revoked or that were deleted since the last snapshot updates.

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-35 Deleted IMPLICIT_SCHEMA Database Privilege message

| Message Name | Title | Class |
|------------------------------|---|-------|
| DEL_GROUPUSER_IMPLSCHEMAAUTH | Deleted group/user set for IMPLICIT_SCHEMA Database Privilege | 2 |

If the deletion is authorized, update the snapshot. Restore the privilege if it should not have been deleted.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Modified Group/User in IMPLICIT_SCHEMA Database Privilege

This check reports groups and users with IMPLICIT_SCHEMA Database Privilege “grantor” or “granteetype” changes since the last snapshot updates.

The Policy Run reports changes to the grantor and the granteetype. For example, a message might read:

```
grantor changed to gwashington from fdouglas
```

Or a message might read:

```
granteetype changed to user from group
```

Run the module one time to create the snapshot, then rerun the module to detect changes between policy runs.

Table 4-36 Modified IMPLICIT_SCHEMA Database Privilege message

| Message Name | Title | Class |
|------------------------------|--|-------|
| MOD_GROUPUSER_IMPLSCHEMAAUTH | Modified group/user set for IMPLICIT_SCHEMA Database Privilege | 2 |

If the modification is authorized, update the snapshot. Restore the privilege if it should not have been modified.

You can update the snapshot directly from the console grid by right-clicking on the Policy Run message.

Troubleshooting

This chapter includes the following topics:

- [Encryption exception](#)
- [DB2 Remote module errors](#)

Encryption exception

An error may display when you run a policy asking you to reconfigure the module.

[Table 5-1](#) lists the error message that is displayed and the solution for the error.

Table 5-1 Encryption exception

| Error | Solution |
|----------------------|--|
| Encryption exception | <p>This error may occur if you have set SSLConfigure=0 after configuring the IBM DB2 module. Or, if you have renamed or deleted the AESConfigure.dat file.</p> <p>To solve this problem, you need to reconfigure the IBM DB2 module.</p> <p>If you want to generate logs for encryption, add Debugon=1 in the AESConfigDB2.dat file from esm\config folder. This generates DB2AESDebuglog.log in the esm\system\<platform> folder.<="" p=""></platform>></p> |

DB2 Remote module errors

You may encounter errors while running policies that may cause the policy to terminate unexpectedly or the user account to get locked.

[Table 5-2](#) lists the errors pertaining to DB2 Remote module and their solutions.

Table 5-2 DB2 Remote module errors

| Error | Solution |
|--|---|
| Policy terminates unexpectedly. | This behaviour is observed only on 6.5.0 linux agent. To solve this problem, you need to upgrade DB2 agent to 6.5.2 or later. |
| User account gets locked after running a Policy run on DB2 Remote module on Windows. | This happens because for every check, the IBM DB2 module connects to the database and the user account gets locked based on the Windows Password policy. To solve this problem, make sure the credentials supplied for each database is correct. |