

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

Release for Symantec ESM 5.5, 6.0, & 6.5.x

For Windows 2000



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

The software that is described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
040719

Copyright Notice

Copyright © 2008 Symantec Corporation.
All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Symantec Enterprise Security Manager, LiveUpdate, and Symantec Security Response are trademarks of Symantec Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product names that are mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Printed in the United States of America.

Technical support

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

Symantec technical support offerings include:

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

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

Licensing and registration

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

Contacting Technical Support

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

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

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

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

Customer Service

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

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Symantec Software License Agreement

Symantec Enterprise Security Manager

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU” OR “YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE “AGREE” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE “I DO NOT AGREE” OR “NO” BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the “Software”) is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a “License Module”) that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

- A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module. Permission to use the software to assess Desktop, Server or Network machines does not constitute permission to make additional copies of the Software. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software you are authorized to use on a single machine.
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
- C. use the Software to assess no more than the number of Desktop machines set forth under a License Module.

“Desktop” means a desktop central processing unit for a single end user;

D. use the Software to assess no more than the number of Server machines set forth under a License Module.

“Server” means a central processing unit that acts as a server for other central processing units;

E. use the Software to assess no more than the number of Network machines set forth under a License Module.

“Network” means a system comprised of multiple machines, each of which can be assessed over the same network;

F. use the Software in accordance with any written agreement between You and Symantec; and

G. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. use the Software to assess a Desktop, Server or Network machine for which You have not been granted permission under a License Module;

C. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

D. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

E. continue to use a previously issued license key if You have received a new license key for such license, such as with a disk replacement set or an upgraded version of the Software, or in any other instance;

F. continue to use a previous version or copy of the Software after You have installed a disk replacement set, an upgraded version, or other authorized replacement. Upon such replacement, all copies of the prior version must be destroyed;

G. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

H. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor

I. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following

Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Syantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW

LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified by, the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the

laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Chapter 1	Introducing ESM Modules for IBM DB2 Universal Databases	
	Preparing for DB2 module installation	4
	Minimum account privileges	4
	System requirements	5
	Installing the DB2 module	6
	Installation log	9
	Editing configuration records and .m files	14
	Editing the configuration records	14
	Editing the .m file	14
	Creating a baseline snapshot	15
Chapter 2	Understanding the DB2 remote module	
	Aliases, Authentication, Version and OS	18
	DB2 Database Aliases	18
	Authentication from the Server	19
	DB2 Version and OS	19
	Discovery Mode	19
	Server Discovery Mode	19
	Instance Discovery Mode	20
	Database Discovery Mode	20
	System authorities	21
	Unauthorized Group Set in System Administrator Authority	21
	Unauthorized Group Set in System Control Authority	21
	Unauthorized Group Set in System Maintenance Authority	22
	Unauthorized Group/User in Database Administrator Authority	22
	New Group/User in Database Administrator Authority	23
	Deleted Group/User in Database Administrator Authority	23
	Modified Group/User in Database Administrator Authority	24
	Unauthorized Group/User in LOAD Authority	24
	New Group/User in LOAD Authority	25
	Deleted Group/User in LOAD Authority	25
	Modified Group/User in LOAD Authority	26
	Database privileges	27
	Unauthorized Group/User in BINDADD Database Privilege	27
	New Group/User in BINDADD Database Privilege	27

Deleted Group/User in BINDADD Database Privilege	28
Modified Group/User in BINDADD Database Privilege	28
Unauthorized Group/User in CONNECT Database Privilege	29
New Group/User in CONNECT Database Privilege	29
Deleted Group/User in CONNECT Database Privilege	30
Modified Group/User in CONNECT Database Privilege	30
Unauthorized Group/User in CREATETAB Database Privilege	31
New Group/User in CREATETAB Database Privilege	31
Deleted Group/User in CREATETAB Database Privilege	32
Modified Group/User in CREATETAB Database Privilege	32
Unauthorized Group/User in CREATE_NOT_FENCED Database Privilege	33
New Group/User in CREATE_NOT_FENCED Database Privilege	33
Deleted Group/User in CREATE_NOT_FENCED Database Privilege ...	34
Modified Group/User in CREATE_NOT_FENCED Database Privilege	34
Unauthorized Group/User in IMPLICIT_SCHEMA Database Privilege	35
New Group/User in IMPLICIT_SCHEMA Database Privilege	35
Deleted Group/User in IMPLICIT_SCHEMA Database Privilege	36
Modified Group/User in IMPLICIT_SCHEMA Database Privilege	36

Introducing ESM Modules for IBM DB2 Universal Databases

This chapter includes the following topics:

- [Preparing for DB2 module installation](#)
- [System requirements](#)
- [Installing the DB2 module](#)
- [Editing configuration records and .m files](#)
- [Creating a baseline snapshot](#)

Preparing for DB2 module installation

To install the DB2 module, you need:

- 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.
- DB2 Client: You must have a DB2 client application 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

The login accounts need minimum privileges to execute the following commands for performing ESM security checks on DB2 Server:

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

System requirements

[Table 1-1](#) lists the DB2 operating systems on which the ESM application modules for Windows can report remotely.

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

Supported DB2 operating systems	Supported OS versions	Supported DB2 versions
Red Hat Enterprise Linux (32-bit, 64-bit, 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	9 Ultra Sparc, 10 Ultra Sparc	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

Installing the DB2 module

The DB2 module is installed from CD using esmdb2tpi.exe. This installation program:

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

Note: The Symantec ESM Modules for IBM DB2 Universal Databases must be installed on Windows 2000. Policies, including the DB2 remote best practice policy, can run against any DB2 v8.1 and v8.2 database.

To run the installation program and register the files

- 1 From the CD, run
\\DATABASES\DB2\Modules\<<architecture>\esmdb2tpi.exe.
- 2 Choose an option:
 - Select option 1 to display the contents of the package.
To install the module, rerun esmdb2tpi.exe and select option 2.
 - Select 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 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 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 DB2 databases.
 - To continue the installation and enable security checking for your databases, type Y.
The installation program automatically detects existing 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 DB2 database alias. Press Enter if you are satisfied with the detected alias.
- 4 Enter the DB2 instance name. Press Enter if you are satisfied with the detected instance name.

Note: If the database is installed on the local computer, the installation program cannot detect the instance name. Open the DB2 Command Center to find the instance name.

- 5 Enter the User ID that is used to log on to the DB2 database.
- 6 Enter the password that is used to log on to the 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 DB2 User ID and password are encrypted when they are displayed for your approval.

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

Installation log

The following log is an example of an ESM Modules for IBM DB2 Universal Databases installation. 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.

Enter option number [1]: 2

Installing package: "ESM modules for DB2" 1.0 (2002/06/06) Tuneup
pack will overlay ESM modules for DB2 version 1.0 with version 1.0

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

File: C:\Program Files\Symantec\ESM\register\win2000\db2module.m.gz
Description: ESM db2module.m module definition 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]? y

ESM manager that the agent is registered to: mymachine1

ESM access name to login to the ESM manager [ESM]: esm Enter the ESM
password used to log in to the ESM manager. Password: *****

Enter the network protocol used to contact the ESM manager.

1) IPX

2) TCP

Enter 1 or 2 [2]: 2

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

Enter the name of the agent as it is registered to the ESM manager

[mymachine1]: mymachine1

ESM Manager : mymachine1

ESM user name : esm Protocol : TCP Port : 5600

ESM agent : mymachine1

Is this information correct? [yes] y

Extracting C:\Program Files\Symantec\ESM\bin\w2k-ix86\mtpkreg.exe.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w2k-ix86\db2module.exe.gz...

Extracting C:\Program Files\Symantec\ESM\register\win2000\db2module.m.gz... Extracting C:\Program Files\Symantec\ESM\bin\w2k-ix86\DB2Collector.exe.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w2k-ix86\SnapshotCollector.exe.gz..

Extracting C:\Program Files\Symantec\ESM\bin\w2k-ix86\db2module.rete.gz...

Extracting C:\Program Files\Symantec\ESM\bin\w2k-ix86\DB2Setup.exe.gz...

Continue and add configuration records to enable ESM security checking

for your DB2 database? [yes] y

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

DB2 database alias : DWCNTRL DB2 instance name : TCP0000

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

[yes]

DB2 database alias [DWCNTRL]: DWCNTRL

DB2 instance name [TCP0000]: TCP0000

User ID used to log on to the DB2 database: db2as

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

: *****

Re-Enter password: ***** DB2 database alias : DWCNTRL DB2 instance name : TCP0000

DB2 database login : 96b64802f784fbfd

Password : 5d04486647d33656

Is this information correct? [yes] y

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

DB2 database alias : DWCTRLDB

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

[yes] y

DB2 database alias [DWCTRLDB]: DWCTRLDB

DB2 instance name : db2

User ID used to log on to the DB2 database: db2admin Enter the
password used to log on to the DB2 database. Password :

Re-Enter password: ***** DB2 database alias : DWCTRLDB DB2
instance name : db2

DB2 database login : 95ce03dd61d380c53408e4e4c86d9d05

Password : 5d04486647d33656

Is this information correct? [yes] y

*** Configuration records *** DB2 database alias : DWCTRL DB2
instance name : TCP0000

DB2 database login : 911d74dd7f3ba414

Password : 5d04486647d33656

=== ===

DB2 database alias : DWCTRLDB DB2 instance name : db2

DB2 database login : 95ce03dd61d380c54f48ab8919da9335

Password : 5d04486647d33656

*** *** *** ***

Options:

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

Enter option number [3]: 3

Tune-up pack installation complete

Re-registering modules/template files... Please wait... Registering
to manager mymachine1

checking: ESM DB2 Module

End of installation.

Editing configuration records and .m files

After installing the DB2 module, you can edit the configuration records and the configuration (.m) files. A configuration record is created for each database alias when you enable security checking during installation. Module configuration (.m) files contain the message information that Symantec ESM uses to report security check results.

Editing the configuration records

You can add, modify, or remove the DB2 database instances that ESM includes in security checks by using the DB2Setup.exe program. By default, DB2Setup.exe is located in the \\Program Files\\Symantec\\ESM\\bin\\<architecture>\\ directory. Run DB2Setup.exe with the following options:

Table 1-2 Editing configuration records

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 existing DB2 database configuration records.	DB2Setup -m
List existing DB2 database configuration records.	DB2Setup -l
Specify a new input file for DB2 database configuration records. The default file is \\ProgramFiles\\Symantec\\ESM\\config\\DB2Module.dat.	DB2Setup -if <filename>
Specify a new output file for DB2 database configuration records. The default file is \\ProgramFiles\\Symantec\\ESM\\config\\DB2Module.dat.	DB2Setup -of <filename>

Editing the .m file

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

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

Creating a baseline snapshot

To establish a baseline for DB2 module security checks, create a new 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 remote module

This chapter includes the following topics:

- [Aliases, Authentication, Version and OS](#)
- [Discovery Mode](#)
- [System authorities](#)
- [Database privileges](#)

Aliases, Authentication, Version and OS

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

DB2 Database Aliases

Configuration records are created during the 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 DB2 module”](#) on page 6 and [“Editing configuration records and .m files”](#) on page 14.

By default, ESM examines every DB2 database alias for which there exists a configuration record. Use the 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 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 2-1 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 2-2 DB2 Version and OS message

Message Name	Title	Class
DB2_VERSION_OS	DB2 Version and OS	0

Discovery Mode

Discovery mode is a DB2 feature that is used to gather information from 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 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 2-3 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 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 2-4 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 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 2-5 Database Discovery Mode message

Message Name	Title	Class
DATABASE_DIS_MODE	DB2 Database Discovery Mode	1

System authorities

The DB2 remote module lets you to maintain lists of groups and users that have been granted 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 2-6 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 2-7 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 2-8 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 2-9 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 2-10 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 2-11 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 2-12 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 2-13 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 2-14 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 2-15 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 2-16 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 DB2 remote module lets you maintain lists of groups and users that have 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 2-17 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 2-18 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 2-19 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 2-20 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 2-21 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 2-22 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 2-23 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 2-24 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 2-25 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 2-26 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 2-27 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 2-28 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 2-29 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 2-30 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 2-31 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 2-32 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 2-33 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 2-34 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 2-35 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 2-36 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.