NetIQ Security Solutions for IBM i
TGSecure 2.3
Report Reference Guide
Revised February 2021

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Copyright © 2021 Trinity Guard LLC. All rights reserved.

1. What's New . . . 6
2. TGSecure Report Reference Introduction . . . 7
2.1 Report Categories . . . 8
3. Access Escalation Reports . . . 9
3.1 Access Escalation Usage Reports . . . 10
3.1.1 Access Escalation Activity . . . 11
3.1.2 Access Escalation Command Activity . . . 13
3.1.3 Access Escalation Db Update Activity . . . 15
3.1.4 Access Escalation Entitlement Usage . . . 17
3.1.5 Access Escalation Failures . . . 19
3.1.6 Access Escalation Program Activity . . . 21
3.2 Access Escalation Configuration Reports . . . 23
3.2.1 Access Escalation Access Controls . . . 24
3.2.2 Access Escalation Defaults . . . 25
3.2.3 Access Escalation Entitlements . . . 27
3.2.4 Access Escalation File Editors . . . 29
3.2.5 Network Groups . . . 30
3.2.6 Object Groups . . . 31
3.2.7 Operation Groups . . . 33
3.2.8 User Groups . . . 35
3.3 Access Escalation Change Reports . . . 36
3.3.1 Access Escalation Access Control Changes . . . 37
3.3.2 Access Escalation Default Changes . . . 39
3.3.3 Access Escalation Entitlement Changes . . . 41
3.3.4 Access Escalation File Editor Changes . . . 43
3.3.5 Network Groups Changes . . . 45
3.3.6 Object Groups Changes . . . 47
3.3.7 Operation Groups Changes . . . 49
3.3.8 User Groups Changes . . . 51
4. Command Security Reports . . . 53
4.1 Command Security Activity Reports . . . 54
4.1.1 Commands Allowed via Command Security . . . 55
4.1.2 Commands Rejected via Command Security . . . 57
4.2 Command Security Configuration Reports . . . 59
4.2.1 Command Security Config Settings . . . 60
4.2.2 Command Security Parameter Level . . . 62
4.2.3 Command Security Command Rules . . . 63
4.3 Command Security Change Reports . . . 65
4.3.1 Command Security Configuration Changes . . . 66
4.3.2 Command Security Command Parameter Level Changes . . . 69
4.3.3 Command Security Command Rule Changes . . . 71
5. Inactivity Session Lockdown Reports . . . 74
5.1 Inactivity Session Usage Reports . . . 75
5.1.1 Inactivity Disconnect . . . 76
5.2 Inactivity Session Configuration Reports . . . 78
5.2.1 ISL Configuration Settings . . . 79
5.2.2 ISL Disconnect Options . . . 81
5.2.3 ISL Inclusion Exclusion Rules . . . 83
5.3 Inactivity Session Change Reports . . . 85
5.3.1 ISL Configuration Changes . . . 86
5.3.2 ISL Disconnect Option Changes . . . 89
5.3.3 ISL Rule Changes . . . 91
6. Network Security Reports . . . 93
6.1 Transaction Reports . . . 94
6.1.1 Central Server Transactions . . . 95
6.1.2 Database Server Transactions . . . 98
6.1.3 Data Queue Transactions . . . 101
6.1.4 DDM Transactions . . . 104
6.1.5 File Server Transactions . . . 107
6.1.6 Incoming Transactions . . . 110

6.1.7 Network Printer Transactions . . . 113
6.1.8 Network Transaction FTP . . . 116
6.1.9 Network Transaction FTP and REXEC . . . 119
6.1.10 Network Transactions . . . 122
6.1.11 Network Transaction Showcase . . . 125
6.1.12 Remote Command Transactions . . . 128
6.1.13 Signon Server Transactions . . . 131
6.1.14 Socket Transactions . . . 134
6.1.15 Telnet Transactions . . . 137
6.2 Summary Reports . . . 140
6.2.1 Socket Summary by Server Report . . . 141
6.2.2 Socket Summary by User Report . . . 143
6.2.3 Transaction Summary by Server Report . . . 145
6.2.4 Transaction Summary by User Report . . . 147
6.3 Configuration Reports . . . 148
6.3.1 Exit Point Configuration Report . . . 149
6.3.2 Remote Exit Rules Report . . . 151
6.3.3 Socket Rules Report . . . 153
6.4 Configuration Change Reports . . . 155
6.4.1 Exit Point Configuration Changes . . . 156
6.4.2 Remote Exit Rules Changes . . . 159
6.4.3 Socket Rules Changes . . . 162
7. Resource Manager Reports . . . 164
7.1 Resource Manager Usage Reports . . . 165
7.1.1 Authority Collection for IFS Objects . . . 166
7.1.2 Authority Collection for Native Objects . . . 168
7.1.3 Authority Compliance Report . . . 170
7.2 Resource Manager Configuration Reports . . . 175
7.2.1 Resource Manager Configuration . . . 176
7.2.2 Resource Manager out of Compliance Data . . . 178
7.2.3 Resource Manager Schema Details . . . 180
7.2.4 Resource Manager Schema Header . . . 182
7.3 Resource Manager Change Reports . . . 184
7.3.1 Rsc Manager Configuration Changes . . . 185
7.3.2 Rsc Manager out of Compliance Data Changes . . . 187
7.3.3 Rsc Manager Schema Details Changes . . . 189
7.3.4 Rsc Manager Schema Header Changes . . . 193
8. User Profile Reports . . . 195
8.1 User Profile Usage Reports . . . 196
8.1.1 Authority Failures . . . 197
8.1.2 Blueprint Compliance Report . . . 199
8.1.3 Invalid Sign-on Attempts . . . 200
8.1.4 Profile Compliance Report . . . 202
8.1.5 User Profile Activity For User: *ALL . . . 204
8.1.6 User Profile Changes . . . 205
8.1.7 User Profile via Blueprint For User: *ALL . . . 206
8.2 User Profile Configuration Reports . . . 207
8.2.1 Blueprint 3rd Party Integration File . . . 208
8.2.2 Blueprint Authority List Settings File . . . 209
8.2.3 Blueprint Master . . . 210
8.2.4 Blueprint Non-Compliance User Profiles . . . 212
8.2.5 Blueprint Object Authority File . . . 214
8.2.6 Blueprint Parameter File . . . 215
8.2.7 Blueprint Permissions File . . . 216
8.2.8 Profile Inactivity Settings . . . 217
8.2.9 Profile Manager Defaults . . . 219
8.2.10 User Profile Archive . . . 221
8.2.11 User Profile Exclusions . . . 222
8.3 User Profile Change Reports . . . 223
8.3.1 Blueprint 3rd Party Changes . . . 224

8.3.2 Blueprint Auth Setting Changes . . . 226
8.3.3 Blueprint Master Changes . . . 228
8.3.4 Blueprint Non-Compliance Changes . . . 230
8.3.5 Blueprint Object Authority Changes . . . 232
8.3.6 Blueprint Parameter Changes . . . 234
8.3.7 Blueprint Permissions Changes . . . 236
8.3.8 Profile Inactivity Changes . . . 238
8.3.9 Profile Manager Default Changes . . . 240
8.3.10 User Profile Archive Changes . . . 242
8.3.11 User Profile Exclusion Changes . . . 244
9. APPENDICES . . . 246
9.1 APPENDIX - TGSecure Collectors . . . 247
9.2 APPENDIX - TGSecure Report Reference Revisions . . . 257
9.2.1 Version 2.3 - TGSecure Report Reference Revisions . . . 258
9.2.2 Version 2.2 - TGSecure Report Reference Revisions . . . 259
9.2.3 Version 2.1 - TGSecure Report Reference Revisions . . . 260

What's New

Version 2.3 - TGSecure Report Reference Revisions
No major updates were made to the TGSecure reports in this release.

TGSecure Report Reference Introduction

This reference guide provides information about built-in reports provided with TGSecure. Use this reference guide to learn why a report passed or failed.

> **Note**: Refer to the TGSecure User Guide for detailed information and concepts on how to use TGSecure.

The TGSecure reports fall into the following categories:

- Access Escalation Reports
- Inactivity Session Lockdown Reports
- Network Security Reports
- Resource Manager Reports
- User Profile Reports

Report Categories

There are three categories of TGSecure reports:

- Access Escalation Reports
- Inactivity Session Lockdown Reports
- Network Security Reports
- Resource Manager Reports
- User Profile Reports

Access Escalation Reports

This section includes descriptions of the following **Access Escalation** reports:

- Access Escalation Usage Reports
- Access Escalation Configuration Reports
- Access Escalation Change Reports

> **Tip**: Refer to the TGSecure User Guide for more information about Access Escalation Management

See also

TGSecure Report Reference Introduction

Access Escalation Usage Reports

This section contains descriptions of the following reports:

- Access Escalation Activity
- Access Escalation Command Activity
- Access Escalation Db Update Activity
- Access Escalation Entitlement Usage
- Access Escalation Failures
- Access Escalation Program Activity

See also

Access Escalation Reports

Access Escalation Activity

This report displays all escalation activity (system access and object update attempts).

Collector ID: ACCESS_ESCALATION_USAGE

Report ID: ACCESS_ESCAL_ACTIVITY

Including:

- Records with action status: *PASS or *FAIL.
- Records with object type: *CMD, *FILE, or *PGM

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Activity).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job

Job Number	Number assigned to the job
User Profile	Name of the user submitting the transaction
System Name	Name of the system submitting the transaction
Receiver	Name of the journal receiver submitting the transaction
Receiver Library	Name of the journal receiver library submitting the transaction
Receiver ASP	Name of the journal receiver ASP submitting the transaction
Action Status	Status of transaction: *PASS - transaction accepted *FAIL - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client-server submitting the transaction
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of the system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction
Object Type	Object type targeted by the transaction
Swap User	If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the user profile associated with the incoming transactions.
Reason	Reason for the transaction
Command Executed	Command executed by the transaction
Usage Description	Description of the transaction

See also

Access Escalation Usage Reports

Access Escalation Command Activity

This report displays command activities. Records with the object type of *CMD.

Collector ID: ACCESS_ESCALATION_USAGE

Report ID: ACCESS_ESCAL_CMD_ACTIVITY

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Command Activity).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the transaction
System Name	Name of the system submitting the transaction

Action Status	Status of incoming transaction: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client-server submitting the transaction
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of the system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction
Object Type	Object type targeted by the transaction
Swap User	If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the user profile associated with the incoming transactions.
Reason	Reason for the transaction
Command Executed	Command executed by the transaction

See also

Access Escalation Usage Reports

Access Escalation Db Update Activity

This report displays database file activities. Records with the object type of *FILE.

Collector ID: ACCESS_ESCALATION_USAGE

Report ID: ACCESS_ESCAL_DB_UPD_ACTIVITY

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Database Update Activity).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the transaction
System Name	Name of the system submitting the transaction

Action Status	Status of incoming transaction: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client-server submitting the communication
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of the system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction
Object Type	Object type targeted by the transaction
Swap User	If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the user profile associated with the incoming transactions.
Reason	Reason for the transaction
Command Executed	Command executed by the transaction

See also

Access Escalation Usage Reports

Access Escalation Entitlement Usage

This report displays successful access attempts. Records with the action status *PASS.

Collector ID: ACCESS_ESCALATION_USAGE

Report ID: ACCESS_ESCAL_ENTITLEMENT_USG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **5** (Entitlement Usage).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the transaction
System Name	Name of system submitting the transaction

Action Status	Status of incoming transaction: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client-server submitting the transaction
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of the system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction
Object Type	Object type targeted by the transaction
Swap User	If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the user profile associated with the incoming transactions.
Reason	Reason for the transaction
Command Executed	Command executed by the transaction
Usage Description	Description of the transaction

See also

Access Escalation Usage Reports

Access Escalation Failures

This report displays failed access attempts. Records with action status *FAIL.

Collector ID: ACCESS_ESCALATION_USAGE

Report ID: ACCESS_ESCAL_FAILURES

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (Failures).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the transaction
System Name	Name of system submitting the transaction

Action Status	Status of incoming transaction: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client-server submitting the transaction
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of the system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction
Object Type	Object type targeted by the transaction
Swap User	If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the user profile associated with the incoming transactions.
Reason	Reason for the transaction
Command Executed	Command executed by the t transaction
Usage Description	Description of transaction

See also

Access Escalation Usage Reports

Access Escalation Program Activity

This report displays program activities. Records with the object type of *PGM.

Collector ID: ACCESS_ESCALATION_USAGE

Report ID: ACCESS_ESCAL_PGM_ACTIVITY

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Program Activity).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the transaction
System Name	Name of system submitting the transaction

Action Status	Status of incoming transaction: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client-server submitting the transaction
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of the system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction
Object Type	Object type targeted by the transaction
Swap User	If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the user profile associated with the incoming transactions.
Reason	Reason for the transaction
Command Executed	Command executed by the transaction

See also

Access Escalation Usage Reports

Access Escalation Configuration Reports

This section contains descriptions of the following reports:

- Access Escalation Access Controls
- Access Escalation Defaults
- Access Escalation Entitlements
- Access Escalation File Editors
- Network Groups
- Object Groups
- Operation Groups
- User Groups

See also

Access Escalation Reports

Access Escalation Access Controls

This report displays the access control configuration details. The users or user groups displayed in this report have been granted or denied access to the Access Escalation Management (AEM) interface. The AEM allows users to perform a task defined in an entitlement using the access privilege of a swap uses. In most cases, the swap user will have higher access privileges than the user.

Collector ID: ACCESS_ESCAL_ACC_CONTROLS

Report ID: ACCESS_CONTROLS_CONFIG

To run this report

1) Access the TGSecure main menu.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **4** (Access Control).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
User	User (or user group) granted permission to access the AEM interface.
Client IP	Client IP address from which the user (or user group) has permission to access the AEM interface.

See also

Access Escalation Configuration Reports

Access Escalation Defaults

This report displays default escalation settings.

Collector ID: ACCESS_ESCAL_DEFAULTS

Report ID: DEFAULTS_CONFIG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Default).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Journal Name	Journal in which configuration changes are stored
Journal Library	Library in which the journal resides
Default Swap	Profile to be used in place of the user profile associated with the transactions
Time-out interval	Max amount of time allowed for the remote server to attempt to communicate with the target server
Command Execution Entry	Journal entry code for the type of transaction
Audit Configuration	Flag indicating whether auditing is enabled for configuration changes: **Y** - Auditing enabled (enable tracking and reporting) **N** - Auditing disabled (disable tracking and reporting)
Alert Message Queue	Queue in which alerts are stored

Alert Message Queue Library	Library in which the queue resides

See also

Access Escalation Configuration Reports

Access Escalation Entitlements

This report displays the entitlement configuration details.

Collector ID: ACCESS_ESCAL_ENTITLEMENTS

Report ID: ENTITLEMENT_CONFIG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Entitlement).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Entitlement Enabled?	Indicates whether the entitlement is enabled **Y** - Entitlement applied **N** - Entitlement ignored
User Name	User/User group to which the entitlement applies
Object Name	Object/Object group to which the entitlement applies
Object Library	Library in which the object resides
Object Type	Type of object: ***CMD** - Command ***PGM** - Program ***FILE** - File
Swap User	User/User group to which the entitlement applies when using the AEM interface
Server	Server/server group to which the entitlement applies

Calendar Name	Calendar that defined when the entitlement is applicable **Note**: Calendars allow you to restrict when an entitlement is applicable.
Authentication Y/N	Indicates whether user authentication (password entry) is required **Y** - User must provide a password as part of the transaction request **N** - No password required as part of the transaction request
Alerts Y/N	Indicates whether notification alerts are submitted to the alert queue **Y** - Alerts enabled **N** - Alerts disabled
Entitlement Description	Description of the entitlement

See also

Access Escalation Configuration Reports

Access Escalation File Editors

This report displays the file editor configuration details. The items listed identify any third-party file editor commands added to the current system available for the user in addition to the standard IBM commands.

Collector ID: ACCESS_ESCAL_FILE_EDITORS

Report ID: FILE_EDITORS_CONFIG

To run this report

1) Access the TGSecure main menu.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **2** (File Editors).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Command	Third-party command
Library	Library to be modified by the command
Parameter	Type of object to be modified by the command: **PGM** - Program **FILE** - File

See also

Access Escalation Configuration Reports

Network Groups

This report displays configuration details for all available network groups.

Collector ID: TG_NETWORK_GROUPS

Report ID: TG_NETWORK_GROUPS_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (Network Groups Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Network Group	Name assigned to the group
Network Name	Name of the member assigned to the group
Network Description	Description of member
Network Group Description	Description of group

See also

Access Escalation Configuration Reports

Configuration Reports

Object Groups

This report displays configuration details for all available object groups.

Collector ID: TG_OBJECT_GROUPS

Report ID: TG_OBJECT_GROUPS_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **8** (Object Groups Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Object Group Name	Name assigned to the group
Object Name	Name of the member assigned to the group
Object Library	Library in which object resides
Object Type	Type of object
Object IFS	IFS object
Object Description	Description assigned to the member
Object Group Description	Description assigned to object group

See also

Access Escalation Configuration Reports

Configuration Reports

Operation Groups

This report displays configuration details for all available operation groups. An operation is a combination of a function and command to be performed on a specific server.

Collector ID: TG_OPERATION_GROUPS

Report ID: TG_OPERATION_GROUPS_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **7** (Operation Groups Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Operation Group	Name assigned to the group
Server Name	Name of server
Function Name	Name of function
Command Name	Name of command
Operation Description	Description assigned to the operation
Operation Group Description	Description assigned to the operation group

See also

Access Escalation Configuration Reports

Configuration Reports

User Groups

This report displays configuration details for all available user groups.

Collector ID: TG_USER_GROUP

Report ID: TG_USER_GROUPS_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **5** (User Groups Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Group Name	Name assigned to the group
Member Name	Name of the member assigned to the group
Member Description	Description of member
Group Description	Description of group

See also

Access Escalation Configuration Reports

Configuration Reports

Access Escalation Change Reports

This section contains descriptions of the following reports:

- Access Escalation Access Control Changes
- Access Escalation Default Changes
- Access Escalation Entitlement Changes
- Access Escalation File Editor Changes
- Network Groups Changes
- Object Groups Changes
- Operation Groups Changes
- User Groups Changes

See also

Access Escalation Reports

Access Escalation Access Control Changes

This report displays changes made to the access control settings. The access control settings determine which users have the ability to perform Access Escalation Management (AEM).

Collector ID: DATABASE_AUDITING

Report ID: ACCESS_ESCALATION_ACCESS_CTRL

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Access Control Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Access Control User	User (or user group) whose access control was modified
Target IP Address	IP address from which the user (user group) whose record was modified can access the AEM interface

See also

Access Escalation Change Reports

Access Escalation Default Changes

This report displays changes to the network security defaults associated with access escalation.

Collector ID: DATABASE_AUDITING

Report ID: ACCESS_ESCALATION_DEFAULTS

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Default Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Journal Name	Journal in which configuration changes are stored
Journal Library	Library in which the journal resides
Default Swap	Profile to be used in place of the user profile associated with the transactions
Time-out interval	Max amount of time allowed for the remote server to attempt to communicate with the target server
Command Execution Entry	Journal entry code for the type of transaction
Audit Configuration	Flag indicating whether auditing is enabled for configuration changes: **Y** - Auditing enabled (enable tracking and reporting) **N** - Auditing disabled (disable tracking and reporting)
Alert Message Queue	Queue in which alerts are stored
Alert Message Queue Library	Library in which the queue resides

See also

Access Escalation Change Reports

Access Escalation Entitlement Changes

This report displays changes to user entitlements. Entitlements are rules that allow you to control user access at a granular level.

Collector ID: DATABASE_AUDITING

Report ID: ACCESS_ESCALATION_ENTITLEMENT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Entitlement Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Entitlement enabled?	Flag indicating whether the entitlement is enabled **Y** - Entitlement applied **N** - Entitlement ignored
User Name	Name of the user/user group to which the entitlement applies
Object Name	Name of the object/object group to which the entitlement applies
Object Library	Name of the library to which the entitlement applies
Object Type	Type of object to which the entitlement applies
Swap User	User/User group to which the entitlement applies when using the AEM interface
Server	Server/Server group to which the entitlement applies

See also

Access Escalation Change Reports

Access Escalation File Editor Changes

This report displays all changes to the file editor.

Collector ID: DATABASE_AUDITING

Report ID: ACCESS_ESCALATION_FILE_EDITORS

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (File Editor Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
File Editor Command	Third-party command
File Editor Library	Library to be modified by the command
File Editor Parameter	Type of object to be modified by the command: **PGM** - Program **FILE** - File

See also

Access Escalation Change Reports

Network Groups Changes

This report displays all changes made to network group configurations.

Collector ID: DATABASE_AUDITING

Report ID: NETWORK_GROUPS_CHANGES_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (Network Groups Changes Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Network Group	Name assigned to the group
Network Name	Name of the member assigned to the group
Network Description	Description of member
Network Group Description	Description of group

See also

Access Escalation Change Reports

Configuration Change Reports

Object Groups Changes

This report displays all changes made to object group configurations.

Collector ID: DATABASE_AUDITING

Report ID: OBJECT_GROUPS_CHANGES_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **8** (Object Groups Changes Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Object Group Name	Name assigned to the group
Object Name	Name of the member assigned to the group
Object Library	Library in which object resides
Object Type	Type of object
Object IFS	IFS object
Object Description	Description assigned to the member
Object Group Description	Description assigned to object group

See also

Access Escalation Change Reports

Configuration Change Reports

Operation Groups Changes

This report displays all changes made to operation group configurations.

Collector ID: DATABASE_AUDITING

Report ID: OPERATION_GROUPS_CHANGES_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **7** (Operation Groups Changes Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Operation Group	Name assigned to the group
Server Name	Name of server
Function Name	Name of function
Command Name	Name of command
Operation Description	Description assigned to the operation
Operation Group Description	Description assigned to the operation group

See also

Access Escalation Change Reports

Configuration Change Reports

User Groups Changes

This report displays all changes made to user group configurations.

Collector ID: DATABASE_AUDITING

Report ID: USER_GROUPS_CHANGES_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **5** (User Groups Changes Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Group Name	Name assigned to the group
Member Name	Name of the member assigned to the group
Member Description	Description of member
Group Description	Description of group

See also

Access Escalation Change Reports

Configuration Change Reports

Command Security Reports

This section includes descriptions of the following reports:

- Command Security Activity Reports
- Command Security Configuration Reports
- Command Security Change Reports

> **Tip**: Refer to the TGSecure User Guide for more information about Command Security.

See also

TGSecure Report Reference Introduction

Command Security Activity Reports

This section contains descriptions of the following reports:

- Commands Allowed via Command Security
- Commands Rejected via Command Security

See also

Command Security Reports

Commands Allowed via Command Security

This report displays command security configuration settings.

Collector ID: CMD_SEC_COMMANDS

Report ID: CMD_SEC_CMD_EXEC

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Command Security Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Commands Allowed via Command Security).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the socket transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the socket transaction request
System Name	Name of system submitting the socket transaction request
Receiver	Name of the journal receiver submitting the SIGNON transaction request

Receiver Library	Name of the journal receiver library submitting the SIGNON transaction request
Receiver ASP	Name of the journal receiver ASP submitting the SIGNON transaction request
RCV ASP	Count of ASP receivers
Status	Status of change ***PASS** - Change was successful ***FAIL** - Change failed
User Name	Name of the user executing the change
Client IP	IP address of the server from which the change was initiated
Command Library	Library in which command resides
Command Name	Name of command
Command String	Parameters used in conjunction with the command

See also

Command Security Reports

Commands Rejected via Command Security

This report displays command security configuration settings.

Collector ID: CMD_SEC_COMMANDS

Report ID: CMD_SEC_CMD_REJECT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Command Security Activity Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Commands Rejected via Command Security).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the socket transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the socket transaction request
System Name	Name of system submitting the socket transaction request
Receiver	Name of the journal receiver submitting the SIGNON transaction request

Receiver Library	Name of the journal receiver library submitting the SIGNON transaction request
Receiver ASP	Name of the journal receiver ASP submitting the SIGNON transaction request
RCV ASP	Count of ASP receivers
Status	Status of change ***PASS** - Change was successful ***FAIL** - Change failed
User Name	Name of the user executing the change
Client IP	IP address of the server from which the change was initiated
Command Library	Library in which command resides
Command Name	Name of command
Command String	Parameters used in conjunction with the command

See also

Command Security Reports

Command Security Configuration Reports

This section contains descriptions of the following reports:

- Command Security Config Settings
- Command Security Parameter Level
- Command Security Command Rules

See also

Command Security Reports

Command Security Config Settings

This report displays command security configuration settings.

Collector ID: CMD_SEC_CONF_SETTINGS

Report ID: CMD_SEC_CONF_SETTINGS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Command Security Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Command Security Configuration Settings).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Audit Status	Flag indicating whether auditing is enabled **Y** - Auditing is enabled **N** - Auditing is disabled **Note**: Auditing must be enabled to capture data for reporting purposes
Audit Journal Name	Name of audit journal
Audit Journal Library	Library in which audit journal resides
Alert Status	Flag indicating whether alerting is enabled: **Y** - Alerting is enabled **N** - Alerting is disabled

Alert Message Queue	Queue in which to store triggered alerts
Alert Message Queue Library	Library in which the message queue resides
Journal Type	Code that identifies the type of journal
Primary Group Inheritance	Flag indicating whether to allow profile inheritance from the primary group ***YES** - Enable profile inheritance for the primary group ***NO** - Disable profile inheritance for the primary group **Note**: The primary group is the user ID entered in the **Group** profile field when using command **CHGUSRPRF**. The primary group is the first ID from which a user inherits privileges.
Supplemental Group Inheritance	Flag indicating whether to allow profile inheritance from supplemental groups ***YES** - Enable profile inheritance for supplemental groups ***NO** - Disable profile inheritance for supplemental groups **Note**: The supplemental groups are user IDs entered in the **Supplemental** group field when using command **CHGUSRPRF**. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.
Command Security	Flag indicating whether the **Command Security** feature is enabled **Y** - Command Security feature is enabled **N** - Command Security feature is disabled

See also

Command Security Reports

Command Security Parameter Level

This report displays command security parameter details.

Collector ID: CMD_SEC_PARAM_LEVEL

Report ID: CMD_SEC_PARAM_LEVEL

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Command Security Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Command Security Parameter Level Settings).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Command Name	Name assigned to command
Command Library	Library in which the command resides
Command Parameter Restrictions	The parameter value for which a restriction has been established

See also

Command Security Reports

Command Security Command Rules

This report displays command security parameter details.

Collector ID: CMD_SEC_RULES

Report ID: CMD_SEC_RULES

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Command Security Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Command Security Rules).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Rule Enabled	Flag indicating whether command security rules are enabled **Y** - Rules enabled **N** - Rules disabled
User Name	Name of user/user group to whom the rule applies
Command Name	Name of command to which the rule applies
Command Library	Library in which to apply the rule
Command Parmeter Restriction	Parameter value to which the rule applies
Client IP Address	IP address to which the rule applies
Calendar Name	Calendar to which the rule applies **Note**: Calendars allow you to restrict when a rule is applicable.

Command Audited	Flag indicating whether auditing is enabled ***YES** - Auditing enabled ***NO** - Auditing disabled **Note**: Auditing must be enabled to generate change reports.
Command Alerting	Flag indicating whether alerting is enabled ***YES** - Alerts enabled ***NO** - Alerts disabled **Note**: Alerting must be enabled to generate notifications.
Command Exit Installed	Flag indicating whether the command security exit program is installed ***YES** - Exit program installed ***NO** - Exit program not installed **Note**: The exit program must be installed to use the Command Security feature.
Command Action	Flag indicating whether the rule is allowing or disallowing the execution of a command ***PASS** - Allow execution of the command ***FAIL**- Disallow execution of the command
Command Description	Short description of the command rule

See also

Command Security Reports

Command Security Change Reports

This section contains descriptions of the following reports:

- Command Security Configuration Changes
- Command Security Command Parameter Level Changes
- Command Security Command Rule Changes

See also

Command Security Reports

Command Security Configuration Changes

This report displays changes made to command security configuration settings.

Collector ID: DATABASE_AUDITING

Report ID: CMD_SEC_CONF_SETTINGS

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Command Security Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Command Security Configuration Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Audit Status	Flag indicating whether auditing is enabled **Y** - Auditing is enabled **N** - Auditing is disabled **Note**: Auditing must be enabled to capture data for reporting purposes
Audit Journal Name	Name of audit journal
Audit Journal Library	Library in which audit journal resides
Alert Status	Flag indicating whether alerting is enabled: **Y** - Alerting is enabled **N** - Alerting is disabled
Alert Message Queue	Queue in which to store triggered alerts

Alert Message Queue Library	Library in which the message queue resides
Journal Type	Code that identifies the type of journal
Primary Group Inheritance	Flag indicating whether primary group inheritance is enabled **Y** - Profile inheritance for the primary group is enabled **N** - Profile inheritance for the primary group is disabled **Note**: The primary group is the user ID entered in the **Group profile** field when using command **CHGUSRPRF**. The primary group is the first ID from which a user inherits privileges.
Supplemental Group Inheritance	Flag indicating whether supplemental group inheritance is enabled ***YES** - Profile inheritance for supplemental groups is enabled ***NO** - Profile inheritance for supplemental groups is enabled **Note**: Supplemental groups are user IDs entered in the **Supplemental group** field when using command **CHGUSRPRF**. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.
Command Security	Flag indicating whether the **Command Security** feature is enabled ***YES** - Command Security feature is enabled ***NO** - Command Security feature is disabled

See also

Command Security Change Reports

Command Security Command Parameter Level Changes

This report displays changes made to command security parameter value restrictions.

Collector ID: DATABASE_AUDITING

Report ID: CMD_SEC_PARAM_LEVEL

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Command Security Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Command Security Command Parameter Level Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Command Name	Name of command to be monitor
Command Library	Name of the library to be monitor
Command Parameter Restrictions	Identify the restriction on the parameter value

See also

Command Security Change Reports

Command Security Command Rule Changes

This report displays changes made to command security parameter value restrictions.

Collector ID: DATABASE_AUDITING

Report ID: CMD_SEC_RULES

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Command Security Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Command Security Command Rule Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Rule Enabled?	Flag indicating whether the rule is enabled ***YES** - Rule enabled ***NO** - Rule disabled
User Name	Name of the user to whom the rule applies
Command Name	Name of command to be monitor
Command Library	Name of the library to be monitor
Command Parameter Restriction	Identify the restriction on the parameter value
Client IP Address	IP address of the server from which the change was initiated
Calendar Name	Name of the calendar that defines when the rule is applicable
Command Audited?	Flag indicating whether the auditing is enabled ***YES** - Auditing enabled ***NO** - Auditing disabled
Command Alerted?	Flag indicating whether the alerting is enabled ***YES** - Alerting enabled ***NO** - Alerting disabled

Command Exit Installed?	Flag indicating whether the exit point is installed on the server ***YES** - Exit points are installed and ready for use ***NO** - Exit points are not installed **Note**: The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to ***YES**.
Command Action?	Flag indicating when to perform the action ***PASS** - Perform action on pass ***FAIL** - Perform action on fail
Command Description	Short description of the command

See also

Command Security Change Reports

Inactivity Session Lockdown Reports

This section includes descriptions of the following **Inactivity Session Lockdown** reports:

- Inactivity Session Usage Reports
- Inactivity Session Configuration Reports
- Inactivity Session Change Reports

> **Tip**: Refer to the TGSecure User Guide for more information about Inactive Session Lockdown.

See also

TGSecure Report Reference Introduction

Inactivity Session Usage Reports

This section contains descriptions of the following reports:

- Inactivity Disconnect

See also

Inactivity Session Lockdown Reports

Inactivity Disconnect

This report displays disconnections caused by user inactivity.

Collector ID: INACTIVITY_DISCONNECTIONS

Report ID: INACTIVITY_DISCONNECTIONS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Inactivity Session Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Inactivity Disconnect Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
InactiveJob User	Name assigned to the user
InactiveJob Name	Name assigned to the inactive job **Note**: A name consists of three components: A code, the user's name, and a number
Subsystem Name	Name assigned to the subsystem
Subsystem Library	Library in which the subsystem resides

Disconnect Type	The type of disconnect triggered by the inactivity: **ENDJOB** - End the job (user must restart their job) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - End the session (user must restart their session and job)
Timestamp	Time at which the user was disconnected due to inactivity

See Also

Inactivity Session Usage Reports

Inactivity Session Configuration Reports

This section contains descriptions of the following reports:

- ISL Configuration Settings
- ISL Disconnect Options
- ISL Inclusion Exclusion Rules

See also

Inactivity Session Lockdown Reports

ISL Configuration Settings

This report displays the Inactivity Session Lockdown (ISL) configuration settings.

Collector ID: ISL_CONFIGURATION_SETTINGS

Report ID: ISL_CONFIGURATION

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Inactivity Session Configuration Settings).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Audit Status	Flag indicating whether auditing is enabled: **Y** - Auditing enabled (enable tracking and reporting) **N** - Auditing disabled (disable tracking and reporting)
Audit Journal Name	Journal in which to store ISL audit data **Note**: The default audit journal for TG products is **TGJRN**. The default journal resides in the **TGDATA** library.
Audit Journal Library	Library in which the journal resides
Alert Status	Flag indicating whether notification alerts are submitted to the alert queue **Y** - Alerts enabled **N** - Alerts disabled

Audit Configuration Change	Flag indicating whether auditing is enabled for configuration changes **Y** - Auditing enabled **N** - Auditing disabled
Alert Message Queue Name	Queue in which ISL alerts are stored **Note**: The default audit journal for TG products is **TGMSGQ**. The default journal resides in the **TGDATA** library.
Alert Message Queue Library	Library in which the queue resides
Check Interval	How often the system checks for inactive sessions
Disconnect Screen Message	Warning message user receives regarding an upcoming disconnect action
Disconnect Screen Title	Title of the dialog box that warns the user of an upcoming disconnect
Send Warning?	Flag indicating whether alerts are sent to warn the user of an impending disconnect ***YES** - Warning alert enabled ***NO** - Warning alert disabled
Warning Interval	When to send the user a warning message (seconds before disconnect)
Revoke Authority	Flag indicating whether to revoke a user's authority when they are locked or their session is ended ***YES** - The user's session is locked or ended, and the user's authority is revoked ***NO** - The user's session is locked or ended, but the user's authority is maintained **Note**: When a user's authority is revoked, the user is prohibited from performing tasks in any concurrent sessions. In other words, the lockdown is not limited to one session; it impacts all sessions associated with a specific user ID. **Warning**: Consider the workflow consequences thoroughly before enabling this feature.
Journal Entry Type	The type of journal entry created by the disconnect action

See also

Inactivity Session Configuration Reports

ISL Disconnect Options

This report displays disconnection options.

Collector ID: ISL_DISCONNECT_OPTIONS

Report ID: ISL_DISCONNECT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Inactivity Session Disconnect Options).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Disconnect Option	Name assigned to the disconnect option **Note**: ***Default** represent the default disconnect option defined for all object.
Disconnect Time Limit (Minutes)	Amount of time the system must remain inactive to trigger a disconnect
Disconnect Type	The type of disconnect: **ENDJOB** - End the job (user must restart their job) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - End the session (user must restart their session and job)

See also

Inactivity Session Configuration Reports

ISL Inclusion Exclusion Rules

This report displays the list of Inactivity Session Lockdown (ISL) exclusion rules.

Collector ID: ISL_RULES

Report ID: ISL_MONITOR_RULES

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Inactivity Session Inclusion Exclusion Rules).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Rule Type	The type of rule: ***PGM** - Rule that affects a program ***WRKSTN** - Rule that affects a workstation ***SBSD** - Rule that affects a subsystem (e.g., country, region, department) ***CTL** - Rule that affects a controller
Object Name	Name assigned to the object
Object Library	Library in which the object resides
Calendar	Calendar to which the rule applies **Note**: Calendars allow you to restrict when a rule is applicable.

Disconnect Option	The type of disconnect: **ENDJOB** - End the job (user must restart their job) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - End the session (user must restart their session and job)
Rule Acton	Flag indicating whether the rule includes or excludes ***INCLUDE** - Who and what is affected by a rule ***EXCLUDE** - Who and what is not affected by a rule
Rule Description	Description of the rule
Change Time Stamp	Date on which the rule was last updated

See also

Inactivity Session Configuration Reports

Inactivity Session Change Reports

This section contains descriptions of the following reports:

- ISL Configuration Changes
- ISL Disconnect Option Changes
- ISL Rule Changes

See also

Inactivity Session Lockdown Reports

ISL Configuration Changes

This report displays changes made to ISL configuration settings.

Collector ID: DATABASE_AUDITING

Report ID: ISL_CONFIGURATION_SETTINGS

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Inactivity Session Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Inactivity Session Configuration Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Audit Status	Flag indicating whether auditing is enabled: **Y** - Auditing enabled (enable tracking and reporting) **N** - Auditing disabled (disable tracking and reporting)
Audit Journal Name	Journal in which audit data is stored
Audit Journal Library	Library in which the journal resides
Alert Status	Flag identifying whether alerts are enabled (stored in the alert queue): ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Audit Configuration Change	Change made to configuration setting
Alert Message Queue Name	Queue in which alerts message are stored
Alert Message Queue Library	Library in which the queue resides
Check Interval	How often the system check for inactivity (in seconds)
Disconnect Screen Message	Warning message user receives before disconnect action
Disconnect Screen Title	Title that appears in the header of the disconnect message dialog box

Send Warning?	Flag identifying whether a warning message appears: ***YES** - Disconnect message enabled ***NO** - Disconnect message disabled
Warning Interval	How much time before the disconnect occurs should a warning message appear
Revoke Authority	Flag identifying whether a user's authority is revoked after the disconnect action: ***YES** - Enable revoke ***NO** - Disable revoke
Journal Entry Type	Type of journal entry created. In the case of an ISL entry, the value should appear as IL.

See also

Inactivity Session Change Reports

ISL Disconnect Option Changes

This report displays changes to ISL disconnect options.

Collector ID: DATABASE_AUDITING

Report ID: ISL_DISCONNECT_OPTIONS

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Inactivity Session Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Inactivity Session Disconnect Option Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Disconnect Option	Name assigned to the disconnect option
Disconnect Time Limit	Time limit defined for the disconnect option
Disconnect Type	Type of disconnect option: **ENDJOB** - End the job (user must start the job over) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - Signoff from the server

See also

Inactivity Session Change Reports

ISL Rule Changes

This report displays changes to ISL rules.

Collector ID: DATABASE_AUDITING

Report ID: ISL_RULES

To enable this report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactivity Session Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Inactivity Session Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Inactivity Session Rules Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Rule Type	The type of rule: ***PGM** - Rule that affects a program ***WRKSTN** - Rule that affects a workstation ***SBSD** - Rule that affects a subsystem (e.g., country, region, department) ***CTL** - Rule that affects a controller
Object Name	Name assigned to the object
Object Library	Library in which the object resides
Calendar	Calendar to which the rule applies **Note**: Calendars allow you to restrict when a rule is applicable.
Disconnect Option	Name assigned to the disconnect option
Rule Action	Flag identifying whether the rule includes or excludes **INCLUDE*** - Who and what is affected by a rule **EXCLUDE*** - Who and what is not affected by a rule
Rule Description	Description of the rule
Change Time Stamp	Time at which the change took place

See also

Inactivity Session Change Reports

Network Security Reports

This section includes descriptions of the following **Network Security** reports:

- Transaction Reports
- Summary Reports
- Configuration Reports
- Configuration Change Reports

Tip: Refer to the TGSecure User Guide for more information about Network Security.

See also

TGSecure Report Reference Introduction

Transaction Reports

This section contains descriptions of the following reports:

- Central Server Transactions
- Database Server Transactions
- Data Queue Transactions
- DDM Transactions
- File Server Transactions
- Incoming Transactions
- Network Printer Transactions
- Network Transaction FTP
- Network Transaction FTP and REXEC
- Network Transactions
- Network Transaction Showcase
- Remote Command Transactions
- Signon Server Transactions
- Socket Transactions
- Telnet Transactions

See also

Network Security Reports

Central Server Transactions

This report lists attempts to access the central server.

Collector ID: NETWORK _TRANS_CENTRAL, NETWORK _TRANSACTIONS_CENTRAL

Report ID: CENTRAL_SERVER_TRANS_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***CENTRAL**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **10** (Central Server Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Sequence Number	Order in which the remote CENTRAL sever transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the CENTRAL transaction request
System Name	Name of system submitting the CENTRAL transaction request
Receiver	Name of the journal receiver submitting the CENTRAL transaction request
Receiver Library	Name of the journal receiver library submitting the CENTRAL transaction request
Receiver ASP	Name of the journal receiver ASP submitting the CENTRAL transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the CENTRAL transactions. This report should display only CENTRAL transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the CENTRAL transaction
Command Name	Command used to execute the CENTRAL transaction
IP Address	IP address from which the CENTRAL transaction originated
Object Name	Object targeted by the CENTRAL transaction

Object Library	Object library targeted by the CENTRAL transaction
Object Type	Object type targeted by the CENTRAL transaction
Request Details	Information about the requestor

See also

Transaction Reports

Database Server Transactions

This report lists attempts to access the database server.

Collector ID: NETWORK_TRANS_DATABASE, NETWORK_TRANSACTIONS_DATABASE

Report ID: DATABASE_SERVER_TRANS_REPORT

Associated exit points

- QIBM_QZDA_INIT
- QIBM_QZDA_NDB1
- QIBM_QZDA_ROI1
- QIBM_QZDA_SQL1

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***DATABASE**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **7** (Database Server Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote DB sever transaction initiated communication with target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the DB transaction request
System Name	Name of system submitting the DB transaction request
Receiver	Name of the journal receiver submitting the DB transaction request
Receiver Library	Name of the journal receiver library submitting the DB transaction request
Receiver ASP	Name of the journal receiver ASP submitting the DB transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the DB transactions. This report displays only DB server transactions. Valid values included: **DBINIT** - Perform server initiation **DBNDB** - Perform native database request **DBSQL** - Perform SQL requests **DBROI** - Retrieve object information and catalog function **Note:** See the **Network Transactions** report for all server type transactions.

Function Name	Function used to execute the DB transaction
Command Name	Command used to execute the DB transaction
IP Address	IP address from which the DB transaction originated
Object Name	Object targeted by the DB transaction
Object Library	Object library targeted by the DB transaction
Object Type	Object type targeted by the DB transaction
Request Details	Information about the requestor

See also

Transaction Reports

Data Queue Transactions

This report lists attempts to access the data queue server.

Collector ID: NETWORK_TRANS_DATAQ, NETWORK_TRANSACTION_DATAQ

Report ID: DATA_QUEUE_TRANSACTIONS_REPORT

Associated exit point

QIBM_Q2HQ_DATA_QUEUE

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***DTAQ**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **8** (Database Queue Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote DTAQ sever transaction initiated communication with target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the DTAQ transaction request
System Name	Name of system submitting the DTAQ transaction request
Receiver	Name of the journal receiver submitting the DTAQ transaction request
Receiver Library	Name of the journal receiver library submitting the DTAQ transaction request
Receiver ASP	Name of the journal receiver ASP submitting the DTAQ transaction request
Action Status	Status of incoming transactions: *__PASS__ - transaction accepted *__FAIL__ - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the DTAQ transactions. This report should display only DTAQ transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the DTAQ transaction
Command Name	Command used to execute the DTAQ transaction
IP Address	IP address from which the DTAQ transaction originated

Object Name	Object targeted by the DTAQ transaction
Object Library	Object library targeted by the DTAQ transaction
Object Type	Object type targeted by the DTAQ transaction
Request Details	Information about the requestor

See also

Transaction Reports

DDM Transactions

This report lists attempts to access the distributed data management server.

Collector ID: NETWORK_TRANS_DDM, NETWORK_TRANSACTIONS_DDM

Report ID: DDM_TRANSACTIONS_REPORT

Associated exit point

QIBM_QTF_TRANSFER

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***DDM**, enter **2** (Edit).

> **Note**: Some server types have multiple exit points.

7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **14** (DDM Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote DDM sever transaction initiated communication with target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the DDM transaction request
System Name	Name of system submitting the DDM transaction request
Receiver	Name of the journal receiver submitting the DDM transaction request
Receiver Library	Name of the journal receiver library submitting the DDM transaction request
Receiver ASP	Name of the journal receiver ASP submitting the DDM transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the DDM transactions. This report should display only DDM transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the DDM transaction
Command Name	Command used to execute the DDM transaction

IP Address	IP address from which the DDM transaction originated
Object Name	Object targeted by the DDM transaction
Object Library	Object library targeted by the DDM transaction
Object Type	Object type targeted by the DDM transaction
Request Details	Information about the requestor

See also

Transaction Reports

File Server Transactions

This report lists attempts to access the file server.

Collector ID: NETWORK_TRANS_FILE, NETWORK_TRANSACTIONS_FILE

Report ID: FILE_SERVER_TRANS_REPORT

Associated exit point

QIBM_QPNFS_FILE_SERV

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***FILE**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (File Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote FILE server transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the FILE transaction request
System Name	Name of system submitting the FILE transaction request
Receiver	Name of the journal receiver submitting the FILE transaction request
Receiver Library	Name of the journal receiver library submitting the FILE transaction request
Receiver ASP	Name of the journal receiver ASP submitting the FILE transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the FILE transactions. This report should display only FILE transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the FILE transaction
Command Name	Command used to execute the FILE transaction
IP Address	IP address from which the FILE transaction originated

Object Name	Object targeted by the FILE transaction
Object Library	Object library targeted by the FILE transaction
Object Type	Object type targeted by the FILE transaction
Request Details	Information about the requestor

See also

Transaction Reports

Incoming Transactions

This report lists all incoming transactions, including socket (*SOC) and exit point (*TRN) transactions.

Collector ID: INCOMING_TRANSACTIONS

Report ID: INCOMING_TRANSACTION_REPORT

To display the audit status

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) Refer to the **Audit Status** column.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Incoming Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Remote Trans Type	Valid values include: ***SOC** - Incoming transaction from socket ***TRN** - Incoming transaction from exit point program
Remote User	User initiating the incoming transaction
Remote Server ID	Remote server initiating the incoming transaction
Remote Function ID	Function initiated by the incoming transaction
Remote Command ID	Command initiated by the incoming transaction
Remote IP Address	IP address of the remote server initiating the incoming transaction
Object Name	Object targeted by the incoming transaction
Object Library	Object library targeted by the incoming transaction
Object Type	Object type targeted by the incoming transaction
IFS Object	Integrated File System objects targeted by the incoming transaction

Server Name	Server targeted by the incoming transaction
Action	Status of incoming transactions: *__PASS__ - transaction accepted *__FAIL__ - transaction rejected
Remote Time Stamp	Time at which the remote server attempted communication with the target server.
Remote Trans Count	Repeat entries are suppressed in this report, but a total count is tracked. For example, if a user attempts 5 SIGNON transactions on a single day, only one row will appear in this report for that user, on that day, for that transaction type. However, each transaction is counted and that count appears in the **Remote Trans Count** column. In this example with the SIGNON transactions, the count would appear as 5.

See also

Transaction Reports

Network Printer Transactions

This report lists attempts to access the network printer server.

Collector ID: NETWORK_TRANS_PRINTER, NETWORK_TRANSACTIONS_PRINTER

Report ID: NETWORK_PRINTER_TRANS_REPORT

Associated exit point

QIBM_QNPS_ENTRY

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***NETPRT**, enter **2** (Edit).

> **Note**: Some server types have multiple exit points.

7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **9** (Network Printer Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the NETPRT transaction request
System Name	Name of system submitting the NETPRT transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Identifies the server type. This report should display only NETPRT (Network Printer) server transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function executed by the NETPRT transaction
Command Name	Command executed by the NETPRT transaction
IP Address	IP address from which the NETPRT transaction originated
Object Name	Object targeted by the NETPRT transaction
Object Library	Object library targeted by the NETPRT transaction
Object Type	Object type targeted by the NETPRT transaction

Request Details	Information about the requestor

See also

Transaction Reports

Network Transaction FTP

This report lists attempts to access the FTP server.

Collector ID: NETWORK_TRANS_FTP_REXEC

Report ID: NETWORK_TRANS_FTP_REPORT

Associated exit points

- QIBM_QTMF_CLIENT_REQ
- QIBM_QTMF_SERVER_REQ
- QIBM_QTMF_SVR_LOGON

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***FTP**, enter **2** (Edit).

> **Note**: Some server types have multiple exit points.

7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (FTP Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote FTP server transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the FTP transaction request
System Name	Name of system submitting the FTP transaction request
Receiver	Name of the journal receiver submitting the FTP transaction request
Receiver Library	Name of the journal receiver library submitting the FTP transaction request
Receiver ASP	Name of the journal receiver ASP submitting the FTP transaction request
Action Status	Status of incoming transactions: *__PASS__ - transaction accepted *__FAIL__ - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the FTP transactions. This report should display only FTP transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the FTP transaction

Command Name	Command used to execute the FTP transaction
IP Address	IP address from which the FTP transaction originated
Object Name	Object targeted by the FTP transaction
Object Library	Object library targeted by the FTP transaction
Object Type	Object type targeted by the FTP transaction
Request Details	Information about the requestor

See also

Transaction Reports

Network Transaction FTP and REXEC

This report lists attempts to access the remote execution server.

Collector ID: NETWORK_TRANS_FTP_REXEC, NETWORK_TRANSACTIONS_FTP_REXEC

Report ID: NETWORK_TRANS_LOGON_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***REXEC**, enter **2** (Edit).

> **Note**: Some server types have multiple exit points.

7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **5** (Remote Execution Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the REXEC transaction request
System Name	Name of system submitting the REXEC transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the REXEC transactions. This report should display only REXEC transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the REXEC transaction
Command Name	Command used to execute the REXEC transaction
IP Address	IP address from which the REXEC transaction originated
Object Name	Object targeted by the REXEC transaction
Object Library	Object library targeted by the REXEC transaction
Object Type	Object type targeted by the REXEC transaction
Request Details	Information about the requestor

See also

Transaction Reports

Network Transactions

This report list all attempts to access the network via any server type (e.g., FTP, Telnet, etc.)

Collector ID: NETWORK_TRANSACTIONS

Report ID: NETWORK_TRANSACTIONS_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the desired network, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Network Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the network transaction request
System Name	Name of system submitting the network transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Identifies the server type. Valid values include: **CENTRAL** - Central server **DB*** - Database server **DDM** - Distributed data management server **DTAQ** - Data queue server **FILE** - File server **FTP** - File transfer protocol server **REXEC** - Remote execution server **RMTCMD** - Remote command server **SIGNON** - TCP signon server **TELNET** - Telnet server
Function Name	Function executed by the network transaction
Command Name	Command executed by the network transaction
IP Address	IP address from which the network transaction originated
Object Name	Object targeted by the network transaction
Object Library	Object library targeted by the network transaction

Object Type	Object type targeted by the network transaction
Request Details	Information about the requestor

See also

Transaction Reports

Network Transaction Showcase

This report returns transactions associated with the Showcase exit program.

Collector ID: NETWORK_TRANS_SHOWCASE

Report ID: NETWORK_TRANS_SHOWCASE

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***SHOWCASE**, enter **2** (Edit).

> **Note**: Some server types have multiple exit points.

7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **15** (Showcase Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Sequence Number	Order in which the remote network transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the network transaction request
System Name	Name of system submitting the network transaction request
Receiver	Name of the journal receiver submitting the network transaction request
Receiver Library	Name of the journal receiver library submitting the network transaction request
Receiver ASP	Name of the journal receiver ASP submitting the network transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Identifies the server type. Valid values include: **CENTRAL** - Central server **DB*** - Database server **DDM** - Distributed data management server **DTAQ** - Data queue server **FILE** - File server **FTP** - File transfer protocol server **REXEC** - Remote execution server **RMTCMD** - Remote command server **SIGNON** - TCP signon server **TELNET** - Telnet server
Function Name	Function executed by the network transaction

Command Name	Command executed by the network transaction
IP Address	IP address from which the network transaction originated
Object Name	Object targeted by the network transaction
Object Library	Object library targeted by the network transaction
Object Type	Object type targeted by the network transaction
Request Details	Information about the requestor

See also

Transaction Reports

Remote Command Transactions

This report lists attempts to access the remote command server using distributed program call requests.

Collector ID: NETWORK_TRANS_COMMAND, NETWORK_TRANSACTIONS_COMMAND

Report ID: REMOTE_COMMAND_TRANS_REPORT

Associated exit point

QIBM_QZRC_RMT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***RMTCMD**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **11** (Remote Command Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the RMTCMD transaction request
System Name	Name of system submitting the RMTCMD transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the RMTCMD transactions. This report should display only RMTCMD transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the RMTCMD transaction
Command Name	Command used to execute the RMTCMD transaction
IP Address	IP address from which the RMTCMD transaction originated
Object Name	Object targeted by the RMTCMD transaction
Object Library	Object library targeted by the RMTCMD transaction
Object Type	Object type targeted by the RMTCMD transaction
Request Details	Information about the requestor

See also

Transaction Reports

Signon Server Transactions

This report lists attempts to access the SIGNON server.

Collector ID: NETWORK_TRANS_SIGNON, NETWORK_TRANSACTION_SIGNON

Report ID: REMOTE_COMMAND_TRANS_REPORT

Associated exit point:

QIBM_QZSO_SIGNONSRV

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***SIGNON**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **12** (Signon Server Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the SIGNON transaction request
System Name	Name of system submitting the SIGNON transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the SIGNON transactions. This report should display only REXEC transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the SIGNON transaction
Command Name	Command used to execute the SIGNON transaction
IP Address	IP address from which the SIGNON transaction originated
Object Name	Object targeted by the SIGNON transaction
Object Library	Object library targeted by the SIGNON transaction
Object Type	Object type targeted by the SIGNON transaction
Request Details	Information about the requestor

See also

Transaction Reports

Socket Transactions

This report lists the socket (*SOC) transaction requests.

Collector ID: SOCKET_TRANSACTIONS

Report ID: SOCKET_TRANSACTIONS_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***SOCKET**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Socket Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Sequence Number	Order in which the socket transaction initiated communication with the target server
Type	Journal entry code for the type of transaction
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the socket transaction request
System Name	Name of system submitting the socket transaction request
Receiver	Name of the journal receiver submitting the SIGNON transaction request
Receiver Library	Name of the journal receiver library submitting the SIGNON transaction request
Receiver ASP	Name of the journal receiver ASP submitting the SIGNON transaction request
Current User	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Remote IP Address	IP address of the remote server from which the socket transaction initiated
Port Number	Port number from which the socket transaction initiated
Operation Name	Name of operation number from which the socket transaction initiated
Subsystem Name	Name of the subsystem impacted by the socket transaction
Subsystem Library	Libray in which the subsystem resides
Action	Status of socket transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected

See also

Transaction Reports

Telnet Transactions

This report lists the attempts to access the Telnet server.

Collector ID: NETWORK_TRANS_TELNET, NETWORK_TRANSACTIONS_TELNET

Report ID: TELENET_TRANSACTIONS_REPORT

Associated exit points

- QIBM_QTMF_CLIENT_REQ
- QIBM_QTMF_SERVER_REQ
- QIBM_QTMF_SVR_LOGON

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***TELNET**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Transaction Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **13** (Telnet Transactions Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user submitting the job
Job Number	Number assigned to the job
User Profile	Name of the user submitting the TELNET transaction request
System Name	Name of system submitting the TELNET transaction request
Action Status	Status of incoming transactions: ***PASS** - transaction accepted ***FAIL** - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the TELNET transactions. This report should display only TELNET transactions. **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the TELNET transaction
Command Name	Command used to execute the TELNET transaction
IP Address	IP address from which the TELNET transaction originated
Object Name	Object targeted by the TELNET transaction
Object Library	Object library targeted by the TELNET transaction
Object Type	Object type targeted by the TELNET transaction

Request Details	Information about the requestor

See also

Transaction Reports

Summary Reports

This section contains descriptions of the following reports:

- Socket Summary by Server Report
- Socket Summary by User Report
- Transaction Summary by Server Report
- Transaction Summary by User Report

See also

Network Security Reports

Socket Summary by Server Report

This report displays a summary of socket (*SOC) transactions by server.

Collector ID: SOCKET_SUMMARY_BY_SERVER

Report ID: SOCKET_SUMM_SERVER_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***SOCKET**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Summary Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Socket Summary by Server).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Server Name	Name of socket server

Total Transactions	Total number of incoming transactions attempted on server
Pass Transactions	Number of incoming transactions with a status of *PASS
Failed Transactions	Number of incoming transactions with a status of *FAIL
Passed Percentage	Percentage of incoming transactions with status of *PASS
Rejected Percentage	Percentage of incoming transactions with status of *PASS

See also

Socket Summary by Server Report

Socket Summary by User Report

This report displays a summary of socket (*SOC) transactions by user.

Collector ID: SOCKET_SUMMARY_BY_USER

Report ID: SOCKET_SUMM_USER_REPORT

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.
6) In the **Opt** column for the network server labeled ***SOCKET**, enter **2** (Edit).
7) Enter ***YES** in the **Audit Status** field.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Summary Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Socket Summary by User).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Server Name	Name of the socket server
Total Transactions	Total number of incoming transactions attempted on server
Pass Transactions	Number of incoming transactions with a status of *PASS
Failed Transactions	Number of incoming transactions with a status of *FAIL
Passed Percentage	Percentage of incoming transactions with the status of *PASS
Rejected Percentage	Percentage of incoming transactions with the status of *FAIL

See also

Socket Summary by User Report

Transaction Summary by Server Report

This report displays a summary of incoming transactions (*TRN) by server.

> **Tip**: Only server types with the **Audit Status** set to ***YES** will appear in this report.

Collector ID: REMOTE_TRAN_SUMMARY_BY_SERVER

Report ID: REMOTE_SUMM_SERVER_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Summary Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Transaction Summary by Server).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Server Name	Name of the transaction server
Total Transactions	Total number of incoming transactions attempted on server
Pass Transactions	Number of incoming transactions with a status of *PASS
Failed Transactions	Number of incoming transactions with a status of *FAIL
Passed Percentage	Percentage of incoming transactions with the status of *PASS
Rejected Percentage	Percentage of incoming transactions with the status of *FAIL

See also

Transaction Summary by Server Report

Transaction Summary by User Report

This report displays a summary of incoming transactions (*TRN) by user.

Tip: Only server types with the **Audit Status** set to ***YES** will appear in this report.

Collector ID: REMOTE_TRAN_SUMMARY_BY_USER

Report ID: REMOTE_SUMM_USER_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Summary Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Transaction Summary by User).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Server Name	Name of the transaction server
Total Transactions	Total number of incoming transactions attempted on server
Pass Transactions	Number of incoming transactions with a status of *PASS
Failed Transactions	Number of incoming transactions with a status of *FAIL
Passed Percentage	Percentage of incoming transactions with the status of *PASS
Rejected Percentage	Percentage of incoming transactions with the status of *FAIL

See also

Transaction Summary by User Report

Configuration Reports

This section contains descriptions of the following reports:

Rules

- Exit Point Configuration Report
- Remote Exit Rules Report
- Socket Rules Report

Groups

- Network Groups
- Object Groups
- Operation Groups
- User Groups

See also

Network Security Reports

Exit Point Configuration Report

This report displays configuration details for all available exit points.

Collector ID: NETWORK_EXIT_CONFIG

Report ID: EXIT_POINT_CONFIG_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Server Name	Type of server
Exit Point	Name of Exit point
Exit Format	Exit format
Exit Point Description	Description of exit point
Exit Program	Name of associated exit program
Exit Program Library	Library location of exit program
Exit Program Journal	Type of journal
Collection Status	Is collector enabled

Audit On?	Flag indicating whether auditing is enabled: ***YES** - Auditing is enabled, so transactions are tracked ***NO** - Auditing is disabled, so transactions are not tracked
Security On?	Flag indicating whether exit point security is enabled: ***YES** - Security monitoring is enabled, so rules are applied ***NO** - Security monitoring is disabled, so rules are not applied

See also

Configuration Reports

Remote Exit Rules Report

This report displays configuration details for all available remote exit rules.

Collector ID: NETWORK_TRAN_RULES

Report ID: REMOTE_EXIT_RULES_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Remote Exit Rules Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Remote User	Remote user (or group) to which the exit rule applies
Remote Server	Remote server to which the exit rule applies
Remote Function	Remote function to which the exit rule applies
Remote Command	Remote command to which the exit rule applies
Remote IP Address	Remote IP address to which the exit rule applies
Object Name	Object (or group) to which the exit rule applies
Object Library	Object library to which the exit rule applies
Object Type	Object type to which the exit rule applies
IFS Object	IFS object to which the exit rule applies

Server Name	Server (or group) to which the exit rule applies
Action	Action executed if exit rule criteria is met
Alert Status	Flag indicating whether notification alerts are supported
Date Time Restriction	Calendar criteria used to limit when the socket rule applies
Rule Description	Description of exit rule
Change Time Stamp	Date on which the exit rule was last updated

See also

Configuration Reports

Socket Rules Report

This report displays configuration details for all available socket rules.

Collector ID: SOCKET_TRAN_RULES

Report ID: SOCKET_RULES_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Socket Rules Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Remote User	Remote user (or group) to which the socket rule applies
Remote Port	Remote ports to which the socket rule applies
Remote Operation	Remote operations to which the socket rule applies
Remote IP Address	Remote IP address to which the socket rule applies
Server Name	Server to which socket rule applies
Action	Action executed if socket rule criteria is met
Alert Status	Flag indicating whether notification alerts are supported
Date Time Restriction	Calendar criteria used to limit when the socket rule applies
Rule Description	Description of socket rule

Change Time Stamp	Date on which the socket rule was last updated

See also

Configuration Reports

Configuration Change Reports

This section contains descriptions of the following reports:

Rules

- Exit Point Configuration Changes
- Remote Exit Rules Changes
- Socket Rules Changes

Groups

- Network Groups Changes
- Object Groups Changes
- Operation Groups Changes
- User Groups Changes

See also

Network Security Reports

Exit Point Configuration Changes

This report displays all changes made to exit point configurations.

Collector ID: DATABASE_AUDITING

Report ID: EXIT_POINT_CONFIGURATION

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Server Name	Type of server
Exit Point	Name of Exit point
Exit Format	Exit format
Exit Point Description	Description of exit point
Exit Program	Name of associated exit program
Exit Program Library	Library location of exit program
Exit Program Journal	Type of journal
Collection Status	Is collector enabled
Audit On?	Flag indicating whether auditing is enabled: ***YES** - Auditing is enabled, so transactions are tracked ***NO** - Auditing is disabled, so transactions are not tracked
Security On?	Flag indicating whether exit point security is enabled: ***YES** - Security monitoring is enabled, so rules are applied ***NO** - Security monitoring is disabled, so rules are not applied

See also

Configuration Change Reports

Remote Exit Rules Changes

This report displays all changes made to remote exit rule configurations.

Collector ID: DATABASE_AUDITING

Report ID: REMOTE_EXIT_RULES_CHANGES

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Remote Exit Rules Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Remote User	Remote user (or group) to which the exit rule applies
Remote Server	Remote server to which the exit rule applies
Remote Function	Remote function to which the exit rule applies
Remote Command	Remote command to which the exit rule applies
Remote IP Address	Remote IP address to which the exit rule applies
Object Name	Object (or group) to which the exit rule applies
Object Library	Object library to which the exit rule applies
Object Type	Object type to which the exit rule applies
IFS Object	IFS object to which the exit rule applies
Server Name	Server (or group) to which the exit rule applies
Action	Action executed if exit rule criteria is met
Alert Status	Flag indicating whether notification alerts are supported
Date Time Restriction	Calendar criteria used to limit when the socket rule applies

Rule Description	Description of exit rule
Change Time Stamp	Date on which the exit rule was last updated

See also

Configuration Change Reports

Socket Rules Changes

This report displays all changes made to socket rule configurations.

Collector ID: DATABASE_AUDITING

Report ID: SOCKET_RULES_CHANGES

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
7) Press **Enter**.
8) Enter **Y** in the **Audit Configuration Changes** field.
9) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Socket Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Remote User	Remote user (or group) to which the socket rule applies
Remote Port	Remote ports to which the socket rule applies
Remote Operation	Remote operations to which the socket rule applies
Remote IP Address	Remote IP address to which the socket rule applies
Server Name	Server to which socket rule applies
Action	Action executed if socket rule criteria is met
Alert Status	Flag indicating whether notification alerts are supported
Date Time Restriction	Calendar criteria used to limit when the socket rule applies
Rule Description	Description of socket rule
Change Time Stamp	Date on which the socket rule was last updated

See also

Configuration Change Reports

Resource Manager Reports

This section includes descriptions of the following **Resource Manager** reports:

- Resource Manager Usage Reports
- Resource Manager Configuration Reports
- Resource Manager Change Reports

> **Tip**: Refer to the TGSecure User Guide for more information about the Resource Manager.

See also

TGSecure Report Reference Introduction

Resource Manager Usage Reports

This section contains descriptions of the following reports:

- Authority Collection for IFS Objects
- Authority Collection for Native Objects
- Authority Compliance Report

See also

Resource Manager Reports

Authority Collection for IFS Objects

This report displays authority data collected for Integrated File System (IFS) file systems.

> **Note**: IFS a newer file management structure that supports stream input/output and is similar to the structure used by personal computers and UNIX operating systems.
>
> For more information about IBM file systems, refer to the IBM Knowledge Center.

Collector ID: AUTHORITY_COLLECTION

Report ID: AUTHORITY_IFS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Authority Collection Report IFS).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Authorization Name	Authority collection name
Check Timestamp	Time at which the change took place
Path Name	IFS path

System Object Type	Type of system object ***BLKSF** - Block files ***CHRSF** - Character files ***DIR** - Directories ***FIFO** - First-in-first-out special files ***SOCKET** - Socket files ***STMF** - Steam files ***SYMLNK** - Symbolic links
Authorization List	Name of the authority list **Note**: An authority list identifies the users who have authority to a specific object.
Authority Check Successful	Flag indicating whether the check was successful
Detailed Required Authority	Minimum object access authority level: ***OBJALTER** - Object alter ***OBJEXIT** - Object exists ***OBJMGT** - Object management ***OBJOPR** - Object operation ***OBJREF** - Object reference Minimum data access authority level: ***ADD** - Add ***DLT** - Delete ***EXECUTE** - Execute ***READ** - Read For more information about IBM object authorities, refer to the IBM Knowledge Center.
Detailed Current Authority	Authority level currently defined for the user
Authority Source	User and objects evaluated
Most Recent Program Invoked	Last program invoked by the user
Most Recent Program Schema	Schema used to conduct the authority level check
Job Name	Name of the job (code + number)
Job User	Name of job user
Job Number	Number assigned to job

See also

Resource Manager Usage Reports

Authority Collection for Native Objects

This report displays authority data collected for QSYS.Lib (tradition) file types.

> **Note**: QSYS the traditional file management structure used to control the storing and accessing of traditional file objects (*FILE objects in the QSYS.LIB library).
>
> For more information about IBM file systems, refer to the IBM Knowledge Center.

Collector ID: AUTHORITY_COLLECTION

Report ID: AUTHORITY_OBJECTS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Authority Collection Report QSYS).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Authorization Name	Authority collection name
Check Timestamp	Time at which the check took place
Path Name	IFS path
System Object Type	Type of system object

ASP Name	Name of the ASP (Auxiliary Storage Pool) or ***SYSBAS** **Note**: If ***SYSBAS** appear, then the system ASP and all basic user ASPs are searched to locate the object.
Authorization List	Name of the authority list **Note**: An authority list identifies the users who have authority to a specific object.
Authority Check Successful	Identifies whether the check was successful
Detailed Required Authority	Minimum object access authority level: ***OBJALTER** - Object alter ***OBJEXIT** - Object exists ***OBJMGT** - Object management ***OBJOPR** - Object operation ***OBJREF** - Object reference Minimum data access authority level: ***ADD** - Add ***DLT** - Delete ***EXECUTE** - Execute ***READ** - Read For more information about IBM object authorities, refer to the IBM Knowledge Center.
Detailed Current Authority	Authority level currently defined for the user
Most Recent Program Invoked	Last program invoked by the user
Most Recent Program Schema	Schema used to conduct the authority level check
Job Name	Name of the job (code + number)
Job User	Name of job user
Job Number	Number assigned to the job

See also

Resource Manager Usage Reports

Authority Compliance Report

This report displays compliance details.

Collector ID: AUTHORITY_COMPLIANCE

Report ID: AUTHORITY_COMPLIANCE_REPORT

To start (enable) authority collection

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**.
7) Press the **F6** (Start Collection) function key on your keyboard.
8) Complete the fields as necessary.

To run authority compliance for a single schemas

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**.
6) In the **OPT** column for the desired schema, enter **22** (Run Compliance Report).
7) Press **Enter**.
8) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

9) Press **Enter**.

To run authority compliance for all schemas

> **Note**: Running authority compliance for all reports might take a lot time and system resources.

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **1** (Authority Compliance Report).

9) Press **Enter**.

10) Modify the run criteria as necessary.

11) Press **Enter**.

Report Column Description

Column	Description
Schema ID	Name assigned to the schema
File System	File system type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types ***NONE** - No file system defined **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center
IFS Path	Path to the IFS system (if applicable)
Auxiliary Storage Pool	ASP to which this authority schema applies or enter ***SYSBAS** (if applicable) **Note**: If ***SYSBAS** appears, then the system ASP and all basic user ASPs are searched to locate the object.
Library Name	Name of the specific library or ***ALL** to indicate all libraries
Object Name	Name of the object or ***ALL** to indicate all objects
Object Type	Name of object type or ***ALL** to indicate all types
Authority List	Name of the authority list **Note**: An authority list identifies the users who have authority to a specific object.
Schema Authority List	Authority list recommended by schema
Program Adopt	Program adopt status for the current state
Schema Program Adopt	Program adopt status recommended by schema
Program Adopt Users	Program adopt user for the current state

Schema Program Adopt Users	Program adopt user recommended by schema
Object Owner	Object owner for the current state
Schema Object Owner	Object owner recommended by schema
User Inheritance Group	User Inheritance group for the current state
Schema User Inheritance Group	User Inheritance group recommended by schema
User Name	User name for the current state
Schema User Name	User name f recommended by schema
Object Authority	Object authority for the current state
Schema Object Authority	Object authority recommended by schema
Data Read	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Read (*__READ__) authority provides the authority needed to get the contents of an entry in an object or to run a program.
Schema Data Read	If an **X** appears in this cell, it indicates a recommended feature
Data Add	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Add (*__ADD__) authority provides the authority to add entries to an object (for example, job entries to a queue or records to a file).
Schema Data Add	If an **X** appears in this cell, it indicates a recommended feature
Data Update	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Update (*__UPDATE__) authority provides the authority to change the entries in an object.
Schema Data Update	If an **X** appears in this cell, it indicates a recommended feature
Data Delete	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Delete (*__DELETE__) authority provides the authority to remove entries from an object.
Schema Data Delete	If an **X** appears in this cell, it indicates a recommended feature

Data Execute	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Execute (*__EXECUTE__) authority provides the authority needed to run a program or locate an object in a library.
Schema Data Execute	If an **X** appears in this cell, it indicates a recommended feature
Object Operation	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Object operational (*__OBJOPR__) provides the authority to look at the description of an object and use the object as determined by the data authority that the user has to the object.
Schema Object Operation	If an **X** appears in this cell, it indicates a recommended feature
Object Management	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Object management (*__OBJMGT__) provides the authority to move or rename the object and add members to database files.
Schema Object Management	If an **X** appears in this cell, it indicates a recommended feature
Object Exists	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Object existence (*__OBJEXIST__) provides the authority to control the object's existence and ownership.
Schema Object Exists	If an **X** appears in this cell, it indicates a recommended feature
Object Alter	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Object alter (*__OBJALTER__) authority provides the authority needed to alter the attributes of an object.
Schema Object Alter	If an **X** appears in this cell, it indicates a recommended feature
Object Reference	If an **X** appears in this cell, it indicates a feature enabled in the current state **Note**: Object reference (*__OBJREF__) authority provides the authority needed to reference an object from another object.
Schema Object Reference	If an **X** appears in this cell, it indicates a recommended feature
Row Column Access Control	For informational use only. This level (granularity) of user access is not currently addressed by schemas
Field Procedure	For informational use only. This level (granularity) of user access is not currently addressed by schemas

Out of Compliance Reason	First reason the system encountered in which the current state does not align with the recommended state **Note**: Review the report for a complete understanding of the misalignment of the current state with the recommended state.

See also

Resource Manager Usage Reports

Resource Manager Configuration Reports

This section contains descriptions of the following reports:

- Resource Manager Configuration
- Resource Manager out of Compliance Data
- Resource Manager Schema Details
- Resource Manager Schema Header

See also

Resource Manager Reports

Resource Manager Configuration

This report displays the Resource Manager configuration details.

Collector ID: RSC_MGR_CONFIG

Report ID: RSC_MGR_CONFIG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Resource Manager Configuration).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Audit Status	Flag indicating whether auditing is enabled: **Y** - Auditing enabled (enable tracking and reporting) **N** - Auditing disabled (disable tracking and reporting)
Audit Journal Name	Name of the journal in which Resource Manager transactions are stored **Note**: The default journal is **TGJRN** in the library **TGDATA**.
Audit Journal Library	Library in which the journal resides
Alert Status	Flag indicating whether alerting is enabled: **Y** - Alerting is enabled **N** - Alerting is disabled
Alert Message Queue Name	Name of the message queue **Note**: The default alert queue is **TGMSGQ** in the library **TGDATA**.

Alert Message Queue Library	Library in which queue resides

See also

Resource Manager Configuration Reports

Resource Manager out of Compliance Data

This report displays the authorities that are out of compliance (do not align with a defined schema).

Collector ID: RSC_MGR_COMPLIANCE_DATA

Report ID: RSC_MGR_COMPLIANCE_DATA

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Resource Manager out of Compliance Data).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Schema ID	Name assigned to the schema
File System	File system type: ***SYS** - QSYS.Lib (tradition, single-library structure) ***IFS** - Integrated File System (newer, multi-node structure) ***NONE** - No file system defined **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center
IFS Path	Path to the IFS system (if applicable)
Auxiliary Storage Pool	ASP to which this authority schema applies or enter ***SYSBAS** (if applicable) **Note**: If ***SYSBAS** appears, then the system ASP and all basic user ASPs are searched to locate the object.

Library Name	Name of the specific library or ***ALL** to indicate all libraries
Object Name	Name of the object or ***ALL** to indicate all objects
Object Type	Name of object type or ***ALL** to indicate all types
Authority List	Name of the authority list **Note**: An authority list identifies the users who have authority to a specific object.
Program Adopt	Program adopt status for the current state
Program Adopt User	Program adopt status recommended by schema
Object Owner	Object owner for the current state
Object Primary Group	Primary group to which the object is assigned
User Name	Name of the user whose authority was changed
User Inheritance Group	Folders (and objects in the folders) can inherit user and group permissions, or the administrator can break the inheritance and make all the permissions/authorities manually set. **Note**: This field is only valid for ***IFS** file systems because ***SYS** file systems have a single-library structure; whereas IFS file systems can have a multi-level node structure. Therefore permission inheritance might be useful.
Object Authority	Authority level: ***ALL** - All authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object) ***AUTL** - Grant public users the default level of authority specified for the authority list
Data Read	If an **X** appears in this cell, it indicates an enabled feature **Note**: Read (***READ**) authority provides the authority needed to get the contents of an entry in an object or to run a program.

See also

Resource Manager Configuration Reports

Resource Manager Schema Details

This report displays the Resource Manager schema details.

Collector ID: RSC_MGR_SCHEMA_DETAILS

Report ID: RSC_MGR_SCHEMA_DETAILS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Schema ID	Name assigned to the schema
Schema Defaults	Flag identifying this is the default schema ***YES** - This entry is an exception ***NO** - This entry is a default (base rule)
File System	File system type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types ***NONE** - No file system defined **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center
IFS System	Path to the IFS system (if applicable)

Auxiliary Storage Pool	ASP to which this authority schema applies or enter ***SYSBAS** (if applicable) **Note**: If you enter ***SYSBAS** the system ASP and all basic user ASPs will be searched to locate the object. No independent ASPs will be searched, even if the job has an ASP group.
Library Name	Name of the specific library or ***ALL** to indicate all libraries
Object Name	Name of the object or ***ALL** to indicate all objects
Object Type	Name of object type or ***ALL** to indicate all types
User Name	Name of the user
Object Operation	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object operational (***OBJOPR**) authority provides authority to look at the description of an object and use the object as determined by the data authority that the user has to the object.
Object Managem ent	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object management (***OBJMGT**) authority provides the authority to move or rename the object and add members to database files.
Object Exists	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object existence (***OBJEXIST**) authority provides the authority to control the object's existence and ownership.
Object Alter	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object alter (***OBJALTER**) authority provides the authority needed to alter the attributes of an object.
Object Reference	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object reference (***OBJREF**) authority provides the authority needed to reference an object from another object.

See also

Resource Manager Configuration Reports

Resource Manager Schema Header

This report displays Resource Manager schema header details.

Collector ID: RSC_MGR_SCHEMA_HEADER

Report ID: RSC_MGR_SCHEMA_HEADER

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Schema ID	Name assigned to the schema
Schema Description	Description assigned to the schema
Compliance Status	Flag indicating whether current authority levels defined in the system align with the schema ***FAIL** - There are discrepancies ***PASS** - There are no discrepancies (authority levels and schema align)
Alerting Status	Flag indicating whether alerting is enabled: **Y** - Alerting is enabled **N** - Alerting is disabled
Last Enforcement Date and Time	Timestamp of last enforcement check
Last Compliance Date and Time	Timestamp of last compliance check

See also

Resource Manager Configuration Reports

Resource Manager Change Reports

This section contains descriptions of the following reports:

- Rsc Manager Configuration Changes
- Rsc Manager out of Compliance Data Changes
- Rsc Manager Schema Details Changes
- Rsc Manager Schema Header Changes

See Also

Resource Manager Reports

Rsc Manager Configuration Changes

This report displays changes made to the resource manager configuration settings.

Collector ID: DATABASE_AUDITING

Report ID: RSC_MGR_CONFIG_CHANGES

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Resource Manager Configuration Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Audit Status	Flag identifying whether auditing is enabled: **Y** - Auditing enabled **N** - Auditing disabled
Audit Journal Name	Journal in which audit data is stored **Note**: The default journal is **TGJRN** in the library **TGDATA**.
Audit Journal Library	Library in which the journal resides
Alert Status	Flag identifying whether alerting is enabled: **Y** - Alerting enabled **N** - Alerting disabled
Alert Message Queue Name	Queue in which alerts message are stored **Note**: The default alert queue is **TGMSGQ** in the library **TGDATA**.
Alert Message Queue Library	Library in which the queue resides

See also

Resource Manager Change Reports

Rsc Manager out of Compliance Data Changes

This report displays changes made to data found to be out of compliance.

Collector ID: DATABASE_AUDITING

Report ID: RSC_MGR_COMPLIANCE_DATA_CHANGE

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Resource Manager out of Compliance Data Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.
11) Press **Enter**.

Report Column Description

Column	Description
Schema ID	Name assigned to the schema

File System	File system type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types ***NONE** - No file system defined **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center
IFS Path	Path to the IFS system (if applicable)
Auxiliary Storage Pool	ASP to which this authority schema applies or enter ***SYSBAS** (if applicable) **Note**: If ***SYSBAS** appears, then the system ASP and all basic user ASPs are searched to locate the object.
Library Name	Name of the specific library or ***ALL** to indicate all libraries
Object Name	Name of the object or ***ALL** to indicate all objects
Object Type	Name of object type or ***ALL** to indicate all types
Authority List	Name of the authority list **Note**: An authority list identifies the users who have authority to a specific object.
Program Adopt	Program adopt status for the current state
Program Adopt User	Program adopt status recommended by schema
Object Owner	Object owner for the current state
Object Primary Group	Primary group to which the object is assigned
User Name	Name of the user whose authority was changed
User Inheritance Group	Name of inheritance group
Object Authority	Authority level: ***ALL** - All authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object) ***AUTL** - Grant public users the default level of authority specified for the authority list
Data Read	If an **X** appears in this cell, it indicates an enabled feature **Note**: Read (***READ**) authority provides the authority needed to get the contents of an entry in an object or to run a program.

See also

Resource Manager Change Reports

Rsc Manager Schema Details Changes

This report displays changes made to the schema details.

Collector ID: DATABASE_AUDITING

Report ID: RSC_MGR_SCHEMA_DETAILS_CHANGES

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Schema ID	Name assigned to the schema
Schema Defaults	Flag identifying this is the default schema ***YES** - This entry is an exception ***NO** - This entry is a default (base rule)
File System	File system type ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center
IFS Path	Path to the IFS system (if applicable)
Auxiliary Storage Pool	Enter the ASP to which this authority schema applies or enter ***SYSBAS** (if applicable)
Library Name	Name of the library or ***ALL** for all libraries
Object Name	Name of the object or ***ALL** for all objects
Object Type	Name of the object type or ***ALL** for all object types

Authority List	Name of the authority list or ***NONE** **Note**: An authority list identifies the users who have authority to specific objects.
Program Adopt	Flag identifying whether the program is allowed to adopt user authorities ***YES** - Enable the program to adopt the authorities from the previous program ***NO** - Disable the program from adopting the authorities from the previous programs
Program Adopt Users	Name of the user whose authorities the program should adopt (if applicable)
Object Owner	Name of the object owner
Object Primary Group	Primary group to which the object is assigned
User Name	Name of the user whose authority was changed
User Inheritance Group	Name of user inheritance group
Object Authority	Authority level: ***ALL** - All authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object) ***AUTL** - Grant public users the default level of authority specified for the authority list
Data Read	If an **X** appears in this cell, it indicates an enabled feature **Note**: Read (***READ**) authority provides the authority needed to get the contents of an entry in an object or to run a program.
Data Add	If an **X** appears in this cell, it indicates an enabled feature **Note**: Add (***ADD**) authority provides the authority to add entries to an object (for example, job entries to a queue or records to a file).
Data Update	If an **X** appears in this cell, it indicates an enabled feature **Note**: Update (***UPDATE**) authority provides the authority to change the entries in an object.
Data Delete	If an **X** appears in this cell, it indicates an enabled feature **Note**: Delete (***DELETE**) authority provides the authority to remove entries from an object.
Data Execute	If an **X** appears in this cell, it indicates an enabled feature **Note**: Execute (***EXECUTE**) authority provides the authority needed to run a program or locate an object in a library.
Object Operation	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object operational (***OBJOPR**) authority provides the authority to look at the description of an object and use the object as determined by the data authority that the user has to the object.

Object Management	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object management (*__OBJMGT__) authority provides the authority to move or rename the object and add members to database files.
Object Exits	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object existence (*__OBJEXIST__) authority provides the authority to control the object's existence and ownership.
Object Alter	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object alter (*__OBJALTER__) authority provides the authority needed to alter the attributes of an object.
Object Reference	If an **X** appears in this cell, it indicates enabled object authority **Note**: Object reference (*__OBJREF__) authority provides the authority needed to reference an object from another object.
Row Column Access Control	For informational use only. This level of user access is not currently addressed by schemas
Field Procedure	For informational use only. This level of user access is not currently addressed by schemas

See also

Resource Manager Change Reports

Rsc Manager Schema Header Changes

This report displays changes made to the schema header (title/name).

Collector ID: DATABASE_AUDITING

Report ID: RSC_MGR_SCHEMA_HEADERS_CHANGES

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Schema ID	Name assigned to the schema
Schema Description	Description assigned to the schema
Compliance Status	Flag indicating whether current authority levels defined in the system align with the schema ***FAIL** - There are discrepancies ***PASS** - Authority levels and schema align
Alerting Status	Flag indicating whether alerting is enabled: ***YES** - Alerting is enabled ***NO** - Alerting is disabled
Last Enforcement Date and Time	Timestamp of last enforcement check
Last Compliance Date and Time	Timestamp of last compliance check

See also

Resource Manager Change Reports

User Profile Reports

This section includes descriptions of the following **User Profile** reports:

- User Profile Usage Reports
- User Profile Configuration Reports
- User Profile Change Reports

> **Tip**: Refer to the TGSecure User Guide for more information about User Profiles.

See also

TGSecure Report Reference Introduction

User Profile Usage Reports

This section contains descriptions of the following reports:

- Authority Failures
- Blueprint Compliance Report
- Invalid Sign-on Attempts
- Profile Compliance Report
- User Profile Activity For User: *ALL
- User Profile Changes
- User Profile via Blueprint For User: *ALL

See also

User Profile Reports

Authority Failures

This report displays authority failures that have occurred in the system. The data displayed in this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with these events is AF.

Collector ID: JOURNAL_AF

Report ID: *BASE

> **Tip**: For AF journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL and *PGMFAIL.

PASS = AF journal entries were not found in QAUDJRN.

FAIL = AF journal entries were found in QAUDJRN.

Types of failures:

A - Not authorized to object

B - Restricted instruction

C - Validation failure

D - Use of unsupported interface, object domain failure

E - Hardware storage protection error, program constant space violation

F - ICAPI authorization error

G - ICAPI authentication error

H - Scan exit program

I - System Java inheritance not allowed

J - Submit job profile error

K - Special authority violation

N - Profile token not a regenerable token

O - Optical Object Authority Failure

P - Profile swap error

R - Hardware protection error

S - Default sign-on attempt

T - Not authorized to TCP/IP port

U - User permission request not valid

V - Profile token not valid for generating new profile token

W - Profile token not valid for swap

X - System violation

Y - Not authorized to the current JUID field during a clear JUID operation.

Z - Not authorized to the current JUID field during a set JUID operation

To run this report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **7** (All Authority Failures).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

See Also

User Profile Usage Reports

Blueprint Compliance Report

This report displays blueprint compliance.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Blueprint Compliance Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
User Name	Name of user
Violation Category	Type of violation
Violation Keyword	Parameter that is in violation (does not match value defined in blueprint)
Violation Description	Short description of parameter violation
Current Value	Current value set for parameter (which does not match value defined in blueprint)
Blueprint Value	Value defined in blueprint
Non-Compliance Reason	Long description parameter violation

See Also

User Profile Usage Reports

Invalid Sign-on Attempts

This report displays password validation failures. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PW.

Collector ID: JOURNAL_PW

Report ID: *BASE

> **Tip**: For PW journal entries to be generated, the QAUDLVL system value must contain *AUTFAIL.

PASS = PW Journal entries were not found in QAUDJRN.

FAIL = PW Journal entries were found in QAUDJRN.

Types of failures:

A - APPC bind failure.

C - User authentication with the CHKPWD command failed.

D - Service tools user ID name not valid.

E - Service tools user ID password not valid.

P - Password not valid.

Q - Attempted sign-on (user authentication) failed because the user profile is disabled.

R - Attempted sign-on (user authentication) failed because the password was expired. This audit record might not occur for some user authentication mechanisms. Some authentication mechanisms do not check for expired passwords.

S - SQL Decryption password is not valid.

U - User name not valid.

X - Service tools user ID is disabled.

Y - Service tools user ID not valid.

Z - Service tools user ID password not valid.

To run this report

1) Access the TGSecure main menu.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (User Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **5** (Invalid Sign-on Attempts).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

See Also

User Profile Usage Reports

Profile Compliance Report

This report displays inactivity compliance sorted by the username.

Collector ID: PROFILE_COMPLIANCE

Report ID: PROFILE_COMPLIANCE_REPORT

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Inactivity Compliance Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
User Name	Name of user
Violation Category	Type of violation
Violation Keyword	Parameter that is in violation (does not match value defined in blueprint)
Violation Description	Short description of parameter violation
Current Value	Current value set for parameter (which does not match value defined in blueprint)
Blueprint Value	Value defined in blueprint
Non-Compliance Reason	Long description parameter violation

See Also

User Profile Usage Reports

User Profile Activity For User: *ALL

This report displays profile activity.

> **Tip**: See the IBM knowledge base for descriptions of the collector ID parameters (which appear as columns in this report).

Collector ID: USER_PROFILE_ACTIVITY

Report ID: USER_PROFILE_ACTIVITY

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (User Profile Activity).
9) Press **Enter**.
10) Modify the run criteria as necessary.
11) Press **Enter**.

See Also

User Profile Usage Reports

User Profile Changes

This report displays changes to user profiles on the system. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is CP.

Collector ID: JOURNAL_CP

Report ID: *BASE

> **Tip**: For CP journal entries to be generated, the QAUDLVL system value must contain *SECCFG and *SECURITY.

PASS = CP Journal entries were not found in QAUDJRN.

FAIL = CP Journal entries were found in QAUDJRN.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (User Profile Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

See Also

User Profile Usage Reports

User Profile via Blueprint For User: *ALL

This report displays profile activity categorized by the blueprint.

> **Tip**: See the IBM knowledge base for descriptions of the collector ID parameters (which appear as columns in this report).

Collector ID: USER_PRF_VIA_BLUEPRINT

Report ID: USER_PRF_VIA_BLUEPRINT

To run this report

1) Access the TGSecure main menu.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (User Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **3** (User Profile Create/Changes via TGPRFMGR).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

See Also

User Profile Usage Reports

User Profile Configuration Reports

This section contains descriptions of the following reports:

- Blueprint 3rd Party Integration File
- Blueprint Authority List Settings File
- Blueprint Master
- Blueprint Non-Compliance User Profiles
- Blueprint Object Authority File
- Blueprint Parameter File
- Blueprint Permissions File
- Profile Inactivity Settings
- Profile Manager Defaults
- User Profile Archive
- User Profile Exclusions

See also

User Profile Reports

Blueprint 3rd Party Integration File

This report displays 3rd party scripts used for user profile integration purposes.

Collector ID: BLUEPRINT_3RD_PARTY_FILE

Report ID: BLUEPRINT_3RD_PARTY_FILE

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
Script Type	Script type
Script Statement	Script text

See also

User Profile Configuration Reports

Blueprint Authority List Settings File

This report displays authority list settings defined for a blueprint.

Collector ID: BLUEPRINT_AUTH_SETTINGS_FILE

Report ID: BLUEPRINT_AUTH_SETTINGS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **5** (Blueprint Authority List Settings File).
9) Press **Enter**.
10) Modify the run criteria as necessary.
11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
Authority List	Authority list assigned to the blueprint
Object Authority	Object authority

See also

User Profile Configuration Reports

Blueprint Master

This report displays blueprint details.

Collector ID: BLUEPRINT_MASTER

Report ID: BLUEPRINT_MASTER

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Blueprint Master).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
User Group	Name of user group assigned to blueprint master **Note**: Modifications made to the blueprint impact this user group.
Blueprint Description	Description of blueprint
Profile Parameters?	Flag indicating whether profile parameters are defined
Profile Authorities?	Flag indicating whether profile authorities are defined
Authority List?	Flag indicating whether profile authorities are defined
3rd Party Integration?	Flag indicating whether 3rd party scripts are defined
Blueprint Alert?	Flag indicating whether alerts are enabled
Inactive Override?	Flag indicating whether inactivity overrides are defined

Inactive Profiles?	Flag indicating whether inactive profiles were identified
Compliance Date	Date on which the blueprint came into effect
Compliance Status	Flag indicating whether all profiles associated with the blueprint are in compliance
Inactivity before Disabled	Number of days the profile was inactive before it was disabled
Inactivity before Delete	Number of days the profile was inactive before it was deleted
Object owner for deleted profiles	Name of the user to whom object ownership was transferred upon deletion of the profile

See also

User Profile Configuration Reports

Blueprint Non-Compliance User Profiles

This report displays user profiles that do not comply with the blueprint.

Collector ID: BLUEPRINT_NON_COMPLIANCE_USER

Report ID: BLUEPRINT_NON_CMPL

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (Blueprint Non-Compliance User Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
User Name	Name of user
Violation Category	Type of violation
Violation Keyword	Keyword associated with the profile parameter
Violation Description	Description associated with the profile parameter
Current Value	Parameter value defined in the user's profile
Blueprint Value	Parameter value defined in the blueprint
Non-Compliance Reason	Description of violation

See also

User Profile Configuration Reports

Blueprint Object Authority File

This report displays the object authorities define for a blueprint.

Collector ID: BLUEPRINT_OBJECT_AUTH_FILE

Report ID: BLUEPRINT_OBJECT_AUTH_FILE

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
Profile Object Owner	Object owner
Profile Object Owner Authority	Authority granted owner
Message Queue Owner	Message queue owner
Message Queue Owner Authority	Authority granted queue owner
Message Queue Public Authority	Authority granted *PUBLIC

See also

User Profile Configuration Reports

Blueprint Parameter File

This report displays user profile parameters defined in a blueprint.

Collector ID: BLUEPRINT_PARAMETER_FILE

Report ID: BLUEPRINT_PARAMETER_FILE

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File).
9) Press **Enter**.
10) Modify the run criteria as necessary.
11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
User Parameter	User profile parameter
User Parameter Value	User profile parameter value

See also

User Profile Configuration Reports

Blueprint Permissions File

This report displays the users/user groups who have permission to use the blueprint to create or modify user profiles.

Collector ID: BLUEPRINT_PERMISSIONS_FILE

Report ID: BLUEPRINT_PERMISSIONS_FILE

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Blueprint Permissions File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint
Authorized User/Group	Name of authorized user/user group
Create Permissions	Flag indicating whether user/user group as create privileges
Change Permissions	Flag indicating whether user/user group as change privileges

See also

User Profile Configuration Reports

Profile Inactivity Settings

This report displays settings handling inactive profiles.

Collector ID: PROFILE_INACTIVITY_SETTINGS

Report ID: PROFILE_INACTIVITY_SETTINGS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **10** (Profile Inactivity Settings).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Inactivity until Profile Disabled	Number of days a profile must be inactive before it is disabled
Inactivity until Profile Deleted	Number of days a profile must be inactive before it is deleted
Delete Profiles with password of *NO	Flag indicating whether to delete profiles with no password defined
Object Owner of Deleted Profiles	Name of user to whom ownership of an object will be transferred if the owner's profile is deleted
Remove User from TG Groups	Flag indicating whether to delete a user from a TG user group if the user's profile is deleted
Remove User from TG Rules	Flag indicating whether to delete a user from a TG rule definition if the user's profile is deleted
Inactivity Alert	Flag indicating whether alerts are sent about inactive users

See also

User Profile Configuration Reports

Profile Manager Defaults

This report displays the default setting for the program manager feature.

Collector ID: PROFILE_MANAGER_DEFAULTS

Report ID: PROFILE_MANAGER_DEFAULTS

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **11** (Profile Manager Defaults).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Audit Status	Flag indicating whether auditing is enabled **Note**: Auditing must be enabled to run reports.
Audit Journal Name	Journal in which to store auditing data
Audit Journal Library	Library in which to store the audit journal
Alert Status	Flag indicating whether alerting is enabled
Alert Message Queue Name	Journal in which to store auditing data
Alert Message Queue Library	Library in which to store the audit journal
Archive Profile?	Flag indicating whether archiving is enabled
Archive Retention Period	Number of days an archived profile is retained by the system
Profile Sync?	*This column is reserved for future use. It relates to integration with TGCentral.

Password Sync?	*This column is reserved for future use. It relates to integration with TGCentral.

See also

User Profile Configuration Reports

User Profile Archive

This report displays archived profiles. The system archives profiles (retires profiles from the system and stores them in an archive file) once inactivity requirements are met.

Collector ID: USER_PROFILE_ARCHIVE

Report ID: USER_PROFILE_ARCHIVE

To run this report

1) Access the TGSecure main menu.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (User Profile Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **9** (User Profile Archive).

9) Press **Enter**.

10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
User Name	Name of the user
User Description	Description of the user
Archive Date	Date on which the profile was archived
Archive File	File in which the profile was archived
Archive Library	Library in which the profile file resides

See also

User Profile Configuration Reports

User Profile Exclusions

This report displays user profile exclusions.

Collector ID: USER_PROFILE_EXCLUSIONS

Report ID: USER_PROFILE_EXCLUSIONS

To run the User Profile Exclusion Report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **8** (User Profile Exclusions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
User/Group	User group to which the exclusion applies
Exclusion Type	Type of exclusion ***ALL** - All types ***ACTIVITY** - Exclude the user group from being checked for inactivity ***SYNC** - exclude the user group from being synchronized with other systems (e.g., TGCentral)

See also

User Profile Configuration Reports

User Profile Change Reports

This section contains descriptions of the following reports:

- Blueprint 3rd Party Changes
- Blueprint Auth Setting Changes
- Blueprint Master Changes
- Blueprint Non-Compliance Changes
- Blueprint Object Authority Changes
- Blueprint Parameter Changes
- Blueprint Permissions Changes
- Profile Inactivity Changes
- Profile Manager Default Changes
- User Profile Archive Changes
- User Profile Exclusion Changes

See also

User Profile Reports

Blueprint 3rd Party Changes

This report displays changes made to 3rd party scripts used for integration purposes.

Collector ID: DATABASE_AUDITING

Report ID: BLUEPRINT_3RD_PARTY_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Blueprint Id	ID assigned to the blueprint
Script Type	Script type
Script Statement	Script text

See also

User Profile Change Reports

Blueprint Auth Setting Changes

This report displays changes to authority lists associated with the blueprints.

Collector ID: DATABASE_AUDITING

Report ID: BLUEPRINT_AUTH_SETTINGS_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **5** (Blueprint Authority List Settings File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Blueprint Id	ID assigned to the blueprint
Authority List	Authority list assigned to the blueprint
Object Authority	Object authority

See also

User Profile Change Reports

Blueprint Master Changes

This report displays changes made to the blueprint master.

Collector ID: DATABASE_AUDITING

Report ID: Report ID: BLUEPRINT_MASTER_CHG

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (User Profile Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **1** (Blueprint Master).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Blueprint Id	ID assigned to the blueprint

User Group	Name of user group assigned to blueprint master **Note**: Modifications made to the blueprint impact this user group.
Blueprint Description	Description of blueprint
Profile Parameters?	Flag indicating whether profile parameters are defined
Profile Authorities?	Flag indicating whether profile authorities are defined
Authority List?	Flag indicating whether profile authorities are defined
3rd Party Integration?	Flag indicating whether 3rd party scripts are defined
Blueprint Alert?	Flag indicating whether alerts are enabled
Inactive Override?	Flag indicating whether inactivity overrides are defined
Inactive Profiles?	Flag indicating whether inactive profiles were identified
Compliance Date	Date on which the blueprint came into effect
Compliance Status	Flag indicating whether all profiles associated with the blueprint are in compliance
Inactivity before Disabled	Number of days the profile was inactive before it was disabled
Inactivity before Delete	Number of days the profile was inactive before it was deleted
Object owner for deleted profiles	Name of the user to whom object ownership was transferred upon deletion of the profile

See also

User Profile Change Reports

Blueprint Non-Compliance Changes

This report displays changes made to user profiles that do not comply with the blueprint.

Collector ID: DATABASE_AUDITING

Report ID: BLUEPRINT_NON_COMPLIANCE_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **6** (Blueprint Non-Compliance User Profiles).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Blueprint Id	ID assigned to the blueprint
User Name	Name of user
Violation Category	Type of violation
Violation Keyword	Keyword associated with the profile parameter
Violation Description	Description associated with the profile parameter
Current Value	Parameter value defined in the user's profile
Blueprint Value	Parameter value defined in the blueprint
Non-Compliance Reason	Description of violation

See also

User Profile Change Reports

Blueprint Object Authority Changes

This report displays changes to object authorities associated with blueprints.

Collector ID: DATABASE_AUDITING

Report ID: BLUEPRINT_OBJECT_AUTH_CHG

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (User Profile Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Changes Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Blueprint Id	ID assigned to the blueprint
Profile Object Owner	Object owner
Profile Object Owner Authority	Authority granted owner
Message Queue Owner	Message queue owner
Message Queue Owner Authority	Authority granted queue owner
Message Queue Public Authority	Authority granted *PUBLIC

See also

User Profile Change Reports

Blueprint Parameter Changes

This report displays changes to blueprint parameters.

Collector ID: DATABASE_AUDITING

Report ID: BLUEPRINT_PARAMETER_CHG

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (User Profile Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Blueprint Id	ID assigned to the blueprint
User Parameter	User profile parameter
User Parameter Value	User profile parameter value

See also

User Profile Change Reports

Blueprint Permissions Changes

This report displays changes to blueprint permissions.

Collector ID: DATABASE_AUDITING

Report ID: BLUEPRINT_PERMISSIONS_CHG

To enable this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (User Profile Manager Defaults).
5) Press **Enter**.
6) Enter **Y** as the **Audit Configuration Changes** flag.
7) Press **Enter**.

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **2** (Blueprint Permissions File).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description

Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption
Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Blueprint Id	ID assigned to the blueprint
Authorized User/Group	Name of authorized user/user group
Create Permissions	Flag indicating whether user/user group as create privileges
Change Permissions	Flag indicating whether user/user group as change privileges

See also

User Profile Change Reports

Profile Inactivity Changes

This report displays changes made to profile inactivity settings.

Collector ID: DATABASE_AUDITING

Report ID: PROFILE_INACTIVITY_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **10** (Profile Inactivity Settings).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Inactivity until Profile Disabled	Number of days a profile must be inactive before it is disabled
Inactivity until Profile Deleted	Number of days a profile must be inactive before it is deleted
Delete Profiles with password of *NO	Flag indicating whether to delete profiles with no password defined
Object Owner of Deleted Profiles	Name of user to whom ownership of an object will be transferred if the owner's profile is deleted
Remove User from TG Groups	Flag indicating whether to delete a user from a TG user group if the user's profile is deleted
Remove User from TG Rules	Flag indicating whether to delete a user from a TG rule definition if the user's profile is deleted
Inactivity Alert	Flag indicating whether alerts are sent about inactive users

See also

User Profile Change Reports

Profile Manager Default Changes

This report displays changes made to Profile Manager defaults.

Collector ID: DATABASE_AUDITING

Report ID: PROFILE_MANAGER_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **11** (Profile Manager Defaults).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
Audit Status	Flag indicating whether auditing is enabled **Note**: Auditing must be enabled to run reports.
Audit Journal Name	Journal in which to store auditing data
Audit Journal Library	Library in which to store the audit journal
Alert Status	Flag indicating whether alerting is enabled
Alert Message Queue Name	Journal in which to store auditing data
Alert Message Queue Library	Library in which to store the audit journal
Archive Profile?	Flag indicating whether archiving is enabled
Archive Retention Period	Number of days an archived profile is retained by the system
Profile Sync?	*This column is reserved for future use. It relates to integration with TGCentral.
Password Sync?	*This column is reserved for future use. It relates to integration with TGCentral.

See also

User Profile Change Reports

User Profile Archive Changes

This report displays changes made to archived profile settings.

Collector ID: DATABASE_AUDITING

Report ID: USER_PROFILE_ARCHIVE_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **9** (User Profile Archive).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
User Name	Name of the user
User Description	Description of the user
Archive Date	Date on which the profile was archived
Archive File	File in which the profile was archived
Archive Library	Library in which the profile file resides

See also

User Profile Change Reports

User Profile Exclusion Changes

This report displays changes made to inactive profile exclusion settings.

Collector ID: DATABASE_AUDITING

Report ID: USER_PROFILE_EXCLUSIONS_CHG

To run this report

1) Access the TGSecure main menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **8** (User Profile Exclusions).
9) Press **Enter**.
10) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report.

11) Press **Enter**.

Report Column Description

Column	Description
Type	Journal entry code for the type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (a relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the remote server attempted communication with the target server
Job Name	Name assigned to the job
User Name	Name of the user executing the job
Job Number	Numbered assigned to the job
Program Name	Name of the program used to perform encryption

Program Library	Name of the library in which the program resides
Object Name	Name of object changed
Library Name	Name of the library in which the object resides
Member Name	Name of member
User Profile	Profile name of user executing the change request
System Name	Name of system submitting the change request
Remote Address	IP address used to submit the change request
User/Group	User group to which the exclusion applies
Exclusion Type	Type of exclusion ***ALL** - All types ***ACTIVITY** - Exclude the user group from being checked for inactivity ***SYNC** - exclude the user group from being synchronized with other systems (e.g., TGCentral)

See also

User Profile Change Reports

APPENDICES

APPENDIX - TGSecure Collectors

Collector ID	Collector Name	Collector Category	Platform
ACCESS_ESCAL_ACC_CONTROLS	Access Escalation Access Controls	Network	IBMi
ACCESS_ESCAL_DEFAULTS	Access Escalation Defaults	Network	IBMi
ACCESS_ESCAL_ENTITLEMENTS	Access Escalation Entitlements	Network	IBMi
ACCESS_ESCAL_FILE_EDITORS	Access Escalation File Editors	Network	IBMi
ACCESS_ESCALATION_USAGE	Access Escalation Usage	Network	IBMi
AUTH_USERS_VIA_AUTH_LISTS	Authorized Users through Authorization Lists	Resource	IBMi
AUTHORITY_COL_ALI	Authority Collection Report (*ALL)	Resources	IBMi
AUTHORITY_COL_IFS	Auth Collection For Objects IFS Report	Resources	IBMi
AUTHORITY_COL_OBJECT	Auth Collection For Objects Native Report	Resources	IBMi
AUTHORITY_COLLECTION	Authority Collection Data	Journal	IBMi
AUTHORITY_COMPLIANCE	Authority Compliance	Resource	IBMi
AUTHORITY_LIST	Authority List Data	System	IBMi
BLUEPRINT_3RD_PARTY_FILE	Blueprint 3rd Party Integration File	Profile	IBMi
BLUEPRINT_AUTH_SETTINGS_FILE	Blueprint Authority List Settings File	Profile	IBMi
BLUEPRINT_MASTER	Blueprint Master	Profile	IBMi
BLUEPRINT_NON_COMPLIANCE_USER	Blueprint Non-Compliance User Profiles	Profile	IBMi
BLUEPRINT_OBJECT_AUTH_FILE	Blueprint Object Authority File	Profile	IBMi
BLUEPRINT_PARAMETER_FILE	Blueprint Parameter File	Profile	IBMi
BLUEPRINT_PERMISSION_FILE	Blueprint Permission File	Profile	IBMi
CMD_SEC_COMMANDS	Commands Allowed/Rejected via Command Security	Resources	IBMi
CMD_SEC_CONF_SETTINGS	Command Security Config Settings	Resources	IBMi
CMD_SEC_PARAM_LEVEL	Command Security Paramater Level	Resources	IBMi
CMD_SEC_RULES	Command Security Config Settings	Resources	IBMi
CONTROLLER_ATTACHED_DEVICES	Command Security Paramater Level	Network	IBMi

CONTROLLER_DESCRIPTION_DATA	Controller Description Information	Network	IBMi
DATA_AREA_AUDITING	Audit data area changes	Network	IBMi
DATABASE ACCESS	Database File Access	N/A	IBMi
DATABASE_AUDITING	Monitor Database changes	Network	IBMi
DATABASE_CONTENT	Database Content	Configuration	IBMi
DATABASE_FIELD_ACTIVITY	Database Field Activity	Resources	IBMi
DATABASE_OPERATIONS	Database Operations	N/A	IBMi
DET_ACT_HISTORY	Detect Activity History	Network	IBMi
DET_DEFAULTS	Detect Defaults	Configuration	IBMi
DET_CMD_RULES	Command Monitor Rules	Configuration	IBMi
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration	IBMi
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration	IBMi
DET_JRNMON_RULES	Journal Monitor Rules	Configuration	IBMi
DET_MON_MASTER	Monitor Master	Configuration	IBMi
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration	IBMi
DET_MSQ_RULES	Message Queue Rules	Configuration	IBMi
DET_SEIM_PROVIDERS	SEIM Providers	Configuration	IBMi
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration	IBMi
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network	IBMi
DEVICE_DESCRIPTION_DATA	Device Description Information	Network	IBMi
DTBASE_OPERATIONS_JRN	Database Operations by Journal	N/A	IBMi
ENCRYPT_DATABASE_FIELD	Encryption Database Field Details	Resource	IBMi
ENCRYPT_DATABASE_FILE	Encryption Database File Details	Resource	IBMi
ENCRYPT_DATABASE_FILTER	Encryption Database File Details	Resource	IBMi
ENCRYPT_DATABASE_RULES	Encryption Database Rule Details	Resource	IBMi
ENCRYPTION_DEFAULTS	Encryption Defaults	Resource	IBMi
EXIT_POINTS	Display Exit Point Data	Network	IBMi
FIELD_AUTHORITY	Display Field Level Authorities	Object	IBMi
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource	IBMi
IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource	IBMi
IFS_CONTENT	IFS Content	Configuration	IBMi

IFS_JOURNALING	Display extended journaling information for the IFS object	Resource	IBMi
IFS_STATUS	Display status information about an IFS file	Resource	IBMi
INACTIVITY_DISCONNECTS	Inactivity Disconnections	Configuration	IBMi
INCOMING_TRANSACTIONS	Incoming Transactions	Network	IBMi
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network	IBMi
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network	IBMi
ISL_RULES	ISL Inclusion Exclusion Rules	Network	IBMi
JOB_ACTIVITY_DETAILS	Job Activity Details	Log	IBMi
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log	IBMi
JOB_DESCRIPTIONS	Job Description Data	Configuration	IBMi
JOURNAL_AD	Object Auditing Attribute Changes	Configuration	IBMi
JOURNAL_AF	Authority Failures	Profile	IBMi
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration	IBMi
JOURNAL_AU	EIM Attribute Changes	Configuration	IBMi
JOURNAL_AX	Row and Column Access Control	Resource	IBMi
JOURNAL_CA	Authorization List or Object Authority Changes	Profile	IBMi
JOURNAL_CD	Commands Executed	Resource	IBMi
JOURNAL_CO	Create Operations	Resource	IBMi
JOURNAL_CP	User Profile Changes	Configuration	IBMi
JOURNAL_CQ	Change Request Descriptor Changes	Configuration	IBMi
JOURNAL_CU	Cluster Operation	Network	IBMi
JOURNAL_CV	Connection Verification	Profile	IBMi
JOURNAL_CY	Cryptographic Configuration Changes	Configuration	IBMi
JOURNAL_DI	LDAP Operations	Resource	IBMi
JOURNAL_DO	Delete Operations	Resource	IBMi
JOURNAL_DS	Changes to Service Tools Profiles	Profile	IBMi
JOURNAL_EV	Environment Variable Changes	Profile	IBMi
JOURNAL_GR	Exit Point Maintenance Operations	Resource	IBMi
JOURNAL_GS	Socket Descriptor Details	Resource	IBMi
JOURNAL_IM	Intrusion Monitor Events	Network	IBMi
JOURNAL_IP	Inter-process Communication Events	Network	IBMi

JOURNAL_IR	Actions to IP Rules	Network	IBMi
JOURNAL_IS	Internet Security Management Events	Network	IBMi
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource	IBMi
JOURNAL_JS	Job Changes	Resource	IBMi
JOURNAL_KF	Key Ring File Changes	Configuration	IBMi
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource	IBMi
JOURNAL_M0	Db2 Mirror Setup Tools	Resource	IBMi
JOURNAL_M6	Db2 Mirror Communication Services	Resource	IBMi
JOURNAL_M7	Db2 Mirror Replication Services	Resource	IBMi
JOURNAL_M8	Db2 Mirror Product Services	Resource	IBMi
JOURNAL_M9	Db2 Mirror Replication State	Resource	IBMi
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration	IBMi
JOURNAL_NA	Network Attribute Changes	Profile	IBMi
JOURNAL_ND	Directory Search Violations	Resource	IBMi
JOURNAL_NE	APPN Endpoint Filter Violations	Network	IBMi
JOURNAL_O1	Single Optical Object Accesses	Resource	IBMi
JOURNAL_O2	Dual Optical Object Accesses	Resource	IBMi
JOURNAL_O3	Optical Volume Accesses	Resource	IBMi
JOURNAL_OM	Object Management Changes	Resource	IBMi
JOURNAL_OR	Objects Restored	Resource	IBMi
JOURNAL_OW	Object Ownership Changes	Resource	IBMi
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration	IBMi
JOURNAL_PF	PTF Operations	Resource	IBMi
JOURNAL_PG	Primary Group Changes	Resource	IBMi
JOURNAL_PO	Printer Output Changes	Resource	IBMi
JOURNAL_PS	Swap Profile Events	Configuration	IBMi
JOURNAL_PU	PTF Object Changes	Profile	IBMi
JOURNAL_PW	Invalid Sign-on Attempts	Profile	IBMi
JOURNAL_RA	Authority Changes to Restored Objects	Configuration	IBMi
JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration	IBMi
JOURNAL_RO	Ownership Changes for Restored Objects	Profile	IBMi
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration	IBMi

JOURNAL_RQ	Change Request Descriptors Restored	Resource	IBMi
JOURNAL_RU	Authority Restored for User Profiles	Profile	IBMi
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration	IBMi
JOURNAL_SD	System Directory Changes	Resource	IBMi
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration	IBMi
JOURNAL_SF	Spooled File Actions	Resource	IBMi
JOURNAL_SG	Asynchronous Signals Processed	Network	IBMi
JOURNAL_SK	Secure Socket Connections	Network	IBMi
JOURNAL_SM	Systems Management Changes	Configuration	IBMi
JOURNAL_SO	Server Security User Information Actions	Configuration	IBMi
JOURNAL_ST	Service Tools Actions	Configuration	IBMi
JOURNAL_SV	System Values Changes	Configuration	IBMi
JOURNAL_VA	Access Control List Changes	Configuration	IBMi
JOURNAL_VC	Connections Started, Ended, or Rejected	Network	IBMi
JOURNAL_VF	Close Operations on Server Files	Resource	IBMi
JOURNAL_VL	Exceeded Account Limit Events	Profile	IBMi
JOURNAL_VN	Network Log On and Off Events	Configuration	IBMi
JOURNAL_VO	Actions on Validation Lists	Resource	IBMi
JOURNAL_VP	Network Password Errors	Profile	IBMi
JOURNAL_VR	Network Resource Accesses	Resource	IBMi
JOURNAL_VS	Server Sessions Started or Ended	Network	IBMi
JOURNAL_VU	Network Profile Changes	Profile	IBMi
JOURNAL_VV	Service Status Change Events	Network	IBMi
JOURNAL_X0	Network Authentication Events	Network	IBMi
JOURNAL_X1	Identity Token Events	Profile	IBMi
JOURNAL_XD	Directory Server Extensions	Profile	IBMi
JOURNAL_YC	DLO Object Changes	Resource	IBMi
JOURNAL_YR	DLO Object Reads	Resource	IBMi
JOURNAL_ZC	Object Changes	Resource	IBMi
JOURNAL_ZR	Object Reads	Resource	IBMi
KEYSTORE_DATA	KeyStore	Configuration	IBMi
LIBRARY_STAT	Library Statistics	Resources	IBMi

LINE_DESCRIPTION_DATA	Line Description Information	Configuration	IBMi
MESSAGE_QUEUE	Message Queue Details	Configuration	IBMi
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration	IBMi
NETWORK_ATTRIBUTES	Network Attribute Information	Network	IBMi
NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network	IBMi
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network	IBMi
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network	IBMi
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network	IBMi
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network	IBMi
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network	IBMi
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network	IBMi
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network	IBMi
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes/Remote Exit Rule	Network	IBMi
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes/Remote Exit Rule	Network	IBMi
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network	IBMi
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network	IBMi
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_DDM	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_FILE	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_FTP_REXEC	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_PRINTER	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network	IBMi
NETWORK_TRANS_SIGNON	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_TELNET	Remote Exit Rules	Network	IBMi
OBJECT_AUTHORITY	Display Object Authority	Resource	IBMi
OBJECT_DETAILS	Display Object Details	Resource	IBMi
OBJECT_STAT	Object/File Statistics	Resource	IBMi
OUTPUT_QUEUE	Output Queue Information	Configuration	IBMi
PRODUCT_INFO	Basic Information about a software product	Configuration	IBMi

PROFILE_COMPLIANCE	Profile Compliance Data	Profile	IBMi
PROFILE_INACTIVITY_SETTINGS	Profile Inactivity Settings	Profile	IBMi
PROFILE_MANAGER_DEFAULTS	Profile Manager Defaults	Profile	IBMi
PROGRAM_ADOPT	Programs that Adopt Authority	Resource	IBMi
PROGRAM_REFERENCE_DATA	Program Reference Data	Resource	IBMi
PTF_DATA	Program Temporary Fix Data	Configuration	IBMi
QHST_MSG_INFO	QHST History Log Information	Configuration	IBMi
QSYS2.ACTIVE_JOB_INFO	Active job information	Configuration	IBMi
QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User access	Configuration	IBMi
QSYS2.FUNCTION_INFO	Function usage identifiers	Configuration	IBMi
QSYS2.FUNCTION_USAGE	Function usage configuration details.	Configuration	IBMi
QSYS2.GROUP_PTF_INFO	Group PTFs Information	Configuration	IBMi
QSYS2.JOURNAL_INFO	Journal and remote journal information	Configuration	IBMi
QSYS2.LICENSE_INFO	Products license information.	Configuration	IBMi
QSYS2.MEDIA_LIBRARY_INFO	Media Library Status details	Configuration	IBMi
QSYS2.MEMORY_POOL	Memory pool details	Configuration	IBMi
QSYS2.MEMORY_POOL_INFO	Active memory pools	Configuration	IBMi
QSYS2.MESSAGE_QUEUE_INFO	Message Queue	Configuration	IBMi
QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 network connection details.	Configuration	IBMi
QSYS2.OBJECT_LOCK_INFO	Object lock information	Configuration	IBMi
QSYS2.OUTPUT_QUEUE_ENTRIES	Spooled file in output queue	Configuration	IBMi
QSYS2.RECORD_LOCK_INFO	Record lock information	Configuration	IBMi
QSYS2.REPLY_LIST_INFO	Current job's reply list entry information	Configuration	IBMi
QSYS2.SCHEDULED_JOB_INFO	Job Schedule Entry information	Configuration	IBMi
QSYS2.SERVER_SBS_ROUTING	Alternate subsystem configurations	Configuration	IBMi
QSYS2.SYSCONTROLS	Permissions or column mask defined	Configuration	IBMi
QSYS2.SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration	IBMi

QSYS2.SYSDISKSTAT	Disk Information	Configuration	IBMi
QSYS2. SYSTEM_STATUS_INFO	Partition information	Configuration	IBMi
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration	IBMi
QSYS2.USER_INFO	User Profile Information	Configuration	IBMi
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration	IBMi
REMOTE_TRAN_SUMMARY_ BY_SERVER	Remote Summary Server	Network	IBMi
REMOTE_TRAN_SUMMARY_ BY_USER	Remote Summary User	Network	IBMi
RSC_MGR_COMPLIANCE_DA TA	Resource Manager Authority Out of compliance data	Network	IBMi
RSC_MGR_CONFIG	Resource Manager Configuration	Network	IBMi
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network	IBMi
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network	IBMi
SENSITIVE_DATABASE_CON TENT	Sensitive Database Content	Profile	IBMi
SERVICE_TOOL_SECURITY_ ATTR	Service Tool Security Attributes	Profile	IBMi
SERVICE_TOOL_USERS	Service Tool User Data	Profile	IBMi
SOCKET_SUMMARY_BY_SER VER	Socket Summary by Server	Network	IBMi
SOCKET_SUMMARY_BY_USER	Socket Summart by User	Network	IBMi
SOCKET_TRAN_RULES	Socket Rules	Network	IBMi
SOCKET_TRANSACTIONS	Socket Transactions	Network	IBMi
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration	IBMi
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration	IBMi
SUBSYSTEM_COMMUNICATI ONS	Subsystem Communication Entries	Configuration	IBMi
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration	IBMi
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration	IBMi
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration	IBMi
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration	IBMi
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration	IBMi
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration	IBMi

SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration	IBMi
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration	IBMi
SYSCOLAUTH	Privileges granted on a column	Configuration	IBMi
SYSCONTROLS	Permission or column mask defined	Configuration	IBMi
SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration	IBMi
SYSCONTROLSDEP	Privileges granted on a row	Configuration	IBMi
SYSFIELDS	Columns with field procedures	Configuration	IBMi
SYSPACKAGEAUTH	Privileges granted on a package	Configuration	IBMi
SYSPROGRAMSTAT	Program, service program, and module with SQL statements	Configuration	IBMi
SYSROUTINEAUTH	Privileges granted on a routine	Configuration	IBMi
SYSSCHEMAAUTH	Privileges granted on a schema	Configuration	IBMi
SYSSEQUENCEAUTH	Privileges granted on a sequence	Configuration	IBMi
SYSTABAUTH	Privileges granted on a table or view	Configuration	IBMi
SYSTABLESTAT	Table statistics include all partitions and members	Configuration	IBMi
SYSTEM_VALUES	Display System Value Data	System	IBMi
SYSTOOLS. GROUP_PTF_CURRENCY	PTF Groups installed per IBM Recommendations	Configuration	IBMi
SYSTOOLS. GROUP_PTF_DETAILS	PTFs within PTF Groups installed per IBM Recommendations	Configuration	IBMi
SYSUDTAUTH	Privileges granted on a type	Configuration	IBMi
SYSVARIABLEAUTH	Privileges granted on a global variable	Configuration	IBMi
SYSXSROBJECTAUTH	Privileges granted on an XML schema	Configuration	IBMi
TGMOBJINF	Object Information	Resource	IBMi
TG_NETWORK_GROUPS	TG Network Groups	Network	IBMi
TG_OBJECT_GROUPS	TG Object Groups	Network	IBMi
TG_OPERATION_GROUPS	TG Operation Groups	Network	IBMi
TG_USER_GROUPS	TG User Groups	Network	IBMi
USER_OBJECT_AUTHORITIES	User Profile Object Authorities	Profile	IBMi
USER_PRF_VIA_BLUEPRINT	User Profile via Blueprint	Profile	IBMi
USER_PROFILE_ACTIVITY	User Profile Activity	Profile	IBMi

USER_PROFILE_ARCHIVE	User Profile Archive	Profile	IBMi
USER_PROFILE_EXCLUSIONS	User Profile Exclusions	Profile	IBMi
USER_PROFILES	Display User Profile Data	Profile	IBMi

APPENDIX - TGSecure Report Reference Revisions

This section includes enhancement by version.

- Version 2.3 - TGSecure Report Reference Revisions
- Version 2.2 - TGSecure Report Reference Revisions
- Version 2.1 - TGSecure Report Reference Revisions

Version 2.3 - TGSecure Report Reference Revisions

No major updates were made to the TGSecure reports in this release.

Version 2.2 - TGSecure Report Reference Revisions

Command Security Reports

The following new reports are now available for use:

- Command Security Config Settings
- Command Security Parameter Level
- Command Security Rules
- Command Security Configuration Changes
- Command Security Command Rule Changes
- Command Security Command Parameter Level Changes
- Commands Allowed via Command Security
- Commands Rejected via Command Security

The following new collectors are now available for use:

- CMD_SEC_COMMANDS
- CMD_SEC_CONF_SETTINGS
- CMD_SEC_PARAM_LEVEL
- CMD_SEC_RULES

Version 2.1 - TGSecure Report Reference Revisions

The following new report is now available for use:

- Network Transaction Showcase