NetIQ Security Solutions for IBM i
TGSecure 2.1
Report Reference Guide

Revised August 2019

Legal Notice

Table of Contents

What's New in Version 2.1

Report

The following new report is now available for use:

- Network Transaction Showcase

1. Introduction

This reference guide provides information about each build-it report in TGSecure. Use this reference guide to learn why a report passed or failed.

Please refer to the TGSecure User Guide for detailed information and concepts on how to use TGSecure.

1.1. 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

2. Access Escalation Reports

This section of reports provides details regarding user access escalation reports:

Access Escalation Usage Reports

- Access Escalation Activity
- Access Escalation Command Activity
- Access Escalation Program Activity
- Access Escalation Database Updates Activity
- Access Escalation Entitlement Usage
- Access Escalation Failures

Access Escalation Configuration Reports

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

Access Escalation Change 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

Introduction

2.1. Access Escalation Usage Reports

This section of contains descriptions for the following reports:

- Access Escalation Activity
- Access Escalation Command Activity
- Access Escalation Database Updates Activity
- Access Escalation Entitlement Usage
- Access Escalation Failures

- Access Escalation Program Activity

See also

Access Escalation Reports

2.1.1. Access Escalation Activity

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

The report is based on the following collector:

- ACCESS_ESCALATION_USAGE

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

Column	Description
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

2.1.2. Access Escalation Command Activity

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

The report is based on the following collector:

- ACCESS_ESCALATION_USAGE

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

2.1.3. Access Escalation Db Update Activity

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

The report is based on the following collector:

- ACCESS_ESCALATION_USAGE

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

Column	Description
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

2.1.4. Access Escalation Usage

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

The report is based on the following collector:

- ACCESS_ESCALATION_USAGE

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

Column	Description
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 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

2.1.5. Access Escalation Failures

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

The report is based on the following collector:

- ACCESS_ESCALATION_USAGE

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 submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of 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

2.1.6. Access Escalation Program Activity

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

The report is based on the following collector:

- ACCESS_ESCALATION_USAGE

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 system receiving the transaction
Object Name	Object targeted by the transaction
Object Library	Object library targeted by the transaction

Column	Description
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

2.2. Access Escalation Configuration Reports

This section of contains descriptions for 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

2.2.1. 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.

The report is based on the following collector:

- ACCESS_ESCAL_ACC_CONTROLS

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

2.2.2. Access Escalation Defaults

This report displays default escalation settings.

The report is based on the following collector:

- ACCESS_ESCAL_DEFAULTS

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 use 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

2.2.3. Access Escalation Entitlements Report

This report displays the entitlement configuration details.

The report is based on the following collector:

- ACCESS_ESCAL_ENTITLEMENTS

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?	Flag indicating whether the entitlement is enabled **Y** - Entitlement applied **N** - Entitlement ignored

Column	Description
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 to which the entitlement applies
Authentication Y/N	Flag indicating 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	Flag indicating 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

2.2.4. Access Escalation File Editors Report

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.

The report is based on the following collector:

- ACCESS_ESCAL_FILE_EDITORS

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

2.2.5. Network Groups

This report displays configuration details for all available network groups.

The report is based on the following collector:

- TG_NETWORK_GROUPS

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 member assigned to group
Network Description	Description of member
Network Group Description	Description of group

See Also

Access Escalation Configuration Reports

2.2.6. Object Groups

This report displays configuration details for all available object groups.

The report is based on the following collector:

- TG_OBJECT_GROUPS

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

See Also

Access Escalation Configuration Reports

Configuration Reports

2.2.7. 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.

The report is based on the following collector:

- TG_OPERATION_GROUPS

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 operation
Operation Group Description	Description assigned to operation group

See Also

Access Escalation Configuration Reports

Configuration Reports

2.2.8. User Groups

This report displays configuration details for all available user groups.

The report is based on the following collector:

- TG_USER_GROUP

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 member assigned to group
Member Description	Description of member
Group Description	Description of group

See Also

Access Escalation Configuration Reports

Configuration Reports

2.3. Access Escalation Change Reports

This section of contains descriptions for 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

2.3.1. 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).

The report is based on the following collector:

- DATABASE_AUDITING

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 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
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name of the object being modified
Library Name	Name of the library in which the object resides

Column	Description
Member Name	Name of the library member
User Profile	Name of the user submitting the modification
System Name	Name of the system submitting the modification
Remote Address	IP address of the remote server submitting the modification
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

2.3.2. Access Escalation Default Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

2.3.3. Access Escalation Entitlement Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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 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
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name of the object being modified

Column	Description
Library Name	Name of the library in which the object resides
Member Name	Name of the library member
User Profile	Name of the user submitting the modification
System Name	Name of the system submitting the modification
Remote Address	IP address of the remote server submitting the modification
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

2.3.4. Access Escalation File Editor Changes

This report displays all changes to the file editor.

The report is based on the following collector:

- DATABASE_AUDITING

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 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
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name of the object being modified
Library Name	Name of the library in which the object resides
Member Name	Name of the library member
User Profile	Name of the user submitting the modification
System Name	Name of the system submitting the modification
Remote Address	IP address of the remote server submitting the modification
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

2.3.5. Network Groups Changes

This report displays all changes made to network group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

2.3.6. Object Groups Changes

This report displays all changes made to object group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

2.3.7. Operation Groups Changes

This report displays all changes made to operation group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

2.3.8. User Groups Changes

This report displays all changes made to user group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

3. Inactivity Session Lockdown Reports

This section of reports provides details regarding ISL:

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

See also

Introduction

3.1. Inactivity Session Usage Reports

This section of contains descriptions for the following reports:

- Inactivity Disconnect

See also

Inactivity Session Lockdown Reports

3.1.1. Inactivity Disconnect

This report displays disconnections caused by user inactivity.

The report is based on the following collector:

- 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 consist 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

3.2. Inactivity Session Configuration Reports

This section of contains descriptions for the following reports:

- Inactivity Session Configuration Settings
- Inactivity Session Disconnect Options
- Inactivity Session Inclusion Exclusion Rules

See also

Inactivity Session Lockdown Reports

3.2.1. ISL Configuration Settings

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

The report is based on the following collector:

- ISL_CONFIGURATION_SETTINGS

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

Column	Description
	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

3.2.2. ISI Disconnect Options

This report displays disconnection options.

The report is based on the following collector:

- ISL_DISCONNECT_OPTIONS

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)

Column	Description
	SIGNOFF - End the session (user must restart their session and job)

See Also

Inactivity Session Configuration Reports

3.2.3. ISL Inclusion Exclusion Rules

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

The report is based on the following collector:

- ISL_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 that defines when the 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)

Column	Description
	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

3.3. Inactivity Session Change Reports

This section of contains descriptions for the following reports:

- Inactivity Session Configuration Changes
- Inactivity Session Disconnect Option Changes
- Inactivity Session Rule Changes

See also

Inactivity Session Lockdown Reports

3.3.1. ISL Configuration Changes

This report displays changes made to ISL configuration settings.

The report is based on the following collector:

- DATABASE_AUDITING

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	Type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the change took place
Job Name	Name assigned to the job
User Name	Name of the user who made the change
Job Number	Number assigned to the job
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name assigned to the object
Library Name	Library in which the object resides
Member Name	Name assigned to the member
User Profile	Profile ID assigned to the user who made the change
System Name	System on which the change was made
Remote Address	Remote address of the system (if applicable)
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 alert queue): ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Audit Configuration Change	Change made to configuration setting

Column	Description
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 entries, the value should appear as IL.

See Also

Inactivity Session Change Reports

3.3.2. ISL Disconnect Option Changes

This report displays changes to ISL disconnect options.

The report is based on the following collector:

- DATABASE_AUDITING

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	Type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the change took place
Job Name	Name assigned to the job
User Name	Name of the user who made the change
Job Number	Number assigned to the job
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name assigned to the object
Library Name	Library in which the object resides
Member Name	Name assigned to the member
User Profile	Profile ID assigned to the user who made the change
System Name	System on which the change was made
Remote Address	Remote address of the system (if applicable)
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)

Column	Description
	SIGNOFF - Signoff from the server

See Also

Inactivity Session Change Reports

3.3.3. ISL Rule Changes

This report displays changes to ISL rules.

The report is based on the following collector:

- DATABASE_AUDITING

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	Type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)

Column	Description
Timestamp	Time at which the change took place
Job Name	Name assigned to the job
User Name	Name of the user who made the change
Job Number	Number assigned to the job
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name assigned to the object
Library Name	Library in which the object resides
Member Name	Name assigned to the member
User Profile	Profile ID assigned to the user who made the change
System Name	System on which the change was made
Remote Address	Remote address of the system (if applicable)
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
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

4. Network Security Reports

This section of reports provides details regarding network reports:

Transaction Reports

- Central Server Transactions
- Data Queue Transactions
- Database Server Transactions
- DDM Transactions
- File Server Transactions
- FTP Transactions
- Incoming Transactions
- Network Printer Transactions
- Network Transactions
- Remote Command Transactions
- Remote Execution Transactions
- Signon Server Transactions
- Socket Transactions
- Telnet Transactions

Summary Reports

- Socket Summary by Server
- Socket Summary By User
- Transaction Summary by Server
- Transaction Summary by User

Configuration Reports

- Exit Point Configuration
- Network Groups
- Object Groups
- Operation Groups
- Remote Exit Rules
- Socket Rules
- User Groups

Configuration Reports

- Exit Point Configuration Changes
- Network Groups Changes
- Object Groups Changes
- Operation Groups Changes
- Remote Exit Rules Changes
- Socket Rules Changes
- User Groups Changes

See also

Introduction

4.1. Transaction Reports

This section of contains descriptions for the following reports:

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

See also

Network Reports

4.1.1. Central Server Transactions

This report lists attempts to access the central server.

The report is based on the following collector:

- NETWORK_TRANS_CENTRAL
- NETWORK_TRANSACTIONS_CENTRAL

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 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

Column	Description
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

4.1.2. Data Queue Transactions

This report lists attempts to access the data queue server.

The report is based on the following collector:

- NETWORK_TRANS_DATAQ
- NETWORK_TRANSACTION_DATAQ

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

4.1.3. Database Server Transactions

This report lists attempts to access the database server.

The report is based on the following collector:

- NETWORK_TRANS_DATABASE
- NETWORK_TRANSACTIONS_DATABASE

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

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 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

4.1.4. DDM Transactions

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

The report is based on the following collector:

- NETWORK_TRANS_DDM
- NETWORK_TRANSACTIONS_DDM

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

Column	Description
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

4.1.5. File Server Transactions

This report lists attempts to access the file server.

The report is based on the following collector:

- NETWORK_TRANS_FILE
- NETWORK_TRANSACTIONS_FILE

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 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 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

Column	Description
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

4.1.6. Network Transaction FTP

This report lists attempts to access the FTP server.

The report is based on the following collector:

- NETWORK_TRANS_FTP_REXEC

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 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

Column	Description
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

4.1.7. Incoming Transaction

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

The report is based on the following collector:

- INCOMING_TRANSACTIONS

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

Column	Description
	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

4.1.8. Network Printer Transactions

This report lists attempts to access the network printer server.

The report is based on the following collector:

- NETWORK_TRANS_PRINTER
- NETWORK_TRANSACTIONS_PRINTER

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

4.1.9. Network Transactions

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

The report is based on the following collector:

- NETWORK_TRANSACTIONS

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

Column	Description
	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

4.1.10. Network Transaction Showcase

This report returns transactions associated with the Showcase exit program.

The report is based on the following collector:

- 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 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

Column	Description
	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

Resource Management Reports

4.1.11. Remote Command Transactions

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

The report is based on the following collector:

- NETWORK_TRANS_COMMAND
- NETWORK_TRANSACTIONS_COMMAND

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

Column	Description
Request Details	Information about the requestor

See Also

Transaction Reports

4.1.12. Network Transaction FTP REXEC

This report lists attempts to access the remote execution server.

The report is based on the following collector:

- NETWORK_TRANS_FTP_REXEC
- NETWORK_TRANSACTIONS_FTP_REXEC

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

Column	Description
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

4.1.13. Signon Server Transactions

This report lists attempts to access the SIGNON server.

The report is based on the following collectors:

- NETWORK_TRANS_SIGNON
- NETWORK_TRANSACTION_SIGNON

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.

Column	Description
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

4.1.14. Socket Transactions

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

The report is based on the following collector:

- SOCKET_TRANSACTIONS

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 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

4.1.15. Telnet Transactions

This report lists the attempts to access the Telnet server.

The report is based on the following collectors:

- NETWORK_TRANS_TELNET
- NETWORK_TRANSACTIONS_TELNET

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

Column	Description
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

4.2. Summary Reports

This section of contains descriptions for the following reports:

- Socket Summary by Server
- Socket Summary By User
- Transaction Summary by Server
- Transaction Summary by User

See also

Network Reports

4.2.1. Socket Summary by Server Report

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

The report is based on the following collector:

- SOCKET_SUMMARY_BY_SERVER

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

Summary Reports

4.2.2. Socket Summary by User Report

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

The report is based on the following collector:

- SOCKET_SUMMARY_BY_USER

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 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

Summary Reports

4.2.3. 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.

The report is based on the following collector:

- REMOTE_TRAN_SUMMARY_BY_SERVER

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 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 status of *PASS
Rejected Percentage	Percentage of incoming transactions with status of *PASS

See Also

Summary Reports

4.2.4. 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.

The report is based on the following collector:

- REMOTE_TRAN_SUMMARY_BY_USER

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 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 status of *PASS
Rejected Percentage	Percentage of incoming transactions with status of *PASS

See Also

Summary Reports

4.3. Configuration Reports

4.3.1. Configuration Reports

This section of contains descriptions for the following reports:

- Exit Point Configuration
- Network Groups
- Object Groups
- Operation Groups
- Remote Exit Rules
- Socket Rules
- User Groups

See also

Network Reports

4.3.2. Exit Point Configuration Report

This report displays configuration details for all available exit points.

The report is based on the following collector:

- NETWORK_EXIT_CONFIG

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

4.3.3. Network Groups

This report displays configuration details for all available network groups.

The report is based on the following collector:

- TG_NETWORK_GROUPS

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 member assigned to group
Network Description	Description of member
Network Group Description	Description of group

See Also

Access Escalation Configuration Reports

4.3.4. Object Groups

This report displays configuration details for all available object groups.

The report is based on the following collector:

- TG_OBJECT_GROUPS

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

See Also

Access Escalation Configuration Reports

Configuration Reports

4.3.5. 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.

The report is based on the following collector:

- TG_OPERATION_GROUPS

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 operation
Operation Group Description	Description assigned to operation group

See Also

Access Escalation Configuration Reports

Configuration Reports

4.3.6. Remote Exit Rules Report

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

The report is based on the following collector:

- NETWORK_TRAN_RULES

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

4.3.7. Socket Rules Report

This report displays configuration details for all available socket rules.

The report is based on the following collector:

- SOCKET_TRAN_RULE

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

4.3.8. User Groups

This report displays configuration details for all available user groups.

The report is based on the following collector:

- TG_USER_GROUP

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 member assigned to group
Member Description	Description of member

Group Description	Description of group

See Also

Access Escalation Configuration Reports

Configuration Reports

4.4. Configuration Changes

This section of contains descriptions for the following reports:

- Exit Point Configuration Changes
- Network Groups Changes
- Object Groups Changes
- Operation Groups Changes
- Remote Exit Rules Changes
- Socket Rules Changes
- User Groups Changes

See also

Network Reports

4.4.1. Exit Point Configuration Changes

This report displays all changes made to exit point configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Configuration Change Reports

4.4.2. Network Groups Changes

This report displays all changes made to network group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

4.4.3. Object Groups Changes

This report displays all changes made to object group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

4.4.4. Operation Groups Changes

This report displays all changes made to operation group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

4.4.5. Remote Exit Rules Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Configuration Change Reports

4.4.6. Socket Rules Changes

This report displays all changes made to socket rule configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Configuration Change Reports

4.4.7. User Groups Changes

This report displays all changes made to user group configurations.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

See Also

Access Escalation Change Reports

Configuration Change Reports

5. Resource Manager Reports

This section of reports provides details regarding the Resource Manager:

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

See also

Introduction

5.1. Resource Manager Usage Reports

This section of contains descriptions for the following reports:

- Authority Compliance
- Authority Collection IFS
- Authority Collection QSYS

See also

Resource Manager Reports

5.1.1. Authority Compliance Report

This report displays compliance details.

The report is based on the following collector:

- AUTHORITY_COMPLIANCE

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 specific library or ***ALL** to indicate all libraries
Object Name	Name of 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 current state

Column	Description
Schema Program Adopt	Program adopt status recommended by schema
Program Adopt Users	Program adopt user for current state
Schema Program Adopt Users	Program adopt user recommended by schema
Object Owner	Object owner for current state
Schema Object Owner	Object owner recommended by schema
User Inheritance Group	User Inheritance group for current state
Schema User Inheritance Group	User Inheritance group recommended by schema
User Name	User name for current state
Schema User Name	User name f recommended by schema
Object Authority	Object authority for 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 an 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

Column	Description
	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**) 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.
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**) authority 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**) authority 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

5.1.2. 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.

The report is based on the following collector:

- AUTHORITY_COLLECTION

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.

Column	Description
Authority Check Successful	Flag indicating whether 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 job (code + number)
Job User	Name of job user
Job Number	Number assigned to job

See Also

Resource Manager Usage Reports

5.1.3. 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.

The report is based on the following collector:

- AUTHORITY_COLLECTION

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 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

Column	Description
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 job (code + number)
Job User	Name of job user
Job Number	Number assigned to job

See Also

Resource Manager Usage Reports

5.2. Resource Manager Configuration Reports

5.2.1. Resource Manager Configurational Reports

This section of contains descriptions for the following reports:

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

See also

Resource Manager Reports

5.2.2. Resource Manager Configuration

This report displays Resource Manager configuration details.

The report is based on the following collector:

- 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 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 message queue **Note**: The default alert queue is **TGMSGQ** in library **TGDATA**.
Alert Message Queue Library	Library in which queue resides

See Also

Resource Manager Configuration Reports

5.2.3. Resource Manager Schema Details

This report displays Resource Manager schema details.

The report is based on the following collector:

- 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 specific library or ***ALL** to indicate all libraries
Object Name	Name of 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 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 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

5.2.4. Resource Manager Schema Header

This report displays Resource Manager schema header details.

The report is based on the following collector:

- 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 discrepancy ***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

5.2.5. Resource Manager out of Compliance Data

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

The report is based on the following collector:

- 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 specific library or ***ALL** to indicate all libraries
Object Name	Name of 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 current state
Program Adopt User	Program adopt status recommended by schema

Column	Description
Object Owner	Object owner for 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 system 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

5.3. Resource Manager Change Reports

This section of contains descriptions for the following reports:

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

See Also

Resource Manager Reports

5.3.1. Rsc Manager Configuration Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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	Type of operation: **DL** - Record delete **PX** - Record added by RRN (relative record number) to a physical file member **PT** - Record add **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the change was saved
Job Name	Name assigned to the job
User Name	Name of the user who made the change
Job Number	Number assigned to the job
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name assigned to the object
Library Name	Library in which the object resides
Member Name	Name assigned to the member

Column	Description
User Profile	Profile ID assigned to the user who made the change
System Name	System on which the change was made
Remote Address	Remote address of the system (if applicable)
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 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 library **TGDATA**.
Alert Message Queue Library	Library in which the queue resides

See Also

Resource Manager Change Reports

5.3.2. Resource Manager Schema Details Changes

This report displays changes made to the schema details.

The report is based on the following collector:

- DATABASE_AUDITING

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	Type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the change took place
Job Name	Name assigned to the job
User Name	Name of the user who made the change
Job Number	Number assigned to the job
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name assigned to the object
Library Name	Library in which the object resides
Member Name	Name assigned to the member
User Profile	Profile ID assigned to the user who made the change
System Name	System on which the change was made
Remote Address	Remote address of the system (if applicable)
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

Column	Description
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 programes
Program Adopt Users	Name of 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 an 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.

Column	Description
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 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

5.3.3. Rsc Manager Schema Header Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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	Type of operation: **DL** - Record delete **PT** - Record add **PX** - Record added by RRN (relative record number) to a physical file member **UB** - Record edit (before-change) **UP** - Record edit (after-change)
Timestamp	Time at which the change took place
Job Name	Name assigned to the job
User Name	Name of the user who made the change
Job Number	Number assigned to the job
Program Name	Name assigned to the program
Program Library	Library in which the program resides
Object Name	Name assigned to the object
Library Name	Library in which the object resides
Member Name	Name assigned to the member
User Profile	Profile ID assigned to the user who made the change
System Name	System on which the change was made
Remote Address	Remote address of the system (if applicable)
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

Column	Description
	***FAIL** - There are discrepancy ***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

5.3.4. Rsc Manager out of Compliance Data Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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 specific library or ***ALL** to indicate all libraries
Object Name	Name of 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 current state
Program Adopt User	Program adopt status recommended by schema
Object Owner	Object owner for 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

6. User Profile Reports

This section of reports provides details regarding user profile reports:

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

See also

Introduction

6.1. User Profile Usage Reports

This section of contains descriptions for the following reports:

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

See also

User Profile Reports

6.1.1. 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

6.1.2. Profile Compliance Report

This report displays inactivity compliance sorted by user name.

The report is based on the following collector:

- PROFILE_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 **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

6.1.3. User Profile via Blueprint For User: *ALL

This report displays profile activity categorized by blueprint.

The report is based on the following collector:

- USER_PRF_VIA_BLUEPRINT

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

6.1.4. User Profile Activity For User: *ALL

This report displays profile activity.

The report is based on the following collector:

- USER_PROFILE_ACTIVITY

Tip: See the IBM knowledge base for descriptions of the collector ID parameters (which appear as columns in this 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 **4** (User Profile Activity).
9) Press **Enter**.
10) Modify the run criteria as necessary.
11) Press **Enter**.

See Also

User Profile Usage Reports

6.1.5. 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.

The report is based on the following collector:

- JOURNAL_PW

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 entries:

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

6.1.6. 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.

The report is based on the following collector:

- JOURNAL_CP

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

6.1.7. Authority Failures

This report displays authority failures that have occurred on 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.

The report is based on the following collector:

- JOURNAL_AF

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.

The following are 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

6.2. User Profile Configuration Reports

This section of contains descriptions for the following reports:

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

See also

User Profile Reports

6.2.1. Blueprint Master

This report displays blueprint details.

The report is based on the following collector:

- 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 in to 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 user to whom object ownership was transferred upon deletion of profile

See Also

User Profile Configuration Reports

6.2.2. Blueprint Permissions File

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

The report is based on the following collector:

- 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

6.2.3. Blueprint Parameter File

This report displays user profile parameters defined in a blueprint.

The report is based on the following collector:

- 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

6.2.4. Blueprint Object Authority File

This report displays the object authorities define for a blueprint.

The report is based on the following collector:

- **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

6.2.5. Blueprint Authority List Settings File

This report displays authority list settings defined for a blueprint.

The report is based on the following collector:

- **Blueprint_Auth_Settings_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 **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

6.2.6. Blueprint Non-Compliance User Profiles

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

The report is based on the following collector:

- BLUEPRINT_NON_COMPLIANCE_USER

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 withe 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

6.2.7. Blueprint 3rd Party Integration File

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

The report is based on the following collector:

- 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

6.2.8. User Profile Exclusions

This report displays user profile exclusions.

The report is based on the following collector:

- 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

6.2.9. 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.

The report is based on the following collector:

- 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

6.2.10. Profile Inactivity Settings

This report displays settings handling inactive profiles.

The report is based on the following collector:

- 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

6.2.11. Profile Manager Defaults

This report displays default setting for the program manager feature.

The report is based on the following collector:

- 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 enable 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

6.3. User Profile Change Reports

This section of contains descriptions for the following reports:

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

See also

User Profile Reports

6.3.1. Blueprint Master Changes

This report displays changes made to the blueprint master.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.2. Blueprint Permissions Changes

This report displays changes to blueprint permissions.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.3. Blueprint Parameter Changes

This report displays changes to blueprint parameters.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.4. Blueprint Object Authority Changes

This report displays changes to object authorities associated with blueprints.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.5. Blueprint Auth Setting Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.6. Blueprint Non-Compliance Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.7. Blueprint 3rd Party Changes

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

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.8. User Profile Exclusion Changes

This report displays changes made to inactive profile exclusion settings.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.9. User Profile Archive Changes

This report displays changes made to archived profile settings.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.10. Profile Inactivity Changes

This report displays changes made to profile inactivity settings.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports

6.3.11. Profile Manager Default Changes

This report displays changes made to Profile Manager defaults.

The report is based on the following collector:

- DATABASE_AUDITING

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**.

Types of entries:

- DL - Record delete
- PT - Record add
- PX - Record added by RRN (relative record number) to a physical file member
- UB - Record edit (before-change)
- UP - Record edit (after-change)

See Also

User Profile Change Reports