NetIQ Security Solutions for IBM i
TG Secure 1.6
Report Reference Guide
Revised October 2017

Legal Notice

Table of Contents

TABLE OF CONTENTS ..... **III**

1. INTRODUCTION **5**

2. ACCESS ESCALATION REPORTS **7**

2.1. ACCESS ESCALATION USAGE 7
2.1.1. Access Escalation Usage Reports *7*
2.1.2. Access Escalation Activity For User *7*
2.1.3. Access Escalation Command Activity For User *8*
2.1.4. Access Escalation Database Update Activity For User *9*
2.1.5. Access Escalation Entitlement Usage For User *10*
2.1.6. Access Escalation Failures For User *12*
2.1.7. Access Escalation Program Activity For User *13*
2.2. ACCESS ESCALATION CONFIGURATION 14
2.2.1. Access Escalation Access Controls Report *14*
2.2.2. Access Escalation Defaults Report *15*
2.2.3. Access Escalation Entitlements Report *15*
2.2.4. Access Escalation File Editors Report *16*
2.2.5. Network Groups Report *17*
2.2.6. Object Groups Report *17*
2.2.7. Operation Groups Report *18*
2.2.8. User Groups Report *19*
2.3. ACCESS ESCALATION CHANGE 19
2.3.1. Access Escalation Access Control Changes *19*
2.3.2. Access Escalation Default Changes *20*
2.3.3. Access Escalation Entitlement Changes *21*
2.3.4. Access Escalation File Editor Changes *22*
2.3.5. Network Groups Changes *23*
2.3.6. Object Groups Changes *24*
2.3.7. Operation Groups Changes *24*
2.3.8. User Groups Changes *25*

3. NETWORK REPORTS **26**

3.1. TRANSACTION REPORTS 26
3.1.1. Central Server Transactions Report *26*
3.1.2. Data Queue Transactions Report *27*
3.1.3. Database Server Transactions Report *29*
3.1.4. DDM Transactions Report *30*
3.1.5. File Server Transactions Report *32*
3.1.6. FTP Transactions Report *33*
3.1.7. Incoming Transactions Report *35*
3.1.8. Network Printer Transactions Report *36*
3.1.9. Network Transactions Report *37*
3.1.10. Remote Command Transactions Report *39*
3.1.11. Remote Execution Transactions Report *40*
3.1.12. Signon Server Transactions Report *42*
3.1.13. Socket Transactions Report *43*

3.1.14. Telnet Transactions Report *44*
3.2. SUMMARY REPORTS 46
3.2.1. Socket Summary by Server *46*
3.2.2. Socket Summary By User *47*
3.2.3. Transaction Summary by Server *48*
3.2.4. Transaction Summary by User *48*
3.3. CONFIGURATION REPORTS 49
3.3.1. Exit Point Configuration Report *49*
3.3.2. Network Groups Report *50*
3.3.3. Object Groups Report *50*
3.3.4. Operation Groups Report *51*
3.3.5. Remote Exit Rules Report *52*
3.3.6. Socket Rules Report *53*
3.3.7. User Groups Report *53*
3.4. CONFIGURATION CHANGES 54
3.4.1. Exit Point Configuration Changes *54*
3.4.2. Network Groups Changes *54*
3.4.3. Object Groups Changes *55*
3.4.4. Operation Groups Changes *56*
3.4.5. Remote Exit Rules Changes *56*
3.4.6. Socket Rules Changes *57*
3.4.7. User Groups Changes *57*

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.

2. Access Escalation Reports

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

2.1. Access Escalation Usage

2.1.1. Access Escalation Usage Reports

This section of reports provides detailed information regarding access escalation usage.

2.1.2. Access Escalation Activity For User

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

Including:

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

To run this report

1) Access the **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**.

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 system submitting the transaction
Receiver	Name of the journal receiver submitting the transaction
Receiver Library	Name of the journal receiver library submitting the transaction
Receiver ASP	Name of the journal receiver ASP submitting the transaction
Action Status	Status of transaction: *PASS - transaction accepted *FAIL - transaction rejected
User Name	Name of the user executing the job
Client IP	IP address of the client server submitting the transaction
Device Name	Device submitting the transaction
Server IP	IP address of the target server receiving the transaction
System Name	Name of 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

2.1.3. Access Escalation Command Activity For User

This report displays command activities.

Records with object type of *CMD.

To run this report

1) Access the **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**.

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
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

2.1.4. Access Escalation Database Update Activity For User

This report displays database file activities.

Records with object type of *FILE.

To run this report

1) Access the **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**.

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 communication
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

2.1.5. Access Escalation Entitlement Usage For User

This report displays successful access attempt.

Records with the action status *PASS.

To run this report

1) Access the **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**.

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
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

2.1.6. Access Escalation Failures For User

This report displays failed access attempts.

Records with action status *FAIL.

To run this report

1) Access the **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**.

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

2.1.7. Access Escalation Program Activity For User

This report displays program activities.

Records with object type of *PGM.

To run this report

1) Access the **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**.

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	Name assigned to the 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

2.2. Access Escalation Configuration

This section of reports provides detailed information regarding access escalation configuration.

2.2.1. Access Escalation Access Controls Report

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.

To run this report

1) Access the **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**.

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.

2.2.2. Access Escalation Defaults Report

This report displays default escalation settings.

To run this report

1) Access the **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**.

Report Column Description

Column	Description
Journal Name	Name of the journal in which configuration changes are stored
Journal Library	Name of the 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
Alert Message Queue	Name of the queue in which alerts are stored
Alert Message Queue Library	Name of the library in which the message queue resides

2.2.3. Access Escalation Entitlements Report

This report displays the entitlement configuration details.

To run this report

1) Access the **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**.

Report Column Description

Column	Description
Entitlement Enabled?	Flag indicating whether the entitlement is enabled Y - Entitlement applied N - Entitlement ignored
User Name	User/User group to which the entitlement applies
Object Name	Object/Object group to which the entitlement applies
Object Library	Library in which the object resides
Object Type	Type of object: *CMD - Command *PGM - Program *FILE - File
Swap User	User/User group to which the entitlement applies when using the AEM interface
Server	Server/server group to which the entitlement applies
Calendar Name	Calendar 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 - Record alerts in the alert queue N - Do not record alerts in the alert queue
Entitlement Description	Description of the entitlement

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.

To run this report

1) Access the **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**.

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

2.2.5. Network Groups Report

This report displays configuration details for all available network groups.

To run this report

1) Access the **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** (Network Groups Report).
9) 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

2.2.6. Object Groups Report

This report displays configuration details for all available object groups.

To run this report

1) Access the **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** (Object Groups Report).
9) 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

2.2.7. Operation Groups Report

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.

To run this report

1) Access the **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 **4** (Operation Groups Report).
9) 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

2.2.8. User Groups Report

This report displays configuration details for all available user groups.

To run this report

1) Access the **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 **4** (User Groups Report).
9) 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

2.3. Access Escalation Change

This section of reports provides detailed information regarding changes made to access escalation.

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).

To enable this report:

1) Access the **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 **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**.

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
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

2.3.2. Access Escalation Default Changes

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

To enable this report:

1) Access the **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 **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**.

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.

To enable this report:

1) Access the **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 **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**.

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
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

2.3.4. Access Escalation File Editor Changes

This report displays all changes to the file editor.

To enable this report:

1) Access the **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 **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**.

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

2.3.5. Network Groups Changes

This report displays all changes made to network group configurations.

To enable this report

1) Access the **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 **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** (Network Groups Changes Report).
9) Press **Enter**.

2.3.6. Object Groups Changes

This report displays all changes made to object group configurations.

To enable this report

1) Access the **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 **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** (Object Groups Changes Report).
9) Press **Enter**.

2.3.7. Operation Groups Changes

This report displays all changes made to operation group configurations.

To enable this report

1) Access the **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 **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** (Operation Groups Changes Report).
9) Press **Enter**.

2.3.8. User Groups Changes

This report displays all changes made to user group configurations.

To enable this report

1) Access the **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 **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 **4** (User Groups Changes Report).
9) Press **Enter**.

3. Network Reports

3.1. Transaction Reports

This section of reports provides detailed information regarding incoming transactions from remote servers.

3.1.1. Central Server Transactions Report

This report lists attempts to access the central server.

To enable this report

1) Access the **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 **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**.

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
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

3.1.2. Data Queue Transactions Report

This report lists attempts to access the data queue server.

To enable this report

1) Access the **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 **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**.

Associated exit point

- QIBM_Q2HQ_DATA_QUEUE

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

3.1.3. Database Server Transactions Report

This report lists attempts to access the database server.

To enable this report

1) Access the **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 **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**.

Associated exit points

- QIBM_QZDA_INIT
- QIBM_QZDA_NDB1
- QIBM_QZDA_ROI1
- QIBM_QZDA_SQL1

Report Column Description

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

System Name	Name of system submitting the DB transaction request
Receiver	Name of the journal receiver submitting the DB transaction request
Receiver Library	Name of the journal receiver library submitting the DB transaction request
Receiver ASP	Name of the journal receiver ASP submitting the DB transaction request
Action Status	Status of incoming transactions: *PASS - transaction accepted *FAIL - transaction rejected
User Name	Name of the user executing the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming transactions.
Server Name	Server used to execute the DB transactions. This report displays only DB server transactions. Valid values included: DBINIT - Perform server initiation DBNDB - Perform native database request DBSQL - Perform SQL requests DBROI - Retrieve object information and catalog function **Note:** See the **Network Transactions** report for all server type transactions.
Function Name	Function used to execute the DB transaction
Command Name	Command used to execute the DB transaction
IP Address	IP address from which the DB transaction originated
Object Name	Object targeted by the DB transaction
Object Library	Object library targeted by the DB transaction
Object Type	Object type targeted by the DB transaction

3.1.4. DDM Transactions Report

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

To enable this report

1) Access the **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 **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**.

Associated exit point

- QIBM_QTF_TRANSFER

Report Column Description

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

IP Address	IP address from which the DDM transaction originated
Object Name	Object targeted by the DDM transaction
Object Library	Object library targeted by the DDM transaction
Object Type	Object type targeted by the DDM transaction

3.1.5. File Server Transactions Report

This report lists attempts to access the file server.

To enable this report

1) Access the **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 **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**.

Associated exit point:

- QIBM_QPNFS_FILE_SERV

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
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

3.1.6. FTP Transactions Report

This report lists attempts to access the FTP server.

To enable this report

1) Access the **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 **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**.

Associated exit points

- QIBM_QTMF_CLIENT_REQ
- QIBM_QTMF_SERVER_REQ
- QIBM_QTMF_SVR_LOGON

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
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

3.1.7. Incoming Transactions Report

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

To display the audit status

1) Access the **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 **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**.

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

3.1.8. Network Printer Transactions Report

This report lists attempts to access the network printer server.

To enable this report

1) Access the **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 **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**.

Associated exit point

- QIBM_QNPS_ENTRY

Report Column Description

Column	Description
Sequence Number	Order in which the remote NETPRT 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 NETPRT transaction request
System Name	Name of system submitting the NETPRT transaction request
Receiver	Name of the journal receiver submitting the NETPRT transaction request
Receiver Library	Name of the journal receiver library submitting the NETPRT transaction request
Receiver ASP	Name of the journal receiver ASP 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

3.1.9. Network Transactions Report

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

To enable this report

1) Access the **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 **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**.

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 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

3.1.10. Remote Command Transactions Report

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

To enable this report

1) Access the **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 **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**.

Associated exit point

- QIBM_QZRC_RMT

Report Column Description

Column	Description
Sequence Number	Order in which the remote RMTCMD 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 RMTCMD transaction request
System Name	Name of system submitting the RMTCMD transaction request
Receiver	Name of the journal receiver submitting the RMTCMD transaction request
Receiver Library	Name of the journal receiver library submitting the RMTCMD transaction request
Receiver ASP	Name of the journal receiver ASP submitting the RMTCD 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

3.1.11. Remote Execution Transactions Report

This report lists attempts to access the remote execution server.

To enable this report

1) Access the **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 **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**.

Report Column Description

Column	Description
Sequence Number	Order in which the incoming REXEC 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 REXEC transaction request
System Name	Name of system submitting the REXEC transaction request
Receiver	Name of the journal receiver submitting the REXEC transaction request
Receiver Library	Name of the journal receiver library submitting the REXEC transaction request
Receiver ASP	Name of the journal receiver ASP 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

3.1.12. Signon Server Transactions Report

This report lists attempts to access the SIGNON server.

To enable this report

1) Access the **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 **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**.

Associated exit point:

- QIBM_QZSO_SIGNONSRV

Report Column Description

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

3.1.13. Socket Transactions Report

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

To enable this report

1) Access the **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 **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**.

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 initiating the socket transaction

3.1.14. Telnet Transactions Report

This report lists the attempts to access the Telnet server.

To enable this report

1) Access the **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 **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**.

Associated exit points

- QIBM_QTMF_CLIENT_REQ
- QIBM_QTMF_SERVER_REQ
- QIBM_QTMF_SVR_LOGON

Report Column Description

Column	Description
Sequence Number	Order in which the incoming TELNET 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 TELNET transaction request
System Name	Name of system submitting the TELNET transaction request
Receiver	Name of the journal receiver submitting the TELNET 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
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

3.2. Summary Reports

This section of reports provides summary information regarding incoming transactions from remote servers.

3.2.1. Socket Summary by Server

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

To enable this report

1) Access the **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 **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**.

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

3.2.2. Socket Summary By User

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

To enable this report

1) Access the **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 **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**.

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

3.2.3. Transaction Summary by Server

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.

To run this report

1) Access the **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**.

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

3.2.4. Transaction Summary by User

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.

To run this report

1) Access the **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**.

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

3.3. Configuration Reports

This section of reports provides details regarding network security configuration.

3.3.1. Exit Point Configuration Report

This report displays configuration details for all available exit points.

To run this report

1) Access the **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**.

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?	Identifies the status auditing: *YES - Auditing is enabled, so transactions are being tracked *NO - Auditing is disabled, so transactions are not being tracked
Security On?	*YES - Security monitoring is enabled, so rules will be applied. *NO - Security monitoring is disabled, so rules will not be applied.

3.3.2. Network Groups Report

This report displays configuration details for all available network groups.

To run this report

1) Access the **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** (Network Groups Report).
9) 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

3.3.3. Object Groups Report

This report displays configuration details for all available object groups.

To run this report

1) Access the **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** (Object Groups Report).
9) 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

3.3.4. Operation Groups Report

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.

To run this report

1) Access the **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 **4** (Operation Groups Report).
9) 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

3.3.5. Remote Exit Rules Report

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

To run this report

1) Access the **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**.

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

3.3.6. Socket Rules Report

This report displays configuration details for all available socket rules.

To run this report

1) Access the **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**.

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

3.3.7. User Groups Report

This report displays configuration details for all available user groups.

To run this report

1) Access the **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 **4** (User Groups Report).

9) 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

3.4. Configuration Changes

This section of reports provides details regarding changes to network security configuration.

3.4.1. Exit Point Configuration Changes

This report displays all changes made to exit point configurations.

To enable this report

1) Access the **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 **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**.

3.4.2. Network Groups Changes

This report displays all changes made to network group configurations.

To enable this report

1) Access the **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 **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** (Network Groups Changes Report).
9) Press **Enter**.

3.4.3. Object Groups Changes

This report displays all changes made to object group configurations.

To enable this report

1) Access the **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 **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** (Object Groups Changes Report).
9) Press **Enter**.

3.4.4. Operation Groups Changes

This report displays all changes made to operation group configurations.

To enable this report

1) Access the **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 **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** (Operation Groups Changes Report).
9) Press **Enter**.

3.4.5. Remote Exit Rules Changes

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

To enable this report

1) Access the **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 **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**.

3.4.6. Socket Rules Changes

This report displays all changes made to socket rule configurations.

To enable this report

1) Access the **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 **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**.

3.4.7. User Groups Changes

This report displays all changes made to user group configurations.

To enable this report

1) Access the **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 **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 **4** (User Groups Changes Report).
9) Press **Enter**.