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

Legal Notice

Table of Contents

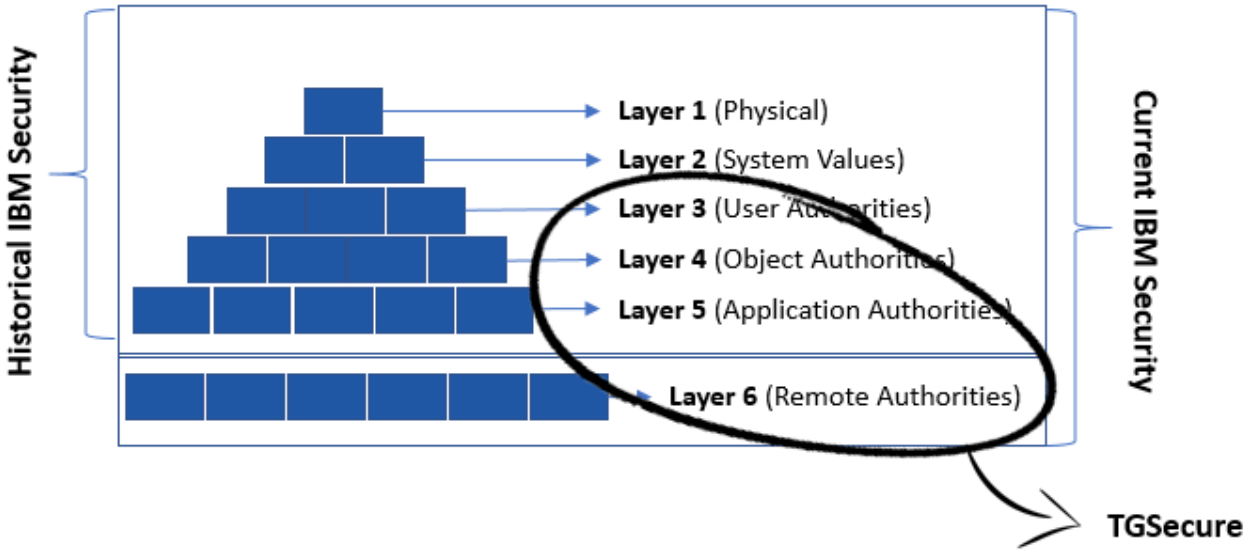
1. Introduction

1.1. Historical Perspective of Security

Before we talk about what TGSecure is or does, let's talk about where it fits. When the IBM® iSeries was introduced in 1988, client/server configurations and Internet-based networks were not widely used. At that time, iSeries servers were accessed through locally attached terminals. Security was controlled through the following structure:

- **Physical Security** - Restrict access by setting up the server in a secure computer room
- **System Values** - Use values that control system access (10: Physical Security, 20: Password Security, 30: Object Security, 40: System Integrity, 50: Resource Security)
- **User Authorities** - Restrict the user's ability to execute i5/OS or user-defined commands
- **Object Authorities** - Restrict the user's ability to execute commands on objects
- **Application Authorities** - Restrict the user's ability to access data or commands
- Times have changed, and many iSeries servers are accessed via remote connections, which requires additional security structure:
- **Remote Authorities** - Restricting remote client access

TGSecure provides tools to help you manage user, object, application, and remote access.



See also:

- Product Overview
- Product Features
- Decision Algorithm
- IBM System Values (external IBM Knowledge base topic)

1.2. Product Overview

TGSecure allows you to manage security threats on IBM® iSeries systems from both external and internal sources. In addition, it provides reports for monitoring the security health of your system.

Note: While you can use TGSecure as a standalone product, it is also one component of a powerful security suite. For more information about the suite or other products in the suite, go to TrinityGuard.com.

See also:

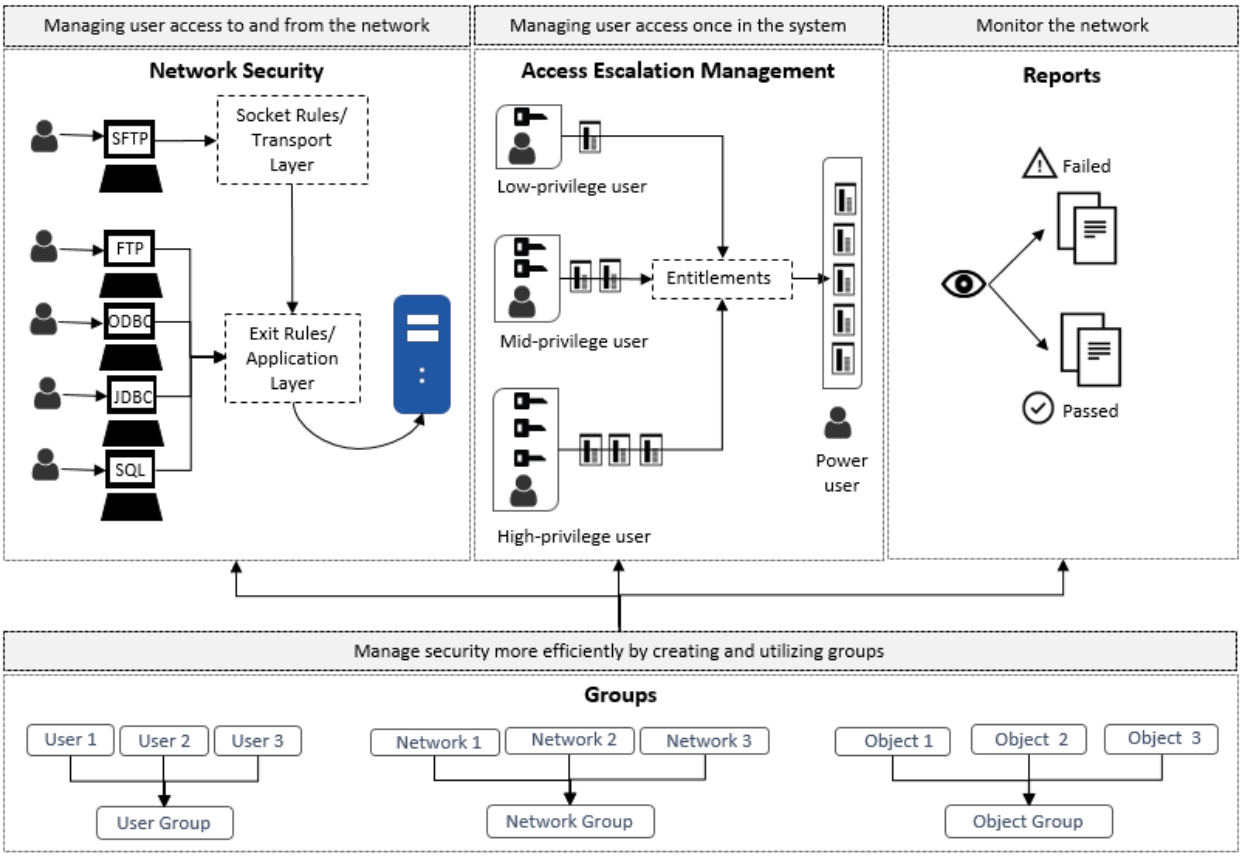
Features

Decision Algorithm

Getting Started Using TGSecure

1.3. Features

To help you design, manage, and maintain a secure system, TGSecure includes the following product features:



Network Security

This feature allows you to monitor remote requests (incoming transactions). The system performs this task by comparing incoming transactions with entry rules (i.e., socket and exit) and assigning each transaction a PASS or FAIL status based on those rules. The rules are evaluated using a decision algorithm.

- Manage Socket Rules

- Manage Exit Rules

Access Escalation Management

This feature allows you to manage privilege escalated access using user entitlements.

- Manage Entitlements
- Manage Access Control

Reports

This feature allows you to monitor activities that impact system security using built-in and custom reports.

Note: See Manage Reports for more information.

Groups

This feature enhances your ability to quickly manage security using user, network, operation, or object groups.

Note: Groups are used in conjunction with user entitlements to manage privilege escalated access.

- Manage User Groups
- Manage Network Groups
- Manage Operations Groups
- Manage Object Groups

See also:

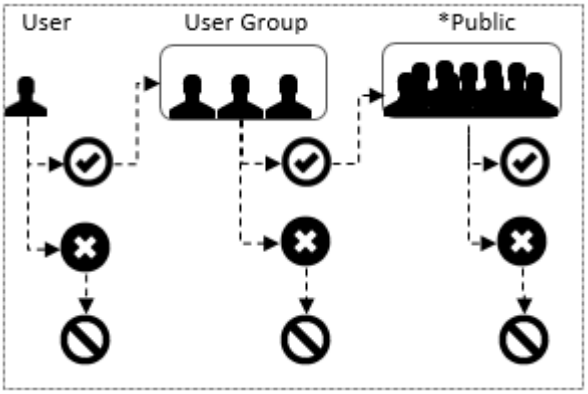
Rules Decision Algorithm
Rules Suggestion Engine

1.4. Rules Decision Algorithm

The rules evaluation process used to manage network security is controlled through a decision-making algorithm, which coordinates a series of authority checks.

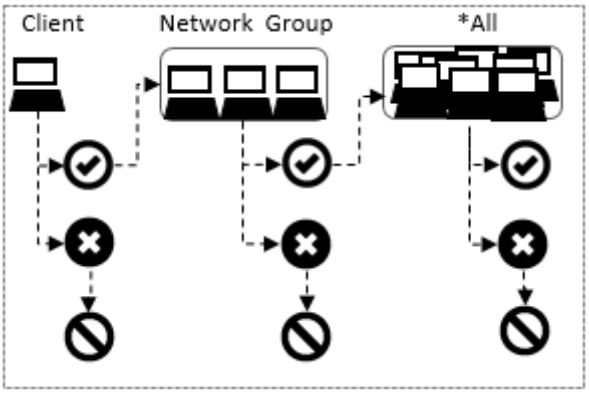
Check 1: Evaluate User

1) Apply rules for a specific user
2) Apply rules for a specific user group
3) Apply rules that apply to all users (*PUBLIC)



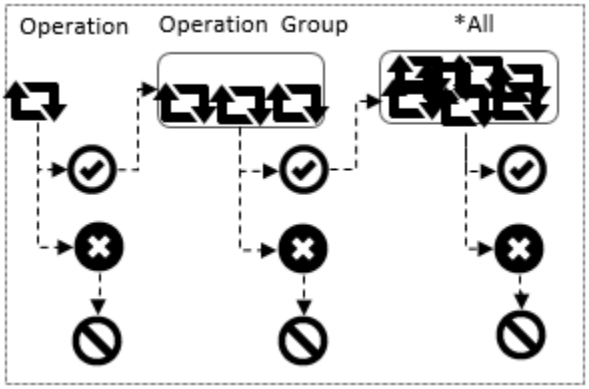
Check 2: Evaluate Network (Client Server)

1) Check rules for a specific client IP
2) Check rules for a generic IP (e.g., 11.111*)
3) Check rules for a network group
4) Check rules that apply to all networks (*ALL)



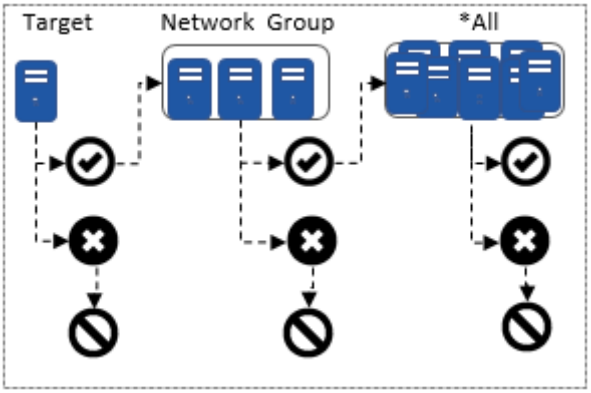
Check 3: Evaluate Operation

1) Check rules for a specific operation
2) Check rules for an operation group
3) Check rules that apply to all operations (*ALL)



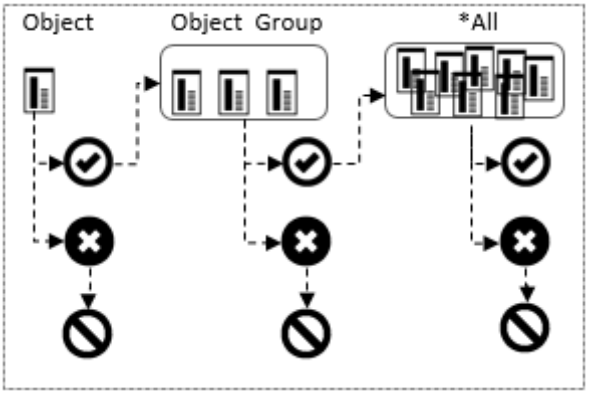
Check 4: Evaluate Network (Target Server)

1) Check rules for a specific target IP
2) Check rules for a generic IP (e.g., 11.111*)
3) Check rules for network group
4) Check rules that apply to all networks (*ALL)



Check 5: Evaluate Object

1) Check rules for a specific object
2) Check rules for a generic object (e.g., /home/etv/*…)
3) Check rules for an object group
4) Check rules that apply to all objects (*ALL)



See also:

For information about how decisions are made regarding access escalation (the other main feature in the product), see Access Escalation Management.
For information about how to run reports, see Working with Reports.

1.5. Rules Suggestion Engine

Rules (i.e., exit rules or socket rules) are a power tool for managing network security, but to use rules efficiently, they must be used in conjunction with groups.

For example, if a new user is added to the system, and the security administrator determines that the user should have limited access, the administrator can easily create a rule defining the appropriate level of access for that individual, but that would be inefficient if the user was hired to fulfil a role shared by many. In that case, it would be more efficient to create a role-based rule that could be apply to a group of users.

Rule Example

Bob joins the company. Bob is provided with an IBM login. That morning, Bob logs into the system from a workstation set up in a training room for new hires. The administrator can see Bob's SIGNON transaction by viewing the list of incoming transactions. The administrator notices that in the evening Bob logs in again, but from a different client IP address. At this point in Bob's onboarding, he should only access the system while under the supervision of his mentor or trainer. Bob is not doing anything wrong, but he has the potential because of his lack of experience to cause harm. Therefore, the administrator decides to create a rule that limits Bob's access while he is completing his training.

Rule Suggestion Example

The administrator creates a rule limiting Bob's access and tries to save the rule, but the suggestion (intelligence) engine notifies the administrator that a similar rule already exists, and instead of creating a rule specific to Bob, the administrator should instead add Bob to a user group titled *:Trainees* that was created six months earlier for a group of new hires in a similar situation.

Rule Suggestion Interface

There's no way to directly access the rules suggestion engine. The interface appears at the time you save a new rule and only if the suggestion (intelligence) engine identifies a situation in which updating an existing user group or network group would be more efficient than creating a new rule.

See also:

Manage Incoming Transactions

Manage Exit Rules

Manage Socket Rules

Manage User Groups

2. Getting Started

2.1. Log into TGSecure

Use this task to log into TGSecure.

To log into TGSecure

1) Sign into your IBM i server.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.

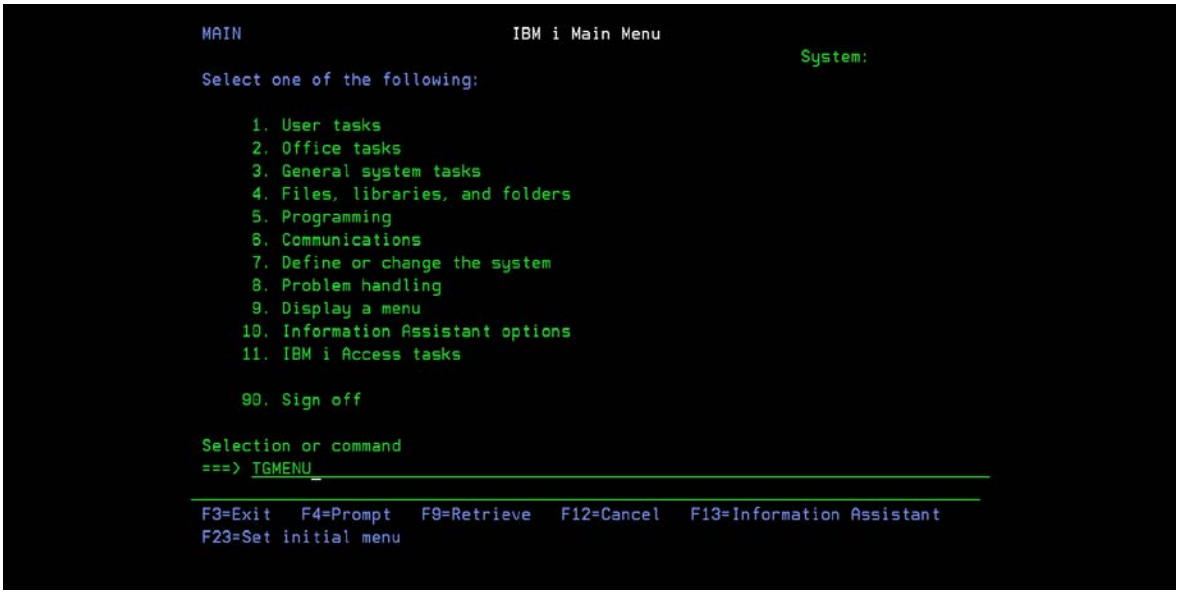


Figure: IBM i Main Menu

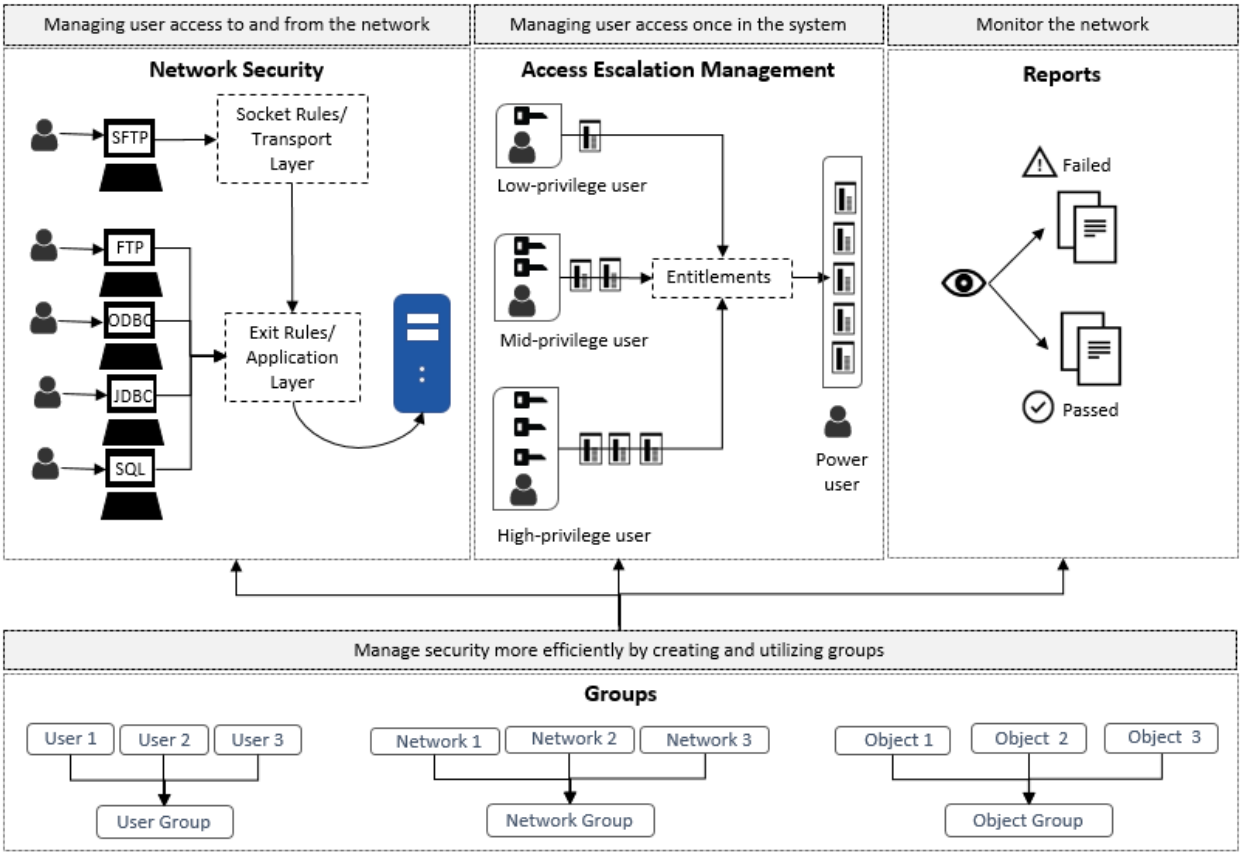
4) At the **Selection or command** prompt, enter **2** (TGSecure).

2.2. Getting Starting Using TGSecure

TGSecure allows you to do the following:

- **Network Security** - Monitor incoming transactions and manage network security threats using rules (i.e., socket rules and exit rules)
- **Access Escalation Management** - Monitor and manage powerful-user activity and implement the least-privilege model using entitlements
- **Reports** - Generate reports to monitor network activity evaluate security health (i.e., pass/fail status)
- **Groups** - Create groups (i.e., user, network, operation, and object) to manage security more efficiently

2.2.1. Features



2.2.2. Tasks

There is no single linear process for implementing TGSecure, but the following describes how a typical implementation might work. It's important to remember that security management is an iterative process.

Step 1 **Monitor Network Access**

To enhance security, you first need to understand who is accessing your network.

The Incoming Transactions module of TGSecure allows you to display the incoming transactions requesting access and executing commands on the server.

Step 2 **Create Groups**

With the vast number of elements that impact security, it might be necessary to group items together for efficiency.

For example, it might not be efficient to create an entitlement for each user. It would be more efficient to apply a single entitlement to a group of users. The same would hold true for a single rule being applied to a group of networks.

The Grouping module of TGSecure allows you to create groups for the following elements:

- Users
- Networks
- Operations
- Objects

Step 3	**Manage Network Access** Once you have a better awareness of who and how your system is accessed and you have created what you feel are logical and useful groupings, you can begin limiting network access. The Exit Point and Socket Rules modules of TGSecure allows you to apply rules to manage network access: • Application layer (exit rules) • Transport layer (socket rules)
Step 4	**Implement Least-privilege Model** Once the appropriate users have access to your system, you then want to ensure that these users have the appropriate level of authority to perform assigned tasks, but no more than that. The Access Escalation Management (AEM) module of TGSecure allows you to create entitlements to manage system access.
Step 5	**Run Reports** Ensuring your server and system remain secure involves continuous and proactive monitoring. The Reporting module of TGSecure allows you to run built-in reports and create custom reports to monitor security health of your server and system. **Note**: The built-in reports available to you are dependent on your license agreement.

3. Network Security

3.1.1. Introduction

In the past, the risk related to network security was limited to internal networks and required limited security measures. With the advancement of technology and availability of open networks, security risks increased. To bridge the security gap caused by open networks, IBM introduced remote exit points, which are hooks that allow you to attach custom exit programs that monitor network traffic (server transactions). You can customize these exit programs not only to monitor, but also limit access with the addition of exit rules, which allow you to establish pass/fail criteria for transactions. The introduction of exit points addressed the security risks associated with many traditional protocols (e.g., FTP, TELNET, and ODBC, etc.), but exit points did not close the security gap completely. Newer protocols (i.e., SSH and SFTP) were introduced to address weaknesses in older protocols in which data was transmitted in clear text. While the newer protocols reduced some security risks, they also opened the door to other risks because they bypassed the established remote exit points, which reside at the application level, and instead used socket communication at the transaction level.

The socket level risk was addressed by IBM with IBM i version 7.1. at which point you could begin monitoring socket communications and applying socket rules.

3.1.2. Working with Network Security

This section describes tasks associated with ensuring your system is secure from outside threats (those attempting to access your network).

To access the Network Security interface

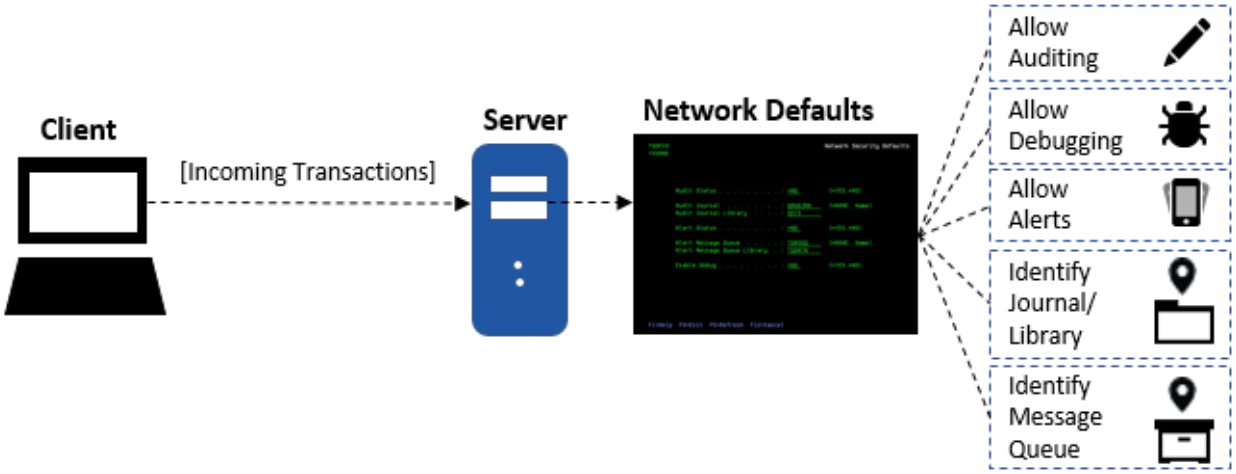
1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

3.2. Network Security Defaults

3.2.1. Working with Network Security Defaults

This section describes working with network security defaults. Network security defaults define the following:

- Journal in which the network transactions are stored
- Library in which the journal resides
- Message queue in which to store alert data
- Library in which message queue resides
- Whether debugging is enabled (log is created)
- Whether auditing (data collection) is enabled
- Whether to enable alerts



To access the Network Security Defaults interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**.

See also:

Log into TGSecure

Display Network Security Defaults

Manage Network Security Defaults

3.2.2. Display Network Security Defaults

Use this task to display network security defaults.

To display the network security defaults

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 **11** (Network Security Defaults).
5) Press **Enter**.

Note: The **Network Security Defaults** interface is displayed

3.2.3. Manage Network Security Defaults

Use this task to do the following:

- Display network security defaults
- Enable auditing
- Enable alerts
- Enable debug log

- Track configuration changes

3.2.3.1. Display Network Security Defaults

To display the network security defaults

1) Login to the IBM i interface.
2) At the **Selection or command** prompt, enter **TGMENU** to access the **Main** menu.
3) At the **Selection or command** prompt, enter **1** (Network Security).
4) Press **Enter**.
5) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
6) Press **Enter**.

Note: The **Network Security Defaults** interface is displayed

Field	Description
Audit Status	Indicates whether auditing is enabled globally (for all exit points). Auditing is required if you plan to run network security reports. ***YES** - Record incoming transaction data in the audit journal ***NO** - Do not record incoming transaction data in the audit journal **Tip**: If auditing is disabled at the network security (module) level, then auditing will not occur. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable auditing at the secondary level (each exit point) if you want to record auditing data for a specific exit point. See Manage Exit Points for information about setting the audit status for an individual exit point.
Audit Journal	Name of the journal in which to store audit data.
Audit Journal Library	The library in which the audit journal resides
Audit Configuration Changes	Indicates whether to track configuration changes made to network security. Tracking is required if you plan to run network security configuration change reports. **Y** - Track network security configuration changes **N** - Do not track network security configuration changes **Note**: There are multiple product modules (e.g., network security, access escalation, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules. **Tip**: See Run Network Security Reports for information about running configuration change reports.
Alert Status	Indicates whether alerting is enabled globally (for all exit points). Alerting is required if you plan to send alert notifications. ***YES** - Record an alert for all (PASS and FAIL) connection attempts ***NO** - Do not record alerts **Tip**: If alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enable at the exit point (secondary) level. The

	module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. See Manage Exit Points for information about setting the alert status for an individual exit point.
Alert Message Queue	Name of the queue in which to store alert messages
Alert Message Queue Library	The library in which the alert message queue resides
Enable Debug	Indicates whether to collect data for a debug log. The debug log is not required, but might help with troubleshoot issues. ***YES** - Create debug log ***NO** - Do not create debug log

3.2.3.2. Enable Auditing

Use this task to enable auditing in the Network Security module. Auditing is required if you plan to run network security reports.

Tip: If auditing is disabled at the network security (module) level, then auditing will not occur. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable it at the secondary level (each exit point) if you want to record auditing data for a specific exit point.

To enable auditing in the Network Security module

1) Access the **Network Security Defaults** interface.
2) In the **Audit Status** field, enter ***YES**.
3) Press **Enter**.

See also

Manage Exit Points

3.2.3.3. Enable Alerts

Use this task to enable alerts in the Network Security module. Alerting is required if you plan to send alert notifications.

Tip: If alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enable at the exit point (secondary) level. The module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point.

To enable alerts in the Network Security module

1) Access the **Network Security Defaults** interface.
2) In the **Alert Status** field, enter ***YES**.
3) Press **Enter**.

See also

Manage Exit Points

3.2.3.4. Enable Debug Log

Use this task to enable the debug log in the Network Security module. The debug log is not required, but might help with troubleshoot issues.

To enable debug log in the Network Security module

1) Access the **Network Security Defaults** interface.
2) In the **Enable Debug** field, enter ***YES**.
3) Press **Enter**.

3.2.3.5. Track Configuration Changes

Use this task to enable tracking of configuration changes in the Network Security module. Tracking is required if you plan to run network security configuration change reports.

To enable tracking of configuration changes in the Network Security module

1) Access the **Network Security Defaults** interface.
2) In the **Audit Configuration Changes** field, enter **Y**.
3) Press **Enter**.

See also

Run Network Security Reports

3.2.4. Run Network Security Reports

Use this task to generate network security reports.

To run Network Security Reports

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) Choose the desired report category from the list.

– Transaction Reports
– Summary Reports
– Configuration Reports
– Configuration Change Reports

7) Press **Enter**.
8) Choose the desired report from the list.
9) Press **Enter**.

See also:

- Run Transaction Reports
- Run Socket Reports

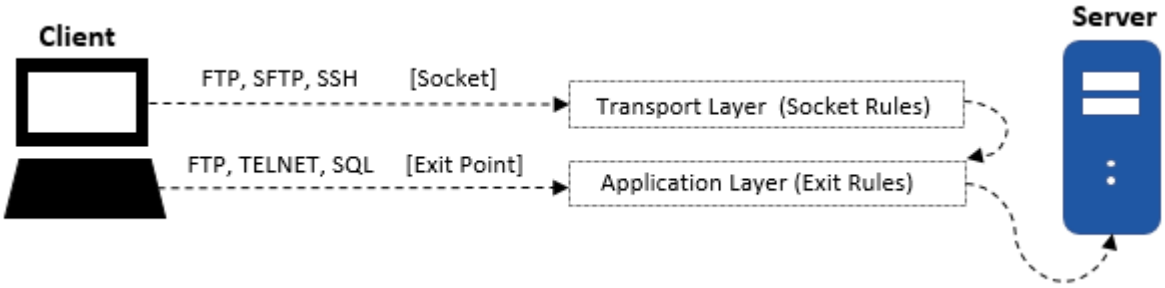
- Run Exit Point Reports
- Run Exit Rule Reports
- Run Socket Rule Reports

3.3. Transactions

3.3.1. Working with Transactions

This section describes how to work with transactions. Remote transactions access the server through either a socket or exit point. The transaction can go directly from the client to the server through a socket unless an associated exit point has been defined. In which case, the system then checks for both socket and exit point rules before allowing access to the server.

For example, a user might attempt to access the system via the socket layer using FTP. If a socket rule exists for the FTP transactions, the system will validate that any socket rule criteria is met before allowing the FTP transaction. IBM has also established a standard exit point for FTP transactions, so any FTP transaction must also go through a second layer of security. The system will validate that any exit rules criteria is met before allowing the FTP transaction. Therefore, depending on the protocol used (e.g., FTP, SFTP, etc.), a transaction might go through both socket and exit point validation.



To access the Incoming Transactions interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Incoming Transactions).
5) Press **Enter**.

Note: The **Incoming Transactions** interface is displayed.

See also:

Log into TGSecure

Display List of Incoming Transactions

Manage Incoming Transactions

Run Incoming Transactions Report

3.3.2. Display List of Incoming Transactions

Use this task to do the following with transactions:

- Display list of transactions
- Sort transactions
- Move to a specific location within list of displayed transactions
- Filter transactions

3.3.2.1. Display List

Use this task to display the list of incoming transactions.

To display the list of incoming transactions

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 **1** (Incoming Transactions).
5) Press **Enter**.

Note: The **Incoming Transactions** interface is displayed.

3.3.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Incoming Transactions** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

3.3.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Incoming Transactions** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

3.3.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Incoming Transactions** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

3.3.3. Manage Incoming Transactions

Use this task to do the following with incoming transactions:

- Display incoming transactions details
- Delete an incoming transaction
- Archive and then delete incoming transactions
- Create a security rule based on the transaction
- Accept rule suggestion

To manage incoming transactions, access the **Incoming Transactions** interface.

To access the Incoming Transactions interface

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 **1** (Incoming Transactions).
5) Press **Enter**.

Note: The **Incoming Transactions** interface is displayed.

3.3.3.1. Display Incoming Transaction Details

Use this task to display the transaction details. There is limited space in the **Incoming Transactions** interface, so not all the details associated with an incoming transaction are displayed. Therefore, this task allows you to see the complete details for each incoming transaction.

To display the incoming transaction details

1) Access the **Incoming Transactions** interface.
2) In the **OPT** column for the desired transaction, enter **5** (Display).
3) Press **Enter**.

Field	Description
Transaction Type	There are two types of transactions: *TRN - Transaction coming through an exit point *SOC - Transaction coming through a socket
User Name	User who initiated the transaction
SSL Communication	Flag indicating whether SSL is enabled
Operation Server	Type of server
Function	Function being executed

Field	Description
Client IP	IP address of the server initiating the transaction
Server Name	Name of the server from which the user is initiating the transaction
Transaction Count	Total number of transactions attempted **Note**: The incoming transactions displayed in the interface are determined by the **Collector Status**. **Tip**: See Manage Exit Points for information about editing the **Collector Status**.
Action	Status of connection attempt (*PASS or *FAIL)
Reason	Reason for the transaction
Suggestion	Comments associated with the transaction
Object Details	Object effected by the transaction

3.3.3.2. Delete Incoming Transaction

Use this task to delete transactions.

Usage examples:

- You find that a specific transaction adds no value to your analysis
- You want to see what effect a new rule has on transactions from a specific client server
- You want to see what effect a new rule has on transactions for a specific user

To delete an incoming transaction

1) Access the **Incoming Transactions** interface.
2) In the **OPT** column for the desired transaction, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct transaction.
5) Press **Enter**.

3.3.3.3. Archive Incoming Transactions

Use this task to delete all transactions older than a specified date. You also have the option to create an archive before deleting the transactions. This is useful if you need to restore the list of transactions at a later point.

Usage examples:

- You want to delete older transactions to see what new transaction are coming in.
- You want to perform a transaction count.

For example, the customer might state that the product is running slowly. Therefore, you clear (delete) the transactions to get a better picture of what is occurring on the server. You discover that the customer is running hundreds of thousands of connections per second just to read one file. This is very inefficient and the transaction counts helps show this.

To archive incoming transactions

1) Access the **Incoming Transactions** interface.
2) Press the **F16** (Archive/Delete Transactions) function key.

3) Enter the age (in days) of the transactions you want to keep.

Note: For example, enter **1** to keep all transaction for today, but delete all transaction older than 1 day.

4) Enter ***YES** to create an archive before deleting the transactions.

3.3.3.4. Create a Rule Based on a Transaction

Use this task to create a security rule to address a security risk identified in your analysis of incoming transactions. For example, while you are reviewing the list of incoming transaction, you might identify suspicious activity coming from a server. You can quickly create a security rule (e.g., socket or exit rule) to block transactions from that server directly from the **Incoming Transactions** interface.

To create a security rule based on a transaction

1) Access the **Incoming Transactions** interface.
2) In the **OPT** column for the desired transaction, enter **1** (Create).

Note: The **Tran Type** field identifies the type of transaction: SOC = socket and TRN = exit point transaction. The screen the appears next is dependent on the type of transaction. The **Create Rule - Socket** screen appears when you are creating a socket rule and the **Create Rule - Exit** screen appears when you are creating an exit rule.

3) Press **Enter**.
4) Enter the necessary parameters to define your rule.
5) Press the **F23** (Accept Rule) function key.
6) Press **Enter**.

Note: At this point, you might receive suggestions from the Rules Suggestion Engine. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server) as well.

Tip: If you decide to accept a suggestion, but then change your mind, in the **OPT** column for the desired rule, enter **6** (Undo Suggestion). **Note**: The opportunity the undo a suggestion is only available during the current session. Once you exit the session (press **F3** or **F12**), the option to undo the suggestion is lost. Any change after the point must be made manually by updating the group(s).

3.3.3.5. Accept a Rule Suggestion

Use this task to accept a suggestion made by the Rules Suggestion Engine. The intelligence engine provides suggestion when it might be more efficient to update a group versus create a new rule. In other words, a rule might already exist that utilizes a group, and instead of creating a new rule specific to an individual user, it might be more efficient to add the user to an existing user group that is reference by an existing rule. Therefore, a new rule is not created. Instead an existing user group is updated.

Note: You will only see the **Rule Suggestion** interface when the intelligence engine finds an opportunity to better utilize existing groups.

Tip: You can press **12** (Cancel) to reject any suggestions and exit the **Rule Suggestion** interface at any time.

To accept a rule suggestion

Obviously, the suggestions provided by the intelligence engine will vary depending on the situation, but expect to see one of the following variations:

Situation	If...	Then..
1	The intelligence engine provides one suggestion.	In the **Opt** column, enter **1** to acknowledge acceptance of the suggestion, and then press **Enter** to exit the **Rule Suggestion** interface.
2	The intelligence engine provides multiple suggestions from which you can select. For example, for socket rules, you could add the user to a user group, or you could add the client IP to a network group, or you could add the server name to a network group. In addition, for exit rules, operation can be added to operation groups, and object can be added to object groups.	In the **Opt** column, enter **1** beside the suggestion you feel is the most appropriate for your situation, and then press **Enter** to exit the **Rule Suggestion** interface.
3	Multiple groups must be modified in combination. In other words, to eliminate the need for the new rule, you must update a user group and a network group in combination. Therefore, in this situation, multiple groups are modified simultaneously.	Press **F23** (Confirm Adding to Group), and then press **Enter** to exit the **Rule Suggestion** interface.
4	You want to reject any and all suggestions.	Press **12** (Cancel) to exit the **Rule Suggestion** interface.

Tip: Use option **6** (Undo Suggestion) from the **Incoming Transactions** interface to undo you selection. Once you exit the session (press **F3** or **F12**), the ability to undo a suggestion is lost.

See also:

Rules Suggestion Engine
Rules Decision Engine
Manage User Groups
Manage Socket Rules
Manage Exit Rules

*3.3.4. Run Transactions (*TRN) Report*

Use this task to generate reports that display the following for incoming transactions:

- Incoming transaction details
- Incoming transaction summary by server
- Incoming transaction summary by user
- Network transaction details

3.3.4.1. Run Incoming Transaction Details

Use this report to display incoming transaction details.

To run Incoming Transactions 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.4.2. Run Transaction Summary by Server Report

Use this report to display incoming transaction details by server.

To run Transaction Summary by Server 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.4.3. Run Transaction Summary by User Report

Use this report to display incoming transaction details by user.

To run Transaction Summary by User 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.4.4. Run Network Transaction Report

Use this report to display network transaction.

To run Network Transaction 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 Transaction Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

*3.3.5. Run Socket Transaction (*SOC) Reports*

Use this task to generate reports that display the following for socket rules.

- Socket transactions details
- Socket summary by server
- Socket summary by user

3.3.5.1. Run Socket Transaction Report

Use this report to display the socket transaction details.

To run Socket Transaction 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.5.2. Run Socket Summary by Server Report

Use this report to display socket transaction details by server.

To run Socket Summary 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.5.3. Run Transaction Summary by User Report

Use this report to display socket transaction details by user.

To Run Transaction Summary by User 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.4. Exit Points

3.4.1. Working with Exit Points

This section describes working with exit points. In the beginning of computing, the risk related to network security was limited to internal networks and required limited security measures. With the advancement of technology and with the increase in availability of open networks, security risks have increased. To bridge the security gap caused by open networks, IBM introduced remote exit points, which are hooks that allow you to attach custom exit programs that evaluate exit rules, which define the criteria used to determine whether a transaction should be allowed or rejected.

Analogy

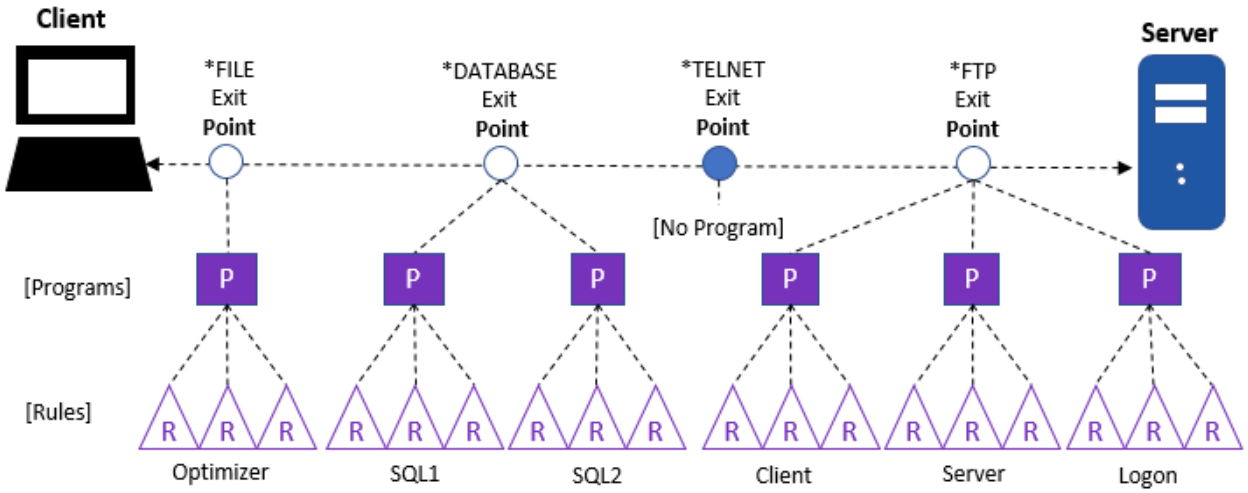
The prior paragraph uses a lot of jargon, so here is an analogy to help you conceptualize what an exit point represents. Say that your IBM server is a building. In the past, if someone wanted to access your building, they would just walk to it. Then, at some point, people started riding horses, and then bicycles, and then cars. To accommodate these newer forms of transportation, IBM built a parking lot. In the parking lot, they provided spots (points): a hitching rail for the horses, a bicycle rack for the bikes, and painted parking slots for the cars. You can image exit points as the elements in a parking lot that accommodate the different modes of transportation. So now image your exit program as a vehicle (a car) that you can park in an exit point (parking spot). Your vehicle (exit program) carries in it passengers (exit rules). Once an exit program is parked in an exit point, the rules (passengers) associated with that exit program become linked to the exit point.

Client-Server Communication Process via transport layer:

(1) Exit Point (Parking Spot): An exit point is a point in the network communication process between a client and a server where control is turned over to an exit program if an exit program exists.

(2) Exit Program (Car): An exit programs can be created for each type of network communication (FTP, ODBC, JDBC, SQL, etc.). Exit programs control execution of transactions between a client and a server.

(3) Exit Rule (Passenger): An exit rule defines the criteria by which an exit program determines whether a transaction is allowed or rejected (forbidden).



Note: It's not necessary to manually associate an exit rule to an exit program. That happens programmatically, but it is necessary to associate an exit program to an exit point. In other words, you must install (add) a program to a point, and the program (once installed) searches through the list of available exit rules to determine which rules should be applied.

To access the Network Security Configuration interface

1) Log into to TGSecure.

Note: The **TGSecure Main** menu appears.

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**.

Note: The **Network Security Configuration** interface is displayed.

See also:

Display List of Exit Points

Manage Exit Points

Run Exit Points Report

3.4.2. Display List of Exit Points

Use this task to display the list of exit points.

To display the list of exit points

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**.

Note: The **Network Security Configuration** interface is displayed.

Tip: Each row in the display represents an exit point. If ***YES** appears in the **Exit Inst?** column, that indicates that an exit program is installed at that exit point.

3.4.3. Manage Exit Points

Use this task to do the following with exit points.

- Display exit point details
- Enable exit point auditing
- Enable exit point security
- Enable exit point alerts
- Enable exit point incoming transaction collection
- Add an exit program to exit point
- Remove an exit program from an exit point
- Cycle (restart) a server
- Cycle multiple servers (mass update)
- Update all exit points (mass update)

To manage exit points, access the **Work with Network Security Configuration** interface.

To access the Work with Network Security Configuration

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**.

Note: The **Network Security Configuration** interface is displayed.

3.4.3.1. Display Exit Point Details

Use this task to display the details (definition) for a specific exit point. There is limited space in the **Network Security Configuration** interface, so not all the details associated with an exit point are displayed. Therefore, this task allows you to see the complete details for each exit point.

To display exit point details

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **5** (Display).
3) Press **Enter**.

Field	Description
Network Server	Name of the server type
Exit Point	Name assigned to the exit point
Exit Format	IBM format associated with the exit point
Exit Description	Description of the exit point
Exit Program Installed	Indicates whether the exit point is installed on the server

Field	Description
	Note: The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to ***YES**.
Function Usage Rule	Indicates whether an IBM function usage rule is being applied at the exit point. This indicator is important because it helps to identify conflicts between exit rules and function usage rules. If there is a conflict (e.g., an exit rule states to do one thing, but a function usage rule states to do something different), then the system might produce an unexpected outcome. ***YES** - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists ***NO** - No function usage rule is applied at the exit point ***NA** - Not applicable because IBM does not provide a function usage rule for this exit point
Audit Status	Indicates whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports ***YES** - Record incoming transaction data in the audit journal ***NO** - Do not record incoming transaction data in the audit journal **Tip**: If auditing is disabled at the module level, then this setting is ignored. In other words, if auditing is disabled at the network security (module) level, then auditing will not occur even if auditing is enable at the exit point (secondary) level. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable alerting at the secondary level if you want to record auditing data for a specific exit point. See Manage Network Security Defaults for information about enabling/disabling auditing globally.
Security Status	Indicates whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go in to effect. ***YES** - Apply exit rules (enable network security) ***NO** - Disable exit rules (disable network security)
Alert Status	Indicates whether alerts are enabled for a specific exit point. Alerts are required if you plan to send alert notifications ***ALL** - Record an alert for all (PASS and FAIL) connection attempts ***FAIL** - Record only FAIL connection attempts ***NONE** - Do not record alerts **Tip**: If alerts are disabled at the module level, then this setting is ignored. In other words, if alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enable at the exit point (secondary) level. The module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. See Manage Network Security Defaults for information about enabling/disabling alerting globally.
Smart Mode	Indicates whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules **Note**: The system administrator can delete rules created by the Rules Intelligence Engine at any time.

Field	Description
Collector Status	Indicates which incoming transactions you want to track (collect) in the **Incoming Transaction** interface ***ALL** - Collect and display all (PASS and FAIL) incoming transactions ***FAIL** - Collect and display only rejected (FAIL) incoming transactions ***NONE** - Do not collect or display any incoming transactions

3.4.3.2. Enable Exit Point Auditing

Use this task to enable auditing of incoming transactional data for a specific exit point. Auditing is required if you plan to run network security reports.

Prerequisite

Auditing must be enabled in the Network Security Module. See Manage Network Security Defaults.

To enable auditing for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Audit Status** field, enter ***YES**.
5) Press **Enter**.

3.4.3.3. Enable Exit Point Security

Use this task to enable security for a specific exit point. Once you enable security, the exit rules associated with the exit point go into effect.

Prerequisite

Create the exit rules you want to apply. See Manage Exit Rule.

Tip: Ensure that your rules provide the appropriate level of user access. If you fail to design your rules properly, you might block legitimate users from performing necessary work transactions.

To enable security for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Security Status** field, enter ***YES**.
5) Press **Enter**.

3.4.3.4. Enable Exit Point Alerts

Use this task to enable alerts for a specific exit point. Alerts are required if you plan to send alert notifications.

Prerequisite

Alerts must be enabled in the Network Security module, see Manage Network Security Defaults.

To enable alerts for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter one of the following:
– ***ALL** - Record an alert for all (PASS and FAIL) connection attempts
– ***FAIL** - Record only FAIL connection attempts
5) Press **Enter**.

3.4.3.5. Enable Exit Point Collection

Use this task to enable the collection of incoming transactions for a specific exit point in the **Incoming Transaction** interface.

To enable incoming transaction collection for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter one of the following:
– ***ALL** - Collect and display all (PASS and FAIL) incoming transactions
– ***FAIL** - Collect and display only rejected (FAIL) incoming transactions
5) Press **Enter**.

3.4.3.6. Add Exit Program to Exit Point

Use this task to add (install) an exit program to a single exit point. The system provides pre-built exit programs for each of the established IBM exit points. You have control of whether to add (install) a pre-built exit program to an exit point. The exit programs are what house the exit rules.

Note: It's not necessary to manually associate an exit rule to an exit program. That happens programmatically, but it is necessary to associate an exit program to an exit point. In other words, you must install (add) a program to a point, and the program (once installed) searches through the list of available exit rules to determine which rules should be applied.

To add exit program to exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired point, enter **11** (Add Exit Program).
3) Press **Enter**.

Note: Once an exit program is installed at an exit point, you will see ***YES** in the **Exit Inst?** column for the exit point.

3.4.3.7. Add Exit Programs to Exit Points (Mass Update)

Use this task to add (install) exit programs to multiple exit points.

Note: Once complete, you will see ***YES** in the **Exit Inst?** column for all modified exit points.

To add an exit programs to exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F20** (Add Exit Programs) function key.
3) Enter ***All** to add all exit points to an exit program, or enter a specific server type.
4) Press **Enter**.

3.4.3.8. Remove Exit Program from Exit Point

Use this task to remove exit program from single exit point.

Note: Once the exit program is uninstalled, you will see ***NO** in the **Exit Inst?** column for the modified exit point.

To remove an exit program from exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired point, enter **12** (Remove Exit Program).
3) Press **Enter**.

3.4.3.9. Remove Exit Programs from Exit Points (Mass Update)

Use this task to remove (uninstall) exit programs to multiple exit points.

Note: Once complete, you will see ***NO** in the **Exit Inst?** column for all modified exit points.

To remove an exit programs from exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F21** (Remove Exit Programs) function key.
3) Enter ***All** to remove all exit programs, or enter a specific server type.
4) Press **Enter**.

3.4.3.10. Cycle Server

Use this task to restart a single server. Cycling a server is useful when you add an exit program and you want to ensure that the exit rule(s) associated with that program are applied immediately (including to transactions currently running.) For example, there might be pre-start jobs that are running. In order for a new rule(s) to be applied to the pre-start jobs, the jobs must be stopped and restarted (cycled) for the new exit rule(s) to take effect.

To cycle a single server

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired point, enter **13** (Cycle Server).
3) Press **Enter**.
4) Ensure that the correct server is selected.
5) Enter one of the following options:

– **Y** - Initiate cycling immediately (run in interactive mode)
– **N** - Place cycling request in queue (run as part of a job queue)

6) Press **Enter**.

3.4.3.11. Cycle Servers (Mass Update)

Use this task to restart multiple servers.

To cycle multiple servers

1) Access the **Network Security Configuration** interface.
2) Press the **F19** (Cycle Servers) function key.

3) Enter ***All** to cycle all servers or identify a specific server type.
4) Enter **Y** to execute the cycling immediately or **N** to add it a batch.
5) Press **Enter**.

3.4.3.12. Update all Exit Points (Mass Update)

Use this task to perform a mass update of all exit points.

To update all exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F7** (Update all) function key.
3) Modify the setting as necessary.

Note: All editable settings are underlined.

Field	Description
Audit Status	Indicates whether auditing is enabled. Auditing is required if you plan to run network security reports. ***YES** - Record incoming transaction data in the audit journal for all installed exit points ***NO** - Do not record incoming transaction data in the audit journal for all installed exit points ***SAME** - Do not perform a mass update of the **Audit Status**. In other words, skip this setting. **Tip**: See Manage Network Security Defaults for information about enabling auditing globally. Global defaults take precedence over local settings.
Security Status	Indicates whether the exit rules associated with the exit point should be applied. ***YES** - Apply exit rules for all installed exit points ***NO** - Do not apply exit rules for all installed exit points ***SAME** - Do not perform a mass update of the **Security Status**. In other words, skip this setting during the mass update.
Alert Status	Indicates whether alerting is enabled. Alerting is required if you plan to send alert notifications. ***ALL** - Record an alert for all (PASS and FAIL) connection attempts ***FAIL** - Record only FAIL alerts for all installed exit points ***NONE** - Do not record alerts for all installed exit points ***SAME** - Do not perform a mass update of the **Alert Status**. In other words, skip this setting during the mass update. **Tip**: See Manage Network Security Defaults for information about enabling alerting globally. Global defaults take precedence over local settings.
Smart Mode	Indicates whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules ***SAME** - Do not perform a mass update of the **Smart Mode**. In other words, skip this setting during the mass update.
Collector Status	Indicates which incoming transactions are tracked (collect) in the **Incoming Transaction** interface.

Field	Description
	***ALL** - Collect and display all (PASS and FAIL) connection attempts ***FAIL** - Collect and display only FAIL connection attempts ***NONE** - Do not collect or display any connection attempts ***SAME** - Do not perform a mass update of the **Collector Status**. In other words, skip this setting during the mass update.

4) Press **Enter**.

3.4.4. Run Exit Points Report

Use this task to generate reports that display the following for exit points:

- Exit point configuration details
- Exit point configuration changes

3.4.4.1. Run Exit Point Configuration Report

Use this report to display exit point configuration details for exit points.

To run Exit Point Configuration 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 when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.4.4.2. Run Exit Point Configuration Changes Report

Use this report to display the list of configuration changes made to exit points.

To run Exit Point Configuration Change 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 when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

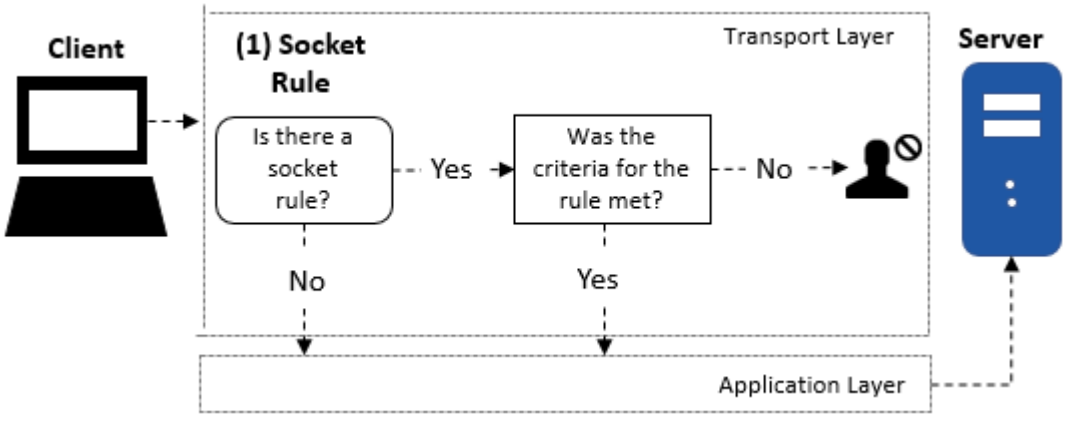
3.5. Socket Rules

3.5.1. Working with Socket Rules

This section describes working with socket rules. Socket rules allow you to address security risks associated with newer protocols (e.g., SFTP and SSH), which are not covered by exit rules at the application level. The newer protocols were designed to address weakness in older protocols (e.g., FTP, TELNET, ODBC, and SQL.) in which data was transmitted in clear text. While the newer protocols reduced some security risks, they opened the door to others. The newer protocols use socket communication at the transaction level, and in some cases might allow users to bypass security established using exit rules at the application level.

Example Usage:

A rule might be created to reject an incoming transaction (connection) to the server listening on a specific port or coming from a particular remote IP address after business hours (6pm - 6am).



To access the Work with Socket Rules interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**.

See also:

Log into TGSecure

Display List of Socket Rules

Manage Socket Rules

Run Socket Rules Report

3.5.2. Display List of Socket Rules

Use this task to do the following with socket rules:

- Display list of socket rules
- Sort socket rules
- Move to a specific location within list of socket rules
- Filter socket rules

3.5.2.1. Display List

Use this task to display the list of socket rules.

To display the list of socket rules

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** (Socket Rules).
5) Press **Enter**.

Note: The **Work with Socket Rules** interface is displayed.

3.5.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Socket Rules** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

3.5.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a network.

To move to a specific position within the list

1) Access the **Work with Socket Rules** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

3.5.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Socket Rules** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

3.5.3. Manage Socket Rules

Use this task to do the following with socket rules:

- Add a socket rule
- Edit a socket rule
- Copy a socket rule
- Delete a socket rule
- Display list of users in a group
- Display list of client networks
- Display list of server networks
- Display list of operations

To manage socket rules, access the **Work with Socket Rules** interface.

To access the Work with Socket Rules interface

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** (Socket Rules).
5) Press **Enter**.

Note: The **Work with Socket Rules** interface is displayed.

3.5.3.1. Add Socket Rule

Use this task to add a socket rule.

Tip: You can define a socket rule for an individual user, network, or operation, and you can define them for groups of users, networks, or operations.

To add a socket rule

1) Access the **Work with Socket Rules** interface.
2) Press the **F6** (Add) function key.
3) Define the rule using the fields provided.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**.

Note: At this point, you might receive suggestions from the system. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server) as well.

See also:

Rules Suggestion Engine
Rules Decision Engine
Manage User Groups
Manage Socket Rules
Manage Exit Rules

3.5.3.2. Edit Socket Rule

Use this task to edit an existing socket rule.

To edit a socket rule

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired rule, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

3.5.3.3. Copy Socket Rule

Use this task to create a new rule by copying a socket rule.

To copy a socket rule

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired rule, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

3.5.3.4. Delete Socket Rule

Use this task to delete a socket rule.

To delete a socket rule

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired transaction, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter**.

3.5.3.5. Display List of Users in a Group

Use this task when the **User Name** field contains a user group. You can access the user group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of users

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired rule, enter **6** (User Grp).
3) Press **Enter**.
4) Review the list of users.

Tip: You can modify the user group at this point as well.

3.5.3.6. Display List of Clients in a Group

Use this task when **Client IP** field contains a network group. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of clients

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired rule, enter **7** (Client Grp).
3) Press **Enter**.
4) Review the list of clients.

Tip: You can modify the network group at this point as well.

3.5.3.7. Display List of Servers in a Group

Use this task when the **Server Name** field contains a network group. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of servers

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired rule, enter **8** (Server Grp).

3) Press **Enter**.
4) Review the list of servers.

Tip: You can modify the network group at this point as well.

3.5.3.8. Display List of Operations in a Group

Use this task when the **Operation/Port** field contains an operation group. You can access the operation group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of operations

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired rule, enter **9** (Opr. Grp).
3) Press **Enter**.
4) Review the list of operations.

Tip: You can modify the operation group at this point as well.

3.5.4. Run Socket Rule Reports

Use this task to generate reports that display the following for socket rules.

- Socket rule configuration details
- Socket rule configuration changes

3.5.4.1. Run Socket Rule Configuration Report

Use this report to display socket rule configuration details.

To run Socket Rule 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.5.4.2. Run Socket Rule Configuration Changes Report

Use this report to display the list of configuration changes made to socket rules.

To run Socket Rule Configuration Changes 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 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 when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.6. Exit Rules

3.6.1. Working with Exit Rules

This section describes working with exit rules. Exit rules control network traffic associated with a specific application level communication protocol (i.e., FTP, TELNET, and ODB).

Example Usage:

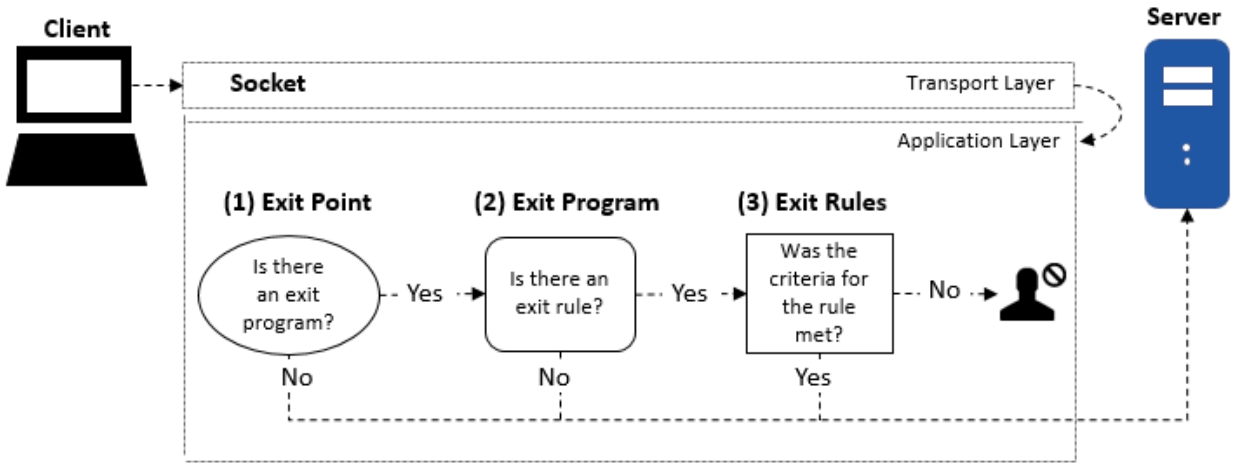
You might need a rule to reject all incoming transaction (connection) initiated by a specific user or member of a user group.

Client-Server Communication Process via transport layer:

(1) Exit Point: An exit point is a point in the network communication process between a client and a server where control is turned over to an exit program if an exit program exists.

(2) Exit Program: An exit programs can be created for each type of network communication (FTP, ODBC, JDBC, SQL, etc.). Exit programs control execution of transactions between a client and a server.

(3) Exit Rule: An exit rule defines the criteria by which an exit program determines whether a transaction is allowed or forbidden.



To access the Work with Exit Rules interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**.

See also:

Log into TGSecure

Display List of Exit Rules

Manage Exit Rules

Run Exit Rule Reports

3.6.2. Display List of Exit Rules

Use this task to do the following with exit rule:

- Display list of exit rules
- Sort exit rules
- Move to a specific location within list of exit rules
- Filter exit rules

3.6.2.1. Display List

Use this task to display the list of exit rules.

To display the list of exit rules

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 **3** (Remote Exit Rules).
5) Press **Enter**.

Note: The **Work with Exit Rules** interface is displayed.

3.6.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Exit Rules** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

3.6.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a network.

To move to a specific position within the list

1) Access the **Work with Exit Rules** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

3.6.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Exit Rules** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

3.6.3. Manage Exit Rules

Use this task to do the following with exit rule:

- Add an exit rule
- Edit an exit rule
- Copy an exit rule
- Delete an exit rule
- Display list of users
- Display list of client networks

- Display list of server networks
- Display list of operations
- Display list of objects

To manage exit rules, access the **Work with Exit Rules** interface.

To access the Work with Exit Rules interface

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 **3** (Remote Exit Rules).
5) Press **Enter**.

Note: The **Work with Exit Rules** interface is displayed.

3.6.3.1. Add Exit Rule

Use this task to add an exit rule.

To add an exit rule

1) Access the **Work with Exit Rules** interface.
2) Press the **F6** (Add) function key.
3) Define the rule using the fields provided.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**.

Note: At this point, you might receive suggestions from the system. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server), object groups, and operations groups as well.

See also:

Rules Suggestion Engine
Rules Decision Engine
Manage User Groups
Manage Socket Rules
Manage Exit Rules

3.6.3.2. Edit Exit Rule

Use this task to edit an existing exit rule.

To edit an exit rule

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

5) Press **Enter** twice.

3.6.3.3. Copy Exit Rule

Use this task to create a new rule by copying an existing rule.

To copy an exit rule

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

3.6.3.4. Delete Exit Rule

Use this task to delete an exit rule.

To delete an exit rule

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired transaction, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter**.

3.6.3.5. Display List of Users

Use this task when the exit rule definition includes a user group in the **User Name** field. You can access the user group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of users

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **6** (User Grp).
3) Press **Enter**.
4) Review the list of users.

See also:

- Manage Users
- Manage User Groups

3.6.3.6. Display List of Clients

Use this task when the exit rule definition includes a network group in the **Client IP** field. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of clients

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **7** (Client Grp).
3) Press **Enter**.
4) Review the list of clients.

See also:

- Manage Networks
- Manage Network Groups

3.6.3.7. Display List of Servers

Use this task when the exit rule definition includes a network group in the **Server Name** field. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of servers

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **8** (Server Grp).
3) Press **Enter**.
4) Review the list of servers.

See also:

- Manage Networks
- Manage Network Groups

3.6.3.8. Display List of Operations

Use this task when the exit rule definition includes an operation group in the **Operation/Port** field. You can access the operation group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of operations

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **9** (Opr. Grp).
3) Press **Enter**.
4) Review the list of operations.

See also:

- Manage Operations
- Manage Operation Groups

3.6.3.9. Display List of Objects

Use this task when the exit rule definition includes an object group in the **Object Details** field. You can access the object group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of objects

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired rule, enter **10** (Obj. Grp).
3) Press **Enter**.
4) Review the list of operations.

See also:

- Manage Objects
- Manage Object Groups

3.6.4. Run Exit Rule Reports

Use this task to generate reports that display the following for exit rules:

- Exit rule configuration details
- Exit rule configuration changes

3.6.4.1. Run Exit Rule Configuration Report

Use this report to display exit point configuration details.

To run the Exit Rule Configuration 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.6.4.2. Run Exit Rule Configuration Changes Report

Use this report to display the list of configuration changes made to exit rules.

To run the Exit Point Configuration Changes 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

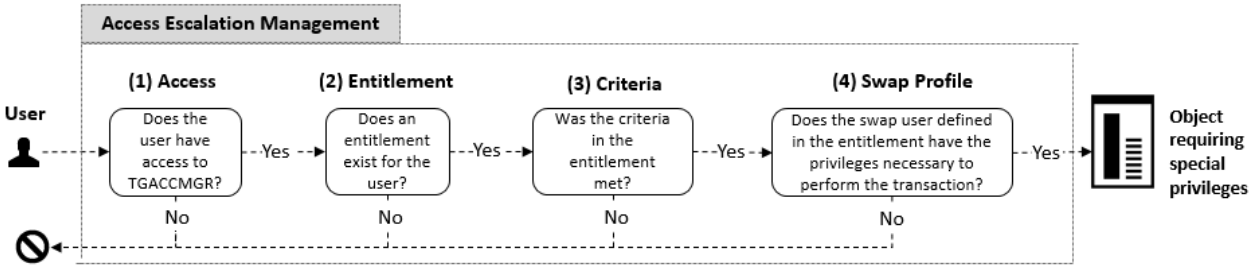
Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4. Access Escalation Management

Security threats are not exclusive to rogue users attempting to access your network from outside sources. Threats can also arise from within (unintentional or intentional). For example, you might have a user who is granted more access than necessary and that user might unintentionally perform a transaction that has negative system-wide implications. One way to reduce internal threats is to ensure that your users have appropriate, role-based access, but situations might arise that require a user to perform a task that is outside of his/her access authority. To address such cases, you can create an entitlement, which the user can execute within the Access Escalation Management (AEM) interface. An entitlement allows a user to perform a specific task (as defined by the entitlement) using the privileges of a swap user (as defined by the entitlement).



4.1.1. Working with Access Escalation Management

This section describes tasks associated with ensuring your system is secure from inside threats (those user with access to your server).

To access the Access Escalation Management interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Access Escalation Management).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4.2. Access Escalation Defaults

4.2.1. Working with Access Escalation Management Defaults

This section describes working with Access Escalation Management (AEM) defaults. These defaults apply to all entitlements unless otherwise defined.

Access escalation defaults define the following:

- Default swap user
- Session timeout
- Journal in which to store access control changes
- Library in which to store access control changes
- Whether to enable auditing of access control changes
- Queue in which to store alerts
- Queue library in which to store alerts

To access the Work with Access Escalation interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

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**.

Note: The **Work with Access Escalation** interface is displayed.

See also:

Log into TGSecure

Display Access Escalation Defaults

Manage Access Escalation

4.2.2. Display Access Escalation Defaults

Use this task to see the default parameters set for access escalation. These defaults apply to all entitlements unless otherwise define.

To display access escalation defaults

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**.

Note: The **Work with Access Escalation** interface is displayed.

4.2.3. Manage Access Escalation

Use this task to do the following:

- Modify access management defaults
- Enable access management auditing, which is required for reporting

To manage access escalation, access the **Work with Access Escalation** interface.

To access the Work with Access Escalation interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.

Note: The **Work with Access Escalation** interface is displayed.

4.2.3.1. Modify Access Defaults

Use this task to modify the exiting access escalation defaults. These defaults determine the following:

- Which journal to monitor
- Where to store the alerts
- Whether to collect data about access escalation changes (This flag must be set to **Y** to if you plan to run change reports.)

To modify access defaults

1) Access the **Work with Access Escalation** interface.
2) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of valid options.

3) Press **Enter** twice.

4.2.3.2. Enable Access Change Reporting

Use this task to enable reporting (start collecting auditing data) for the system elements involved in controlling system access (e.g., groups).

To enable access change reporting

1) Access the **Work with Access Escalation** interface.
2) In the **Audit Configuration Changes** field, ensure the flag is set to **Y** (Yes).
3) Press **Enter** twice.

4.2.4. Run Access Escalation Reports

Use this task to generate access escalation reports.

To run Access Escalation Reports

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

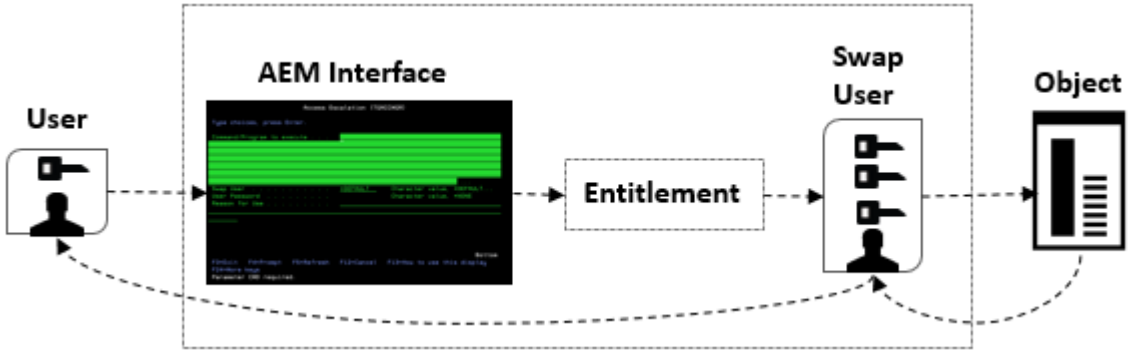
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) Choose the desired report category from the list.
– Usage Reports
– Configuration Reports
– Change Reports
7) Press **Enter**.
8) Choose the desired report from the list.
9) Press **Enter**.

4.3. Entitlements

4.3.1. Working with Entitlements

This section describes working with entitlements. Entitlements allow a user to borrow the access rights of a higher-privileged user (swap user) temporarily to execute an activity on an object.

Tip: A user can execute entitlements only from within the Access Escalation Management (AEM) interface. The system administrator can limit who has access to the AEM interface, which provides an additional layer of security.



Usage Example: Say your company has a day-shift and a night-shift administrator. In this scenario, the night administrator's only high-level task is creating a daily system backup. Instead of granting the night-shift administrator the same privileges as the day-shift administrator, you could create an entitlement that allows the night-shift administrator to perform the evening backup. In other words, this entitlement allows you to implement a privilege model that reduces your security exposure.

To access the Work with Entitlements interface

1) Log into to TGSecure.
Note: The **Main** menu appears.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with Entitlements).
5) Press **Enter**.

Note: The **Work with Entitlements** interface is displayed.

To access the AEM interface

1) At the **Selection or command** prompt, enter **TGACCMGR**.
2) Press **Enter**.

Note: The **AEM** interface is displayed.

See also:

Log into TGSecure

Display List of Entitlements

Manage Entitlements

Run Entitlement Reports

Executing a Task using an Entitlements

4.3.2. Display List of Entitlements

Use this task to do the following with entitlements:

- Display list of entitlements
- Sort entitlements
- Move to a specific location within list of entitlements
- Filter entitlements

4.3.2.1. Display List

Use this task to display the list of incoming transactions.

To display the list of incoming transactions

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 **1** (Work with Entitlements).
5) Press **Enter**.

Note: The **Work with Entitlements** interface is displayed.

4.3.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Entitlements** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

4.3.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Entitlements** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

4.3.2.4. Filter List

Use this task to limit the entitlement displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Entitlements** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

4.3.3. Manage Entitlements

Use this task to do the following with entitlements:

- Add entitlements
- Edit entitlements
- Copy entitlements
- Delete entitlements

To manage entitlements, access the **Work with Entitlements** interface.

To access the Work with Entitlements interface

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 **1** (Work with Entitlements).
5) Press **Enter**.

Note: The **Work with Entitlements** interface is displayed.

4.3.3.1. Add Entitlement

Use this task to add an entitlement. The entitlement parameters (e.g., object, library, server, etc.) you define allow you to control the access-level for a user or a use group at a granular level.

To add entitlement

1) Access the **Work with Entitlement** interface.
2) Press the **F6** (Add) function key.
3) Enter the parameters necessary to define the entitlement.

Note: Most parameters require a name. If you see a + sign next to the field, you may enter a group. Press **F4** (Prompt) for a list available groups.

Tip: Press **F1** (Help) to access field descriptions.

Field	Description
User Name	User or user group to which the entitlement applies
Object Name	Object or object group to which the entitlement applies
Object Library	Library in which the object impacted by the entitlement resides -- Program *PGM -- Command *CMD -- Database File *FILE
Swap User	Swap profile whose privileges will be used to execute the entitlement
Server Name	Server or server group from which the user must be accessing the system
Calendar	Calendar to be applied
Enable Status	Flag indicating whether the entitlement is enabled or disabled
Authentication	Flag indicating whether as user must enter a password (authenticate) in order to use the entitlement
Alerting	Flag indicating whether an alert is sent to the alert queue when an attempt is made to use the entitlement
Entitlement Description	Short description identifying the purpose of the entitlement

4) Press **Enter** twice.

4.3.3.2. Edit Entitlement

Use this task to edit an entitlement.

To edit entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of available groups.

5) Press **Enter** twice.

4.3.3.3. Copy Entitlement

Use this task to copy an entitlement. This is a fast way to create a new entitlement based on an existing entitlement.

To copy entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of available groups.

5) Press **Enter**.

4.3.3.4. Delete Entitlement

Use this task to delete an entitlement.

To delete entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct entitlement.
5) Press **Enter**.

4.3.4. Run Entitlement Reports

Use this task to generate reports that display the following for entitlements:

- Entitlement usage details
- Entitlement configuration details
- Entitlement configuration changes

4.3.4.1. Run Entitlement Usage Report

Use this report to display entitlement usages details.

To run Entitlement Usage 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.3.4.2. Entitlement Configuration Report

Use this report to display entitlement configuration details.

To run Entitlement Configuration 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** (Entitlements).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.3.4.3. Entitlement Configuration Changes Report

Use this report to display the list of configuration changes made to exit rules.

To run Entitlement Configuration Changes 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 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 when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

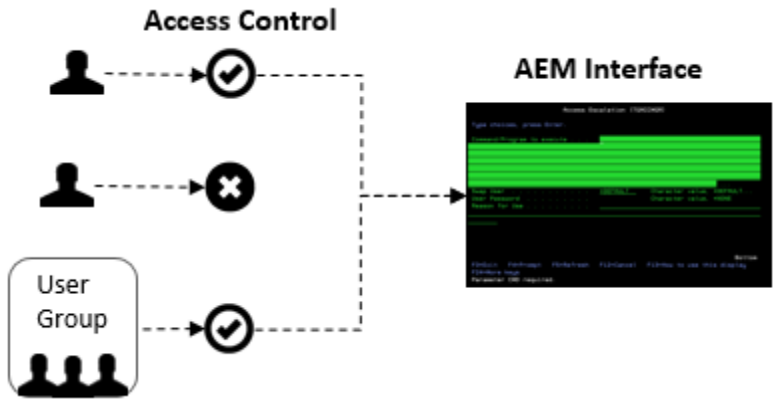
4.4. Access Control

4.4.1. Working with Access Control

This section describes how to grant or revoke access to the Access Escalation Management (AEM) interface. The AEM interface is the tool from which a user can execute an entitlement.

The tasks described in this section apply to both users and user groups.

Tip: Until the administrator adds the first user (or user group), all users have access to the AEM interface. Once the first user is explicitly granted access, then only the administrator and the user(s) who have been granted access control can access the AEM interface.



To access the Work with Access Control interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Access Control).
5) Press **Enter**.

Note: The **Work with Access Control** interface is displayed.

See also:

Log into TGSecure

Display Who Has Access Control

Manage Access Control

Run Access Control Reports

Execute and Entitlement Using the AEM Interface

4.4.2. Display Who Has Access to the AEM Interface

Use this task to do the following with the Access Escalation Management (AEM) interface:

- Display list of users who have authority to use the AEM interface
- Sort users

- Move to a specific position within list of users
- Filter users

4.4.2.1. Display List

Use this task to display the list of users (including user groups).

To display the list of users who have access control

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Access Control).
5) Press **Enter**.

Note: The **Work with Access Control** interface is displayed.

4.4.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Access Control** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

4.4.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Access Control** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

4.4.2.4. Filter List

Use this task to limit the entitlement displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Access Control** interface.
2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset. Type topic text here.

4.4.3. Manage Access Control

Use this task to do the following:

- Add access control
- Edit access control
- Copy access control
- Delete access control

To manage access control, access the **Work with Access Control** interface.

To access the Work with Access Control interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Access Control).
5) Press **Enter**.

Note: The **Work with Access Control** interface is displayed.

4.4.3.1. Add Access Control

Use this task to add access control for a user/user group. Once added, they are granted access to the AEM interface.

Tip: Until the first user is added, all users can access the AEM interface. Once the first user is added, only an administrator and the user(s) who have been granted access control (added) can access the AEM interface.

1) Access the **Work with Access Control** interface.
2) Press the **F6** (Add) function key.
3) Enter the user/user group.

Note: Press **F4** (Prompt) for a list available groups.

Tip: Press **F1** (Help) to access field descriptions.

4) Enter the Client IP from which the user/user group is allowed to access the server.
5) Press **Enter** twice.

4.4.3.2. Edit Access Control

Use this task to modify an exiting access control record.

To edit entitlement

1) Access the **Work with Access Control** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of valid entries.

5) Press **Enter** twice.

4.4.3.3. Copy Access Control

Use this task to create a new access control record based on an existing access control record.

To copy access control

1) Access the **Work with Access Control** interface.
2) In the **OPT** column for the user control record you want to copy, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of valid entries.

5) Press **Enter**.

4.4.3.4. Delete Access Control

Use this task to delete an access control record.

To delete entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the right user.
5) Press **Enter**.

4.4.4. Run Access Control Reports

Use this task to generate reports that display the following for the Access Escalation Management (AEM) interface.

- Access control configuration details
- Access control configuration changes

4.4.4.1. Run Access Control Configuration Report

Use this report to display the users who have access to the AEM interface.

To Access Control Configuration 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 Controls).

9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.4.4.2. Access Control Change Report

Use this report to display the list of configuration changes made to access control. In other words, which users have been added or delete.

To run Access Control Change 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** (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 when you generate it.

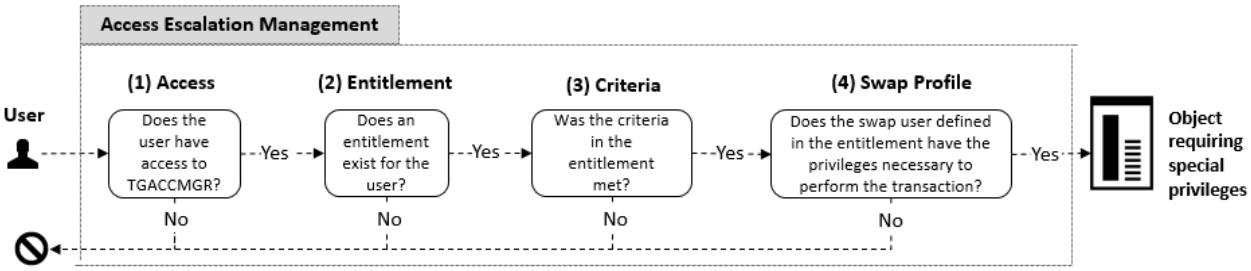
Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.4.5. Execute an Entitlement Using the AEM Interface

Use this task to access the Access Escalation Management (AEM) interface and execute an entitlement (which allows the users to borrow the privileges of a swap profile).
The following requirements must be met for a user to access the AEM interface and execute a task (e.g., download a highly sensitive HR document) using a swap profile:
Requirement 1: The user must have access to the AEM interface.
Requirement 2: An entitlement must be defined for the user.
Requirement 3: The criteria in the entitlement must be met.
Requirement 4: A user with appropriate privileges to perform the task must be identified as the swap user within the entitlement.



Tip: If you are unable to access the AEM interface, contact your system administrator and request that an access control record be added for your user profile.

To access the AEM interface

1) At the **Selection or command** prompt, enter **TGACCMGR**.
2) Press **Enter**.
3) Enter the program/command you want to execute.
4) Enter the appropriate swap profile.

Note: This is the user who has the privilege to perform the command/program you are attempting to execute.

5) Enter your user password (for some entitlements this is optional).
6) Enter a description for why you are performing this task.
7) Press **Enter**.

4.5. File Editor

4.5.1. Working with File Editor

This section describes working with the File Editor tool. The file editors are third-party commands used to modify files (objects). These commands might be used in conjunction with the standard IBM iSeries commands or they might be used as replacement commands. In any case, the third-party commands you plan to use must be registered using the File Editor tool in order for TG products to recognize those commands.

Usage Example: Your company might have purchased a third-party DFU (data file utility). Most, but not all, IBM clients use the standard IBM DFU. TG products recognize all standards IBM i Series commands. If your company plans to use third-party commands, you must use the File Editor tool to register those third-party commands so that they are recognized and executed properly by TG products.

To access the Work with File Editors interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Work with File Editors).
5) Press **Enter**.

Note: The **Work with File Editors** interface is displayed.

See also:

Log into TGSecure

Display List of File Editors

Manage File Editors

Run File Editor Reports

4.5.2. Display List of File Editors

Use this task to display a list of third-party file editors.

To display the list of File Editors

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 **11** (Work with File Editors).
5) Press **Enter**.

Note: The **Work with File Editors** interface is displayed.

4.5.3. Manage File Editors

Use these tasks to do the following with file editors:

- Add file editor
- Edit file editor
- Copy file editor
- Delete file editor

To access the Work with File Editors interface

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 **11** (Work with File Editors).
5) Press **Enter**.

Note: The **Work with File Editors** interface is displayed.

4.5.3.1. Add File Editor

Use this task to add a file editor.

To add file editor

1) Access the **Work with File Editors** interface.
2) Press the **F6** (Add) function key.
3) Enter the parameters necessary to define the file editor.

Tip: Press **F1** (Help) to access field descriptions.

4) Enter a description for the file editor.
5) Press **Enter** twice.

4.5.3.2. Edit File Editor

Use this task to edit a file editor.

To edit file editor

1) Access the **Work with File Editor** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

4.5.3.3. Copy File Editor

Use this task to copy a file editor. This is a fast way to reference a new file editor based on an existing file editor record.

To copy file editor

1) Access the **Work with File Editor** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter**.

4.5.3.4. Delete File Editor

Use this task to delete a file editor.

To delete file editor

1) Access the **Work with File Editor** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct file editor.
5) Press **Enter**.

4.5.4. Run File Editor Reports

Use these tasks to generate reports that display the following for file editors.

- File editor configuration details
- File editor configuration changes

4.5.4.1. Run File Editors Configuration Report

Use this task to display file editor configuration details.

To run File Editor 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.5.4.2. Run File Editor Change Report

Use this task to display the list of configuration changes made to file editors.

To run File Editor Change 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 Editors Changes).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

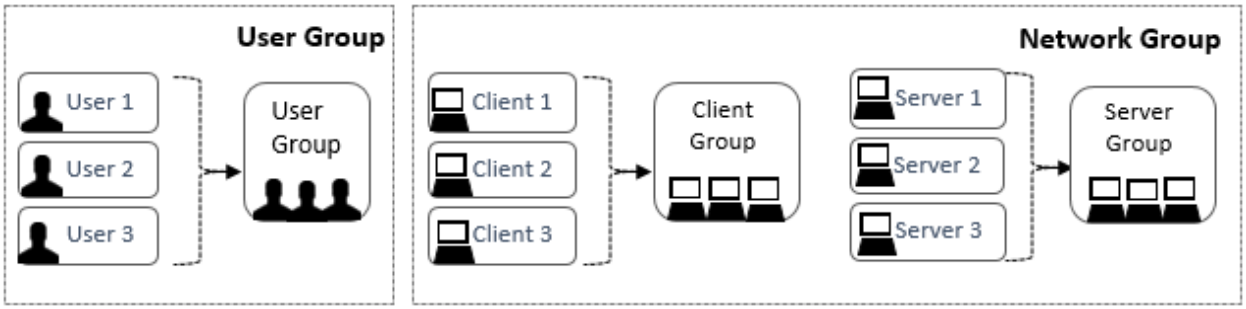
Note: The status of the report is displayed at the bottom of the screen.

5. Groups

5.1. Working with Groups

There are several types of groups that you can create.

- User
- Network
- Operation
- Object



To access the Work with Groups interface

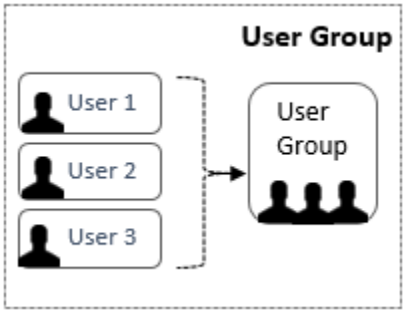
1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.

Note: The **Work with Groups** interface is displayed.

5.2. Users

5.2.1. Working with User

This section describes what you need to know about users and user groups.



To work with user groups, you must access the **Work with User Groups** interface.

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

See also:

Display List of User Groups

Display List of Users

Manage User Groups

Manage Users

Run User Groups Report

5.2.2. Display List of User Groups

Use this task to do the following with user groups:

- Display the list of user groups
- Sort the list of user groups
- Move to a specific location within the list of user groups
- Filter the list user groups

5.2.2.1. Display List

Use this task to display the list of user groups.

To display the list of user groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

5.2.2.2. Sort List

Use this task to sort the list of available networks. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with User Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.2.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with User Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.2.2.4. Filter List

Use this task to limit the user groups displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with User Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

5.2.3. Display List of Users in a Group

Use this task to do the following with user groups:

- Display the list of users within a group
- Sort the list of users within a group
- Move to a specific location within the list of users

5.2.3.1. Display List

Use this task to display the list of users assigned to a user group.

To display the list of users assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Users).
7) Press **Enter**.

Note: The **Work with Users** interface is displayed.

5.2.3.2. Sort List

Use this task to sort the list of available users.

To sort the list

1) Access the **Work with Users** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.2.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Users** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.2.4. Manage User Groups

Use this task to do the following with user groups:

- Add user groups
- Edit user groups
- Delete user groups

To manage user groups, access the **Work with User Groups** interface.

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

5.2.4.1. Add User Group

Use this task to add a user group.

To add user group

1) Access the **Work with User Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

5.2.4.2. Edit User Group

Use this task to edit a user group.

To edit user group

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.

Note: You cannot edit the name.

5) Press **Enter** twice.

5.2.4.3. Delete User Group

Use this task to delete a user group

To delete user group

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

5.2.5. Manage Users Within a Group

Use this task to do the following with user groups:

- Add users
- Edit users
- Delete users

To manage users, access the **Work with Users** interface.

To access the Work with Users interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.
6) In the **OPT** column of the user group you want to manage, enter **10** (Work with Users).
7) Press **Enter**.

Note: The **Work with Users** interface is displayed.

5.2.5.1. Add a User

Use this task to add a user.

To add user

1) Access the **Work with Users** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the user.

Tip: Names cannot contain spaces.

4) Enter a description for the user.
5) Press **Enter** twice.

Note: If the user already exists, you will see a ***YES** in the **Exists on Server** field the first time you press **Enter**. If the user does not exist, you will see ***No** in the **Exists on Server** field the first time you press **Enter**.

5.2.5.2. Edit a User

Use this task to edit a user.

Note: You can only edit the user description, not the user name.

To edit user

1) Access the **Work with Users** interface.
2) In the **OPT** column for the desired user, enter **2** (Edit).
3) Press **Enter**.
4) Modify the user description as necessary.

Note: You cannot edit the user name.

5) Press **Enter** twice.

5.2.5.3. Delete a User

Use this task to delete a user.

To delete user

1) Access the **Work with Users** interface.
2) In the **OPT** column for the desired user, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct user.
5) Press **Enter** twice.

5.2.6. Run User Groups Report

Use this task to generate reports that display the following for user groups.

- User group configuration details
- User group configuration changes

5.2.6.1. Run User Group Configuration Report

Use this task to display user group configuration details.

To run User Group Configuration 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.2.6.2. Run User Group Configuration Changes Report

Use this task to display the list of configuration changes made to user groups.

To run User Group Configuration Changes 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

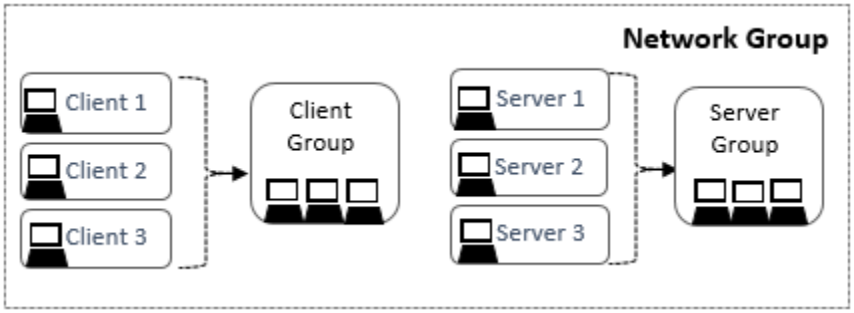
11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.3. Networks

5.3.1. Working with Networks

This section describes how to work with networks and network groups.



To work with network groups, you must access the **Work with Network/Server Groups** interface.

To access the Work with Network/Server Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.

Note: The **Work with Network/Server Groups** interface displays.

See also:

Display List of Network/Server Groups

Display List of Networks

Manage Network Groups

Manage Networks

Run Network Groups Report

5.3.2. Display List of Network Groups

Use this task to do the following with network groups:

- Display the list of network groups
- Sort the list of network groups
- Move to a specific location within the list of network groups
- Filter the list of network groups

5.3.2.1. Display List

Use this task to display the list of network groups.

To display the list of network groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.

Note: The **Work with Network/Server Groups** interface displays.

5.3.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Network Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.3.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Network Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.3.2.4. Filter List

Use this task to limit the network groups displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Network Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

5.3.3. Display List of Networks in a Group

Use this task to do the following with network groups:

- Display the list of networks within a group
- Sort the list of networks within a group
- Move to a specific location within the list of networks

5.3.3.1. Display List

Use this task to display the list of networks assigned to a network group.

To display the list of networks assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Networks).
7) Press **Enter**.

Note: The **Work with Networks** interface is displayed.

5.3.3.2. Sort List

Use this task to sort the list of available networks.

To sort the list

1) Access the **Work with Networks** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.3.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Networks** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.3.4. Manage Network Groups

Use this task to do the following with network groups:

- Add network groups
- Edit networks groups
- Copy network groups
- Delete network groups

To manage network groups, access the **Work with Network Groups** interface.

To access the Work with Network Groups interface

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 **4** (Work with Groups).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
7) Press **Enter**.

Note: The **Work with Network Groups** interface is displayed.

5.3.4.1. Add Network Group

Use this task to add a network group.

To add network group

1) Access the **Work with Network Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign the network group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the network group.
5) Press **Enter** twice.

5.3.4.2. Edit Network Group

Use this task to edit a network group.

To edit network group

1) Access the **Work with Network Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

5.3.4.3. Copy Network Group

Use this task to copy a network group. This is a fast way to create a new group based on an existing group.

To copy network group

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

5) Enter a description for the group.
6) Press **Enter**.

5.3.4.4. Delete Network Group

Use this task to delete a network group

To delete network group

1) Access the **Work with Network Group** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

5.3.5. Manage Networks Within a Group

Use this task to do the following with network groups:

- Add networks
- Edit networks
- Delete networks

To manage networks, access the **Work with Networks** interface.

To access the Work with Networks interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.
6) In the **OPT** column of the network group you want to manage, enter **10** (Work with Networks)
7) Press **Enter**.

Note: The **Work with Networks** interface is displayed.

5.3.5.1. Add Network

Use this task to add a network.

To add network

1) Access the **Work with Networks** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the network.

Tip: Names cannot contain spaces.

4) Enter a description for the network.
5) Press **Enter** twice.

5.3.5.2. Edit Network

Use this task to edit a network.

To edit network

1) Access the **Work with Networks** interface.
2) In the **OPT** column for the desired network, enter **2** (Edit).
3) Press **Enter**.
4) Modify the network parameters as necessary.

Note: You cannot edit the network name.

5) Press **Enter** twice.

5.3.5.3. Delete Network

Use this task to delete a network.

To delete network

1) Access the **Work with Networks** interface.
2) In the **OPT** column for the desired network, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct network.
5) Press **Enter** twice.

5.3.6. Run Network Groups Report

Use this task to run a report that displays the list of network groups.

- Network group configuration details
- Network group configuration changes

5.3.6.1. Run Network Group Configuration Report

Use this task to display user group configuration details.

To run Network Group Configuration 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.3.6.2. Run Network Group Configuration Changes Report

Use this task to display the list of configuration changes made to network groups.

To run Network Group Configuration Changes 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

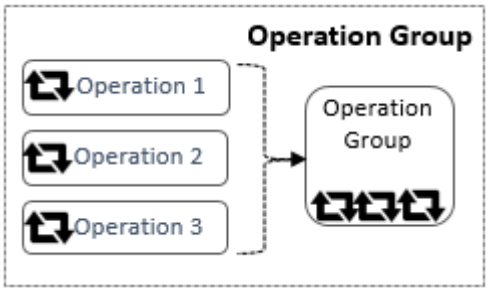
11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.4. Operations

5.4.1. Working with Operations

This section describes how to work with operations and operation groups.



To work with operations, you must access the **Work with Operation Groups** interface.

To access the Work with Operation Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.

Note: The **Work with Operation Groups** interface displays.

See also:

Display List of Operation Groups

Display List of Operations

Manage Operation Groups

Manage Operations

Run Operation Groups Report

5.4.2. Display List of Operation Groups

Use this task to do the following with operation groups:

- Display the list of operations within a group
- Sort the list of operations within a group
- Move to a specific location within the list of operations
- Filter the list of operations within a group

5.4.2.1. Display List

Use this task to display the list of operation groups.

To display the list of operation groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.

Note: The **Work with Operation Groups** interface displays.

5.4.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Operation Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.4.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Operation Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.4.2.4. Filter List

Use this task to limit the operation groups displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Operation Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

5.4.3. Display List of Operations in a Group

Use this task to do the following with operation groups:

- Display the list of operations within a group
- Sort the list of operations within a group
- Move to a specific location within the list of operations

5.4.3.1. Display List

Use this task to display the list of operations assigned to an operations group.

To display the list of operations assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Operations).
7) Press **Enter**.

Note: The **Work with Operations** interface is displayed.

5.4.3.2. Sort List

Use this task to sort the list of available operations.

To sort the list

1) Access the **Work with Operations** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.4.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Operations** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.4.4. Manage Operation Groups

Use this task to do the following with operation groups:

- Add operation groups
- Edit operation groups
- Copy operation groups
- Delete operation groups

To manage operation groups, access the **Work with Operation Groups** interface.

To access the Work with Operation Groups interface

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 **4** (Work with Groups).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
7) Press **Enter**.

Note: The **Work with Operation Groups** interface is displayed.

5.4.4.1. Add Operation Group

Use this task to add an operation group.

To add operation group

1) Access the **Work with Operation Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

5.4.4.2. Edit Operation Group

Use this task to edit an operation group.

To edit operation group

1) Access the **Work with Operation Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

5.4.4.3. Copy Operation Group

Use this task to copy an operation group. This is a fast way to create a new group based on an existing group.

To copy network group

1) Access the **Work with Operation Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

5) Enter a description for the group.
6) Press **Enter**.

5.4.4.4. Delete Operation Group

Use this task to delete an operation group.

To delete operation group

1) Access the **Work with Operation Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

5.4.5. Manage Operations Within a Group

Use this task to do the following with operation groups:

- Add operations
- Edit operations
- Delete operations

To manage operations, access the **Work with Operations** interface.

To access the Work with Operations interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Operations).
7) Press **Enter**.

Note: The **Work with Operations** interface is displayed.

5.4.5.1. Add Operation

Use this task to add an operation.

To add operation

1) Access the **Work with Operations** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the operation.

Tip: Names cannot contain spaces.

4) Enter a description for the operation.
5) Press **Enter** twice.

5.4.5.2. Edit Operation

Use this task to edit an operation.

To edit operation

1) Access the **Work with Operations** interface.
2) In the **OPT** column for the desired operation, enter **2** (Edit).
3) Press **Enter**.
4) Modify the operation parameters as necessary.

Note: You cannot edit the name.

5) Press **Enter** twice.

5.4.5.3. Delete Operation

Use this task to delete an operation.

To delete an operation

1) Access the **Work with Operations** interface.

2) In the **OPT** column for the desired operation, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct operation.
5) Press **Enter** twice.

5.4.6. Run Operation Groups Report

Use this task to run a report that displays the list of operation groups.

- Operation group configuration details
- Operation group configuration changes

5.4.6.1. Run Operation Groups Configuration Report

Use this task to display operation group configuration details.

To run Operation Group Configuration 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 **6** (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 when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.4.6.2. Run Operation Group Configuration Changes Report

Use this task to display the list of configuration changes made to operation groups.

To run Operation Group Configuration Changes 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

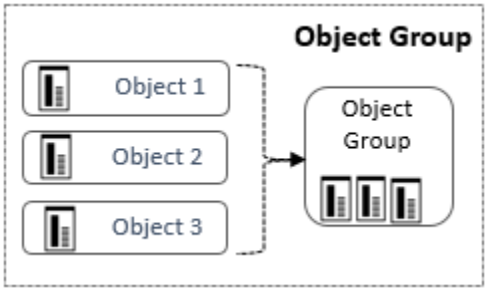
11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.5. Objects

5.5.1. Working with Objects

This section describes what you need to know about objects and object groups.



To work with object groups, you must access the **Work with Object Groups** interface.

To access the Work with Object Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.

Note: The **Work with Object Groups** interface is displayed.

See also:

Display List of Object Groups

Display List of Objects

Manage Object Groups

Manage Objects

Run Object Groups Report

5.5.2. Display List of Object Groups

Use this task to do the following with object groups:

- Display the list objects within a group
- Sort the list of objects within a group
- Move to a specific location within the list of objects

- Filter the list of objects within a group

5.5.2.1. Display List

Use this task to display the list of object groups.

To display the list of object groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.

Note: The **Work with Object Groups** interface is displayed.

5.5.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Object Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.5.2.3. Move to a Position in the List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Object Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.5.2.4. Filter List

Use this task to limit the object groups displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Object Groups** interface.
2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

5.5.3. Display a List of Object in a Group

Use this task to do the following with object groups:

- Display the list of objects within a group
- Sort the list of objects within a group
- Move to a specific location within the list of objects

5.5.3.1. Display List

Use this task to display the list of operations assigned to an operations group.

To display the list of operations assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Objects).
7) Press **Enter**.

Note: The **Work with Objects** interface is displayed.

5.5.3.2. Sort List

Use this task to sort the list of available objects.

To sort the list

1) Access the **Work with Objects** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.5.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Operations** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.5.4. Manage Object Groups

Use this task to do the following with object groups:

- Add objects groups
- Edit objects groups
- Copy object groups
- Delete object groups

To manage object groups, access the **Work with Object Groups** interface.

To access the Work with Object Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.

Note: The **Work with Object Groups** interface is displayed.

5.5.4.1. Add Object Group

Use this task to add an object group.

To add object group

1) Access the **Work with Object Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

5.5.4.2. Edit Object Group

Use this task to edit an object group.

To edit object group

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

5.5.4.3. Copy Object Group

Use this task to copy an object group. This is a fast way to create a new group based on an existing group.

To copy object group

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

5) Enter a description for the group.
6) Press **Enter**.

5.5.4.4. Delete Object Group

Use this task to delete an object group

To delete object group

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

5.5.5. Manage Objects Within a Group

Use this task to do the following with object groups:

- Add object
- Edit object
- Delete object

To manage objects, access the **Work with Objects** interface.

To access the Work with Objects interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Objects).
7) Press **Enter**.

Note: The **Work with Objects** interface is displayed.

5.5.5.1. Add Object

Use this task to add an object.

To add operation

1) Access the **Work with Objects** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the object.

Tip: Names cannot contain spaces.

4) Enter a description for the object.
5) Press **Enter** twice.

5.5.5.2. Edit Object

Use this task to edit an object.

To edit object

1) Access the **Work with Objects** interface.
2) In the **OPT** column for the desired object, enter **2** (Edit).
3) Press **Enter**.
4) Modify the object parameters as necessary.

Note: You cannot edit the name.

5) Press **Enter** twice.

5.5.5.3. Delete Object

Use this task to delete an object.

To delete an object

1) Access the **Work with Objects** interface.
2) In the **OPT** column for the desired operation, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct object.
5) Press **Enter** twice.

5.5.6. Run Object Groups Report

Use this task to run a report that displays the list of object groups.

- Object group configuration details
- Object group configuration changes

5.5.6.1. Run Object Group Configuration Report

Use this task to display operation group configuration details.

To run Object Group Configuration 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.5.6.2. Run Object Group Configuration Changes Report

Use this task to display the list of configuration changes made to object groups.

To run Object Groups Configuration Changes 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**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

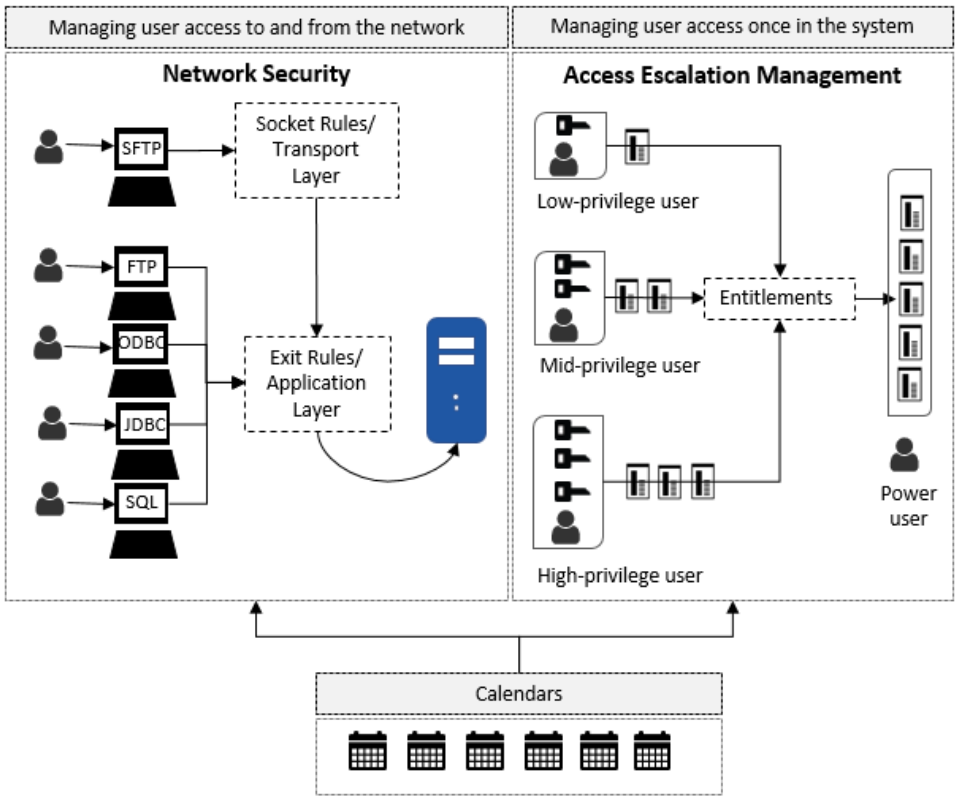
11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6. Calendars

6.1. Working with Calendars

This section describes how to work with calendars. Calendars allow you to enable a rule or entitlement for a specific duration (e.g., after hours, during weekends, on a holiday, etc.).



To work with calendars, you must access the **Work with Calendar Interface**.

To access the Work with Calendar interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

See also:

Display List of Calendars

Manage Calendars

Manage Day/Time Access

6.2. Display List of Calendars

Use this task to do the following with calendars:

- Display the list of calendars
- Sort the list of calendars
- Move to a specific location within the list of calendars
- Filter the list of calendars

6.2.1. Display List

Use this task to display the list of calendars.

To display the list of calendars

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

6.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Calendar** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Calendar** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

6.2.3. Move to a Position in the List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Calendar** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

6.2.4. Filter List

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Calendar** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

6.3. Manage Calendars

Use this task to do the following with calendars:

- Display calendar duration details
- Display calendar day/time access details
- Edit calendar duration details
- Edit calendar day/time access details
- Add calendar
- Copy calendar
- Delete calendar

To manage calendars, access the **Work with Calendar** interface.

To access the Work with Calendar interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

6.3.1. Display Calendar Duration Details

Use this task to display the calendar duration details. The duration details identify the period for which a calendar is valid. For example, you could create a calendar to enable a rule or entitlement to be valid only during the month of December in the calendar year 2020.

To display the calendar duration details

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **5** (Display).
3) Press **Enter**.
4) Review the duration details for the selected calendar.

6.3.2. Display Calendar Day/Time Access Details

Use this task to display the calendar day/time access details. The day/time access details identify the days of the week and specific time for which the calendar is valid. For example, you could create a calendar to enable a rule or entitlement to be valid only on Sundays between 12:00am to 6:00am.

To display the calendar day/time access details

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **10** (Day/Time Access).

3) Press **Enter**.
4) Review the day/time access details for the selected calendar.

6.3.3. Edit Calendar Duration Details

Use this task to edit the duration of a calendar.

To edit calendar duration

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **2** (Edit).
3) Press **Enter**.
4) Modify the duration details as necessary.
5) Press **Enter** twice.

6.3.4. Edit Calendar Day/Time Access Details

Use this task to edit the day/time access for a calendar

To edit calendar day/time access

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired group, enter **10** (Day/Time Access).
3) Press **Enter**.
4) In the **OPT** column for the desired day/time access entry, enter **2** (Edit).
5) Modify the day/time access details as necessary.

Tip: You can add a new day/time access entry by pressing the **F6** (Add) function key. For example, your calendar might require two day/time access entries: the first entry for Monday-Friday with a start time of 08:00:00 and an end time of 17:00:00, and the second entry for Saturday only with a start time of 08:00:00 and an end time of 12:00:00.

6) Press **Enter** twice.

See also:

Manage Calendar Day/Time Access

6.3.5. Add Calendar

Use this task to add a calendar.

To add calendar

1) Access the **Work with Calendar** interface.
2) Press the **F6** (Add) function key.
3) Enter the parameters necessary to define the duration for which the calendar is valid.

Tip: Press **F1** (Help) to access field descriptions.

Field	Description
Calendar Name	ID used to identify the calendar

Field	Description
Start Date	Start date on which the calendar is valid
Start Time	Start time on which the calendar is valid
End Date	End date on which the calendar becomes invalid
End Time	End time on which the calendar becomes invalid
Description	Short description identifying the purpose of the calendar

4) Press **Enter** twice.
5) Enter the days of the week for which the calendar is valid.

Tip: For example, to limit the application of a rule or entitlement to Monday-Friday, remove the **X** value beside Saturday and Sunday.

6) Enter the start and end time for which the calendar is valid for the selected day(s).

Note: The system applies the start/end time to all selected days. To enter different day/time access combinations, you must edit the calendar once it is saved.

7) Press **Enter**.

See also:

Manage Calendar Day/Time Access

6.3.6. Copy Calendar

Use this task to copy a calendar. This is a fast way to create a new calendar based on an existing calendar.

To copy a calendar

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Modify the calendar details as necessary.
5) Press **Enter** twice.

6.3.7. Delete Calendar

Use this task to delete a calendar.

To delete calendar

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct calendar.
5) Press **Enter** twice.

6.4. Manage Calendar Day/Time Access

Use this task to do the following with calendars:

- Display day/time details
- Add day/time details
- Edit day/time details
- Copy a day/time details
- Delete a day/time details

To manage the calendar day/time details, access the **Work with Calendar** interface.

To access the Work with Calendar interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

6.4.1. Display Day/Time Details

Use this task to display the details for a specific day/time access requirement.

To display the day/time requirement details

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **10** (Day/Time Access).
3) Press **Enter**.
4) In the **OPT** column for the desired day/time requirement, enter **5** (Display).

Note: The **Day/Time Access** interface is displayed.

6.4.2. Add Day/Time Requirement

Use this task to add a day/time access requirement.

To add day/time requirement

1) Access the **Day/Time Access** interface.
2) Press the **F6** (Add) function key.
3) Add an **X** beside the day(s) of the week for which you want to add a requirement.
4) Enter a start and time.

Tip: For example, enter 00:00:00 as the start time and 24:00:00 as the end time to indicate 24 hours.

5) Press **Enter** twice.

6.4.3. Edit Day/Time Requirement

Use this task to edit a day/time access requirement.

To edit day/time requirement

1) Access the **Day/Time Access** interface.
2) In the **OPT** column, enter **2** (Edit) for the desired day/time requirement.
3) Press **Enter**.
4) Modify the day/time requirement as necessary.

5) Press **Enter** twice.

6.4.4. Copy Day/Time Requirement

Use this task to copy a day/time access requirement. This is a fast way to create a requirement based on an existing requirement.

To copy day/time requirement

1) Access the **Day/Time Access** interface.
2) In the **OPT** column for the desired requirement, enter **3** (Copy).
3) Press **Enter**.
4) Modify the requirement details as necessary.
5) Press **Enter**.

6.4.5. Delete Day/Time Requirement

Use this task to delete a day/time access requirement.

To delete day/time requirement

1) Access the **Day/Time Access** interface.
2) In the **OPT** column for the desired requirement, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct requirement.
5) Press **Enter** twice.

7. Reports

7.1. Working with Reports

This section describes working with built-in reports.

To work with reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

See also:

Custom Reports

7.2. Display List of Reports

Use this task to do the following:

- Display the list
- Sort the list
- Move to a specific location within the list
- Filter the list

7.2.1. Display list

Use this task to display the list of available reports.

To display the list of reports

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

Note: The **Work with Reports** interface is displayed.

7.2.2. Sort List

Use this task to sort the list of available reports. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Collector ID** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Reports** interface.

2) Place your cursor on a column heading (e.g., Collector ID, Report Name, or Category).
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list of reports in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

7.2.3. Move to Location in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a report.

To move to a specific position within the list

1) Access the **Work with Reports** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

7.2.4. Filter List

Use this task to limit the reports displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Reports** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

7.3. Run Reports

Use this task to run a built-in or custom report using the **Work with Reports** interface.

To run a report using the Work with Reports interface

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.
4) Enter **7** in the **Opt** column for the report you want to run.
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Field	Description
Collector ID	ID identifying the collector (not an editable field)
Collector	Name assigned to the collector (not an editable field)

Field	Description
Report ID	ID assigned to the report you want to run (must be a report associated with the collector) **Note**: Multiple reports can be produced from a single collector, so at this point you could change the report ID to any of the reports linked to the identified collector.
Override report defaults	***YES** - Ignore run-time collector defaults. ***NO** - Apply Run-time collector defaults. **Tip**: Run-time collector defaults maximize report efficiency. Collector defaults allow you to filter collector data before attempting to generate your report. See Create Reports for additional information about setting up run-time collector defaults.
Reload collector data	***AI** - Allow the artificial intelligence engine to determine if data source collection should be re-run ***YES** - Re-run data source collection before producing the report output ***NO** - Used cached version of data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Run interactively?	***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.4. Create Reports

Use this task to create a custom report. Creating a report is a multi-step process:

Step 1 - Add report

Step 1 - Select source from which to collect report data

Step 2 - Name the report

Step 3 - Select the columns you want to include in the report

Step 4 - Define the filter criteria

Step 5 - Define the run-time collector defaults

Step 6 - Confirm the report details

To create reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**.

7.4.1. Add Report

To add a Report

1) Access the **Work with Reports** interface.
2) Press the **F6** (Add Report) function key.
3) Follow the steps in the report wizard.

7.4.2. Select Data Source Collector

Use this task to select the data source collector for your custom report.

To select the data source collector

1) In the **Opt** column for the collector that you want to use as the data source for your report, enter **1** (Select).
2) Press **Enter**.

7.4.3. Name the Report

Use this task to assign a name, ID, and category to your custom report.

To identify the report

1) Complete the following fields:

Field	Description
Report ID	Id you want to assign to the report **Tip**: The name cannot contain spaces.
Report Name	Name you want to assign the report **Tip**: Use a name that describes the data that will appear in the report.
Category	The report category under which you want to group the report **Tip**: There are four standard categories: Configuration, Resources, Profiles, Network.

2) Press **Enter**.

Note: The report should now be linked to the collector and appear in your list of available reports under the identified category.

7.4.4. Select Report Fields

Use this task to select the collector fields that you want to appear as columns in your report.

Note: By default, all collector fields are selected when you create a custom report.

Tip: To customize which collector fields to include, press the **F4** (Select Fields) function key.

To select report fields

1) Press the **F4** (Select Fields) function key.
2) Enter **1** in the **Sel** column for each field you want to include as a column in your custom report.

3) Press **Enter**.

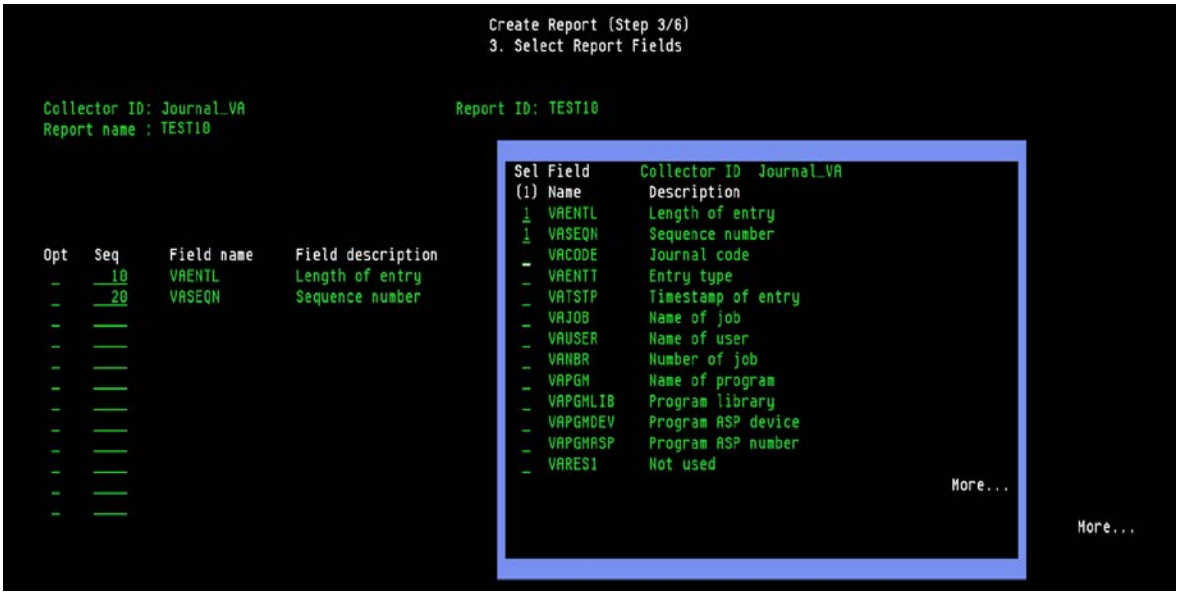


Figure: Select Report Fields

To change the order of the selected fields

Use this task to define the order in which fields should appear in the report.

Tip: The column with the lowest sequence number appears as the first column. The column with the highest sequence number appears as the last column.

1) Adjust the sequence numbers in the **Seq** column.
2) Press **Enter**.

7.4.5. Define Report Filter Criteria

Use this task to define the filter criteria for your custom report.

Note: Filters are not necessary but might improve the performance of your report.

To build report filter criteria

1) Press the **F4** (Select Fields) function key.
2) Enter **1** in the **Sel** column for each field to which you want to apply a filter.
3) Press **Enter**.

To add filter criteria

1) Add operators and comparison values as necessary.
2) Press **Enter**.

Tip: An SQL-like format is used to create report filters. For a list of supported operators, press **F10**.

Note: You can use up to five levels of nesting. To begin a nested condition, enter an open parenthesis "(" in the **Nest Str** column. Likewise, to end a nested condition, enter a closing parenthesis ")" in the **Nest End** column.

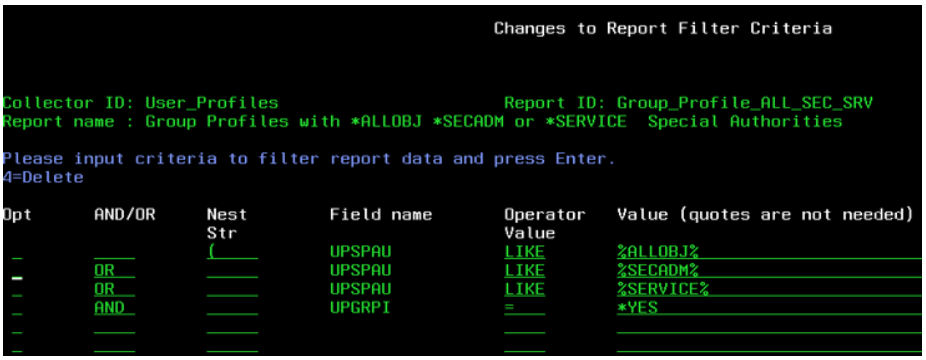


Figure: Build Report Filter Criteria

To delete filter criteria

1) Enter **4** (Delete) in the **Opt** column for the filter criteria you want to delete.
2) Press **Enter**.

7.4.6. Define Run-time Collector Defaults

Use this task to customize the defaults for the data source collection. This enables you to maximize how efficiently the report runs. Report defaults provide options specific to the data source collector on which the report is based, so you can filter the actual data source before the report filter is even applied.

An example of when report defaults are very useful is in the case of reports based on QAUDJRN journal data or database file journal data, where very large amounts of data can potentially accumulate and take a long time to process in a typical reporting scheme. With report defaults, you can specify particular date ranges so that any report filters are only run across a subset of data instead of the entire range of available data.

Report defaults are processed before any report run-time options, except when a user selects ***YES** in the **Override report defaults** field at the time they run a report.

(See Run Reports for additional information about the **Override report defaults** field.)

Tip: Collector defaults are highly recommended, but they are not required. Click the **F2** function key to skip this step.

To define report defaults

1) Enter the desired run-time collector default values.
2) Press **Enter**.

7.4.7. Confirm Report Creation

Use this task to confirm that you want to create the report that you have just defined.

Tip: Click the **F12** function key to go back one step at a time if you want to make changes or verify that you entered the correct information.

To confirm report creation

1) Review the information.
2) Press **Enter**.

7.5. Manage Reports

Use this task to do the following:

- Edit reports
- Copy reports
- Delete reports

To manage reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

Note: The **Work with Reports Interface** is displayed.

Alternatively, at the IBM i command line, enter **TGWRKRPT**, and press **Enter**.

7.5.1. Edit Report

Use this task to edit a report.

Important: The **Report ID** cannot be edited after the report is created.

To edit a report

1) Access the **Work with Reports** interface.
2) Enter the appropriate option in the **Opt** column for the report you want to modify:

Option	Description
2 (Edit)	Modify the report name, category, and regulation details **Note**: Only available for custom reports, not built-in reports (those shipped with the product)
6 (Defaults)	Modify the run-time collector defaults, which help to filter collector data **Note**: See Create Reports for additional information about run-time collector defaults.
8 (Field Lists)	Modify which collector fields you want to display in your report **Note**: Modifications cannot be made to built-in reports
9 (Filter)	Modify the filters you want applied to the data obtained from the collector **Note**: Modifications cannot be made to built-in reports

7.5.2. Copy Report

Use this task to copy a report. This is useful when an existing report provides results that are close to what you need, but still do not quite meet your requirements. You can save time by copying the report and customizing it instead of beginning from scratch.

To copy a report

1) Access the **Work with Reports** interface.
2) Enter **3** in the **Opt** column for the report you want to copy.

3) Enter a unique Report ID and continue customization as desired. Please refer to “Creating Reports” for details.

7.5.3. Delete Report

Use this task to delete a report.

Note: You can delete only customer reports, not built-in reports.

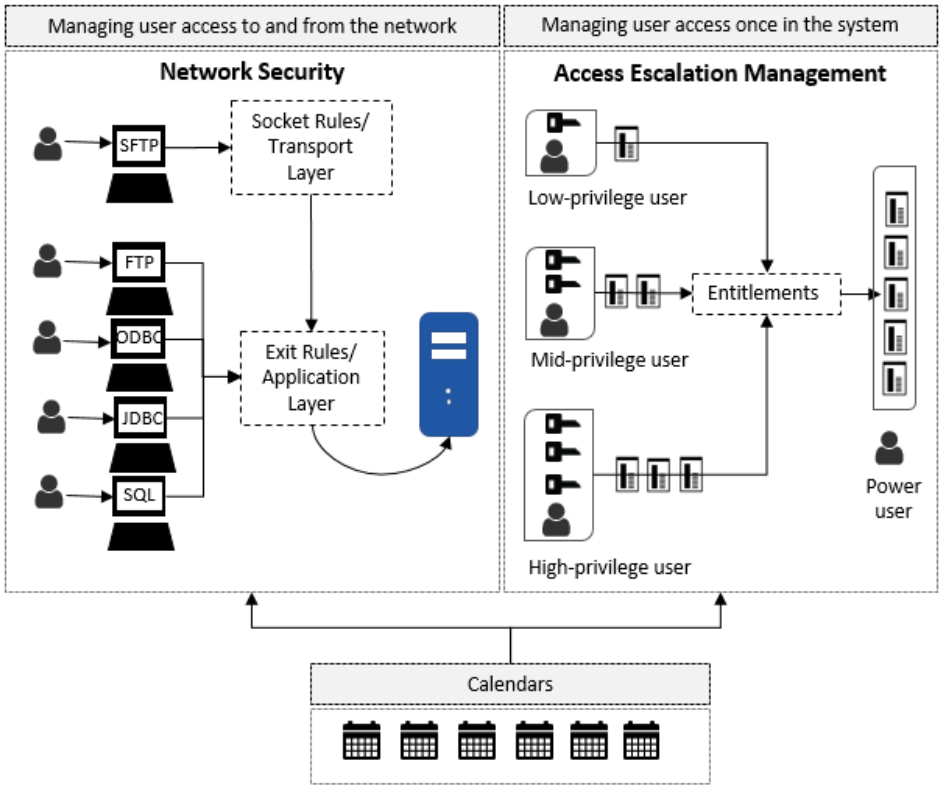
To delete a report

1) Access the **Work with Reports** interface.
2) Enter **4** in the **Opt** column for the report you want to delete.

8. Glossary

Calendars

The calendar allows you to enable a rule or entitlement for a specific duration (e.g., after hours, during weekends, on a holiday, etc.).



Collectors

A collector is the primary source used to gather data for a report. There are many collectors available for use.

The following is a summary of the general types of data available in collectors:

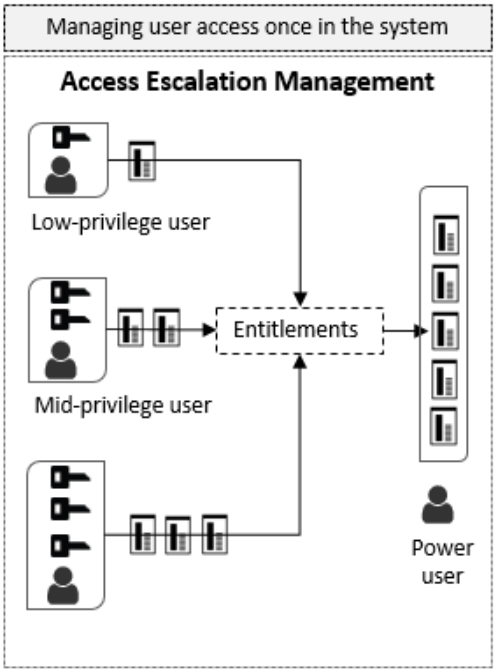
- User Profile Information
- System Value Data
- System Security Audit Journal (QAUDJRN)
- Database Journal Data
- Data Area Journal Data
- Exit Point Information
- Authority List Data
- Object Authority Information
- Object Details
- Network Status Information

Important: Collectors are required for defining new reports.

See also: For a complete list of available collectors, refer to Appendix A - Collectors.

Entitlement

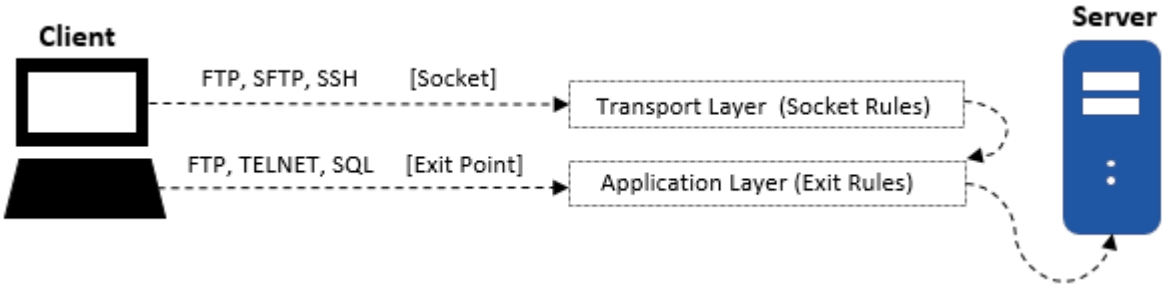
Entitlements are a form of rule associated with access management. Entitlements allow you to control the access level of a user or a user group at a very granular level. For example, a user might be required to perform a high-level task at the end of each fiscal year. Instead of granting the user high-level access throughout the year, you could create an entitlement that allows the user to perform the task at a designated time. In addition to identifying the specific task to be performed, you must also identify a swap user. A swap user is normally a user with higher-level privileges. In most cases, the user will need to temporarily borrow the swap users' privileges to perform the high-level task identified in the entitlement.



Exit Rules

Exit rules allow you to define criteria that control network access via TLS (Transport Layer Security). Exit rules are applied at exit points.

Note: Socket rules (if they exist) are applied before exit rules. In addition, function usage rules, which are also applied at exit points have the potential to conflict with exit rules. See Manage Exit Points for additional information about identifying conflicts.



Tip: There is a third type of rule called a function usage rule. These are generic rules provided by IBM that clients can apply at exit points. Function usage rules have limited functionality compared to exit rules, but your company might have applied one or more of these lower-capability function usage rules prior to implementing higher-capability exit rules. Therefore, there is the possibility that an existing function usage rule might conflict with a newly created exit rule. It is important that you identify and resolve any conflicts before deploying exit rules. See Manage Exit Points for more information about how to identify conflicts.

File Editors

File editors are custom IBM UPDDTA commands or third-party commands that you can use in addition to the standard IBM iSeries commands.
These commands might be used in conjunction with the standard IBM iSeries commands or they might be used as replacement commands. In any case, the third-party commands you plan to use must be registered using the File Editor tool in order for TG products to recognize it as a command.

Function Usage Rules

Function usage rules are provided by IBM and allow clients to limit the functions that a specific user can perform. These rules are not as nuanced or powerful as exit rule and do not take advantage of groups.

Function usage rules have the potential to conflict with exit rules. See Manage Exit Points for additional information about identifying conflicts.

For more information about function usage rules, refer to the IBM knowledge base article titled: Granular security control with function usage.

Groups

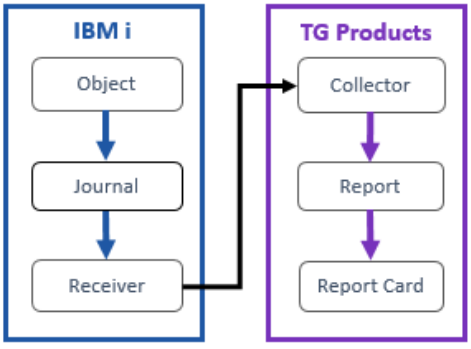
Groups are a means by which to organize system elements (which will be referred to as members). Once you create a group, you can use that group for different purposes. For example, you could use a group as a parameter when defining a rule. Therefore, the rule would apply to all user in the group. You can also use a group as a parameter when generating a report. For example, you might want your report to include information about a network group versus a specific server.

Note: The types of groups and reports available to you are dependent on your license agreement.

Journals

Journals provide a means by which you can record the activity of an object. This activity is captured in the form of a journal entry and stored in a journal receiver. TG products use collectors to pull data from journal receivers. The data pulled by the collectors is then used to produce reports.

For example, you can use the audit journal (QAUDJRN) to monitor object activity and to log security event.

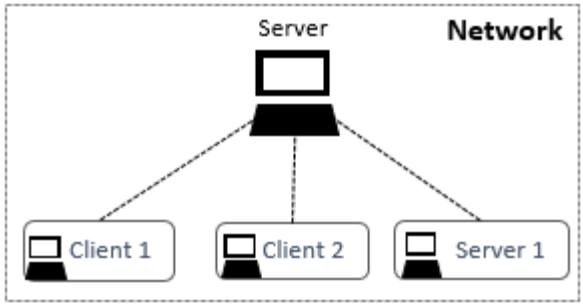


Library

A library is a means by which to group related objects and to find objects by name when they are used. Therefore, a library is a directory of grouped objects.

Networks

A network consists of a hub of computers. Normally, in a network, a more powerful, centralized computer (called the server) is connected to less powerful, distributed personal computers (called clients).



Objects

An object is a unit that exists (occupies space) in storage. Journals provide a means by which you can record the activity of an object.

Operations

An operation consists of a server, a function, and a command referenced by an incoming (remote) transaction. For example, the following table displays a list of functions and commands that might be received from an FTP server.

	Server	Function	Command
1	FTP	*ALL	*ALL
2	FTP	PUT	*ALL
3	FTP	GET	*ALL
4	FTP	CD	*ALL
5	FTP	DEL	*ALL

Receivers

Receives store journal transactions. Transactions are the data elements that document the activities of an object. TG products use collectors to pull transactions from receivers. Those pulled transactions are used to generate reports.

Built-in Reports

A report is a visual representation of data from a collector. The system provides built-in reports, and you can create custom reports as needed.

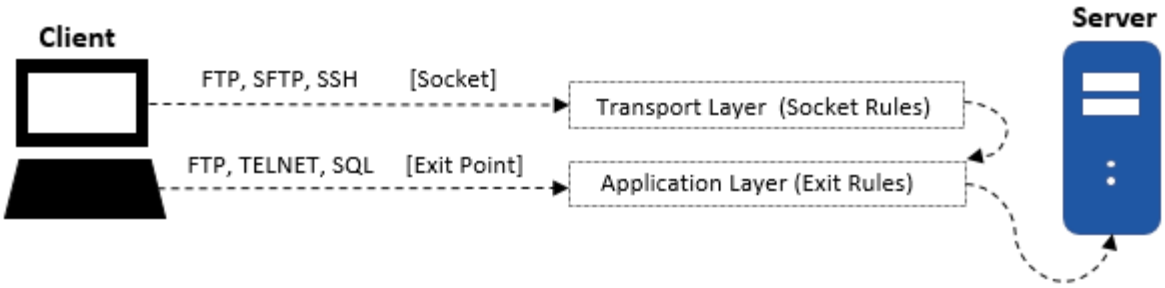
Note: The built-in reports available are dependent on your license agreement.

Rules

A rule allows you to control or limit an action or activity.
Note: The types of rules available to you are dependent on your license agreement.

Socket Rules

Socket rules allow you to define criteria that control network access via a socket. The socket provides an extra layer of security (or vulnerability) prior to the application layer, which provides security through exit rules.



Swap Profile

A swap profile is a user profile that allows another user to acquire more or less authority temporally. This might be necessary when a user needs to complete an activity or task for which the user does not have the privilege to execute. The ability to use a swap profile is defined in an entitlement.

Transactions

Transactions are remote requests that originate from outside of a target server.
A remote transaction can include the following information:

- User
- Network address (TCP/IP or SNA)
- Operation (server/function/command)
- Object
- Timestamp

Transactions in TGSecure are classified into the following categories:

- SOC - Transactions that come through the socket layer and are managed using socket rules.
- TRN - Transactions that come through exit points (application layer) and are managed using exit rules.

User

A user when referenced in this documentation is referring to an individual who required access to the system.

9. APPENDIX A - Collectors

Collector Category	Collector Name	Collector ID
Configuration	Job Description Data	Job_Descriptions
Configuration	Message Queue Information	Message_Queue
Configuration	Output Queue Information	Output_Queue
Configuration	Subsystem Autostart Jobs	Subsystem_Autostart
Configuration	Subsystem Communication Entries	Subsystem_Communications
Configuration	Subsystem Information Details	Subsystem_Information
Configuration	Subsystem Job Queue	Subsystem_Job_Queue
Configuration	Subsystem Pool Data	Subsystem_Pool_Data
Configuration	Subsystem Prestart Jobs	Subsystem_Prestart
Configuration	Subsystem Remote Entries	Subsystem_Remote
Configuration	Subsystem Routing Entries	Subsystem_Routing
Configuration	Subsystem Workstation Names	Subsystem_Workstation_Names
Configuration	Subsystem Workstation Types	Subsystem_Workstation_Types
DataAudit	Audit data area changes	Data_Area_Auditing
DataAudit	Monitor Database changes	Database_Auditing
IFS	Display Extended Journaling information for the IFS object	IFS_Journaling
IFS	Display status information about an IFS file	IFS_Status
IFS	Display the Attributes for the IFS objects	IFS_Attributes
IFS	Display the public and private authorities associated with the object	IFS_Authorities
Journal	Access Control List Changes	Journal_VA
Journal	Actions on Validation Lists	Journal_VO
Journal	Actions to IP Rules	Journal_IR
Journal	APPN Endpoint Filter Violations	Journal_NE
Journal	Asynchronous Signals Processed	Journal_SG
Journal	Authority Changes to Restored Objects	Journal_RA
Journal	Authority Collection Data	Authority_Collection
Journal	Authority Failures	Journal_AF

Collector Category	Collector Name	Collector ID
Journal	Authority Restored for User Profiles	Journal_RU
Journal	Authorization List or Object Authority Changes	Journal_CA
Journal	Change Request Descriptor Changes	Journal_CQ
Journal	Change Request Descriptors Restored	Journal_RQ
Journal	Changes to Service Tools Profiles	Journal_DS
Journal	Close Operations on Server Files	Journal_VF
Journal	Cluster Operation	Journal_CU
Journal	Commands Executed	Journal_CD
Journal	Connection Verification	Journal_CV
Journal	Connections Started, Ended, or Rejected	Journal_VC
Journal	Create Operations	Journal_CO
Journal	Cryptographic Configuration Changes	Journal_CY
Journal	Delete Operations	Journal_DO
Journal	Directory Link, Unlink, and Search Operations	Journal_LD
Journal	Directory Search Violations	Journal_ND
Journal	Directory Server Extensions	Journal_XD
Journal	DLO Object Changes	Journal_YC
Journal	DLO Object Reads	Journal_YR
Journal	Dual Optical Object Accesses	Journal_O2
Journal	EIM Attribute Changes	Journal_AU
Journal	Environment Variable Changes	Journal_EV
Journal	Exceeded Account Limit Events	Journal_VL
Journal	Exit Point Maintenance Operations	Journal_GR
Journal	Identity Token Events	Journal_X1
Journal	Internet Security Management Events	Journal_IS
Journal	Inter-process Communication Events	Journal_IP
Journal	Intrusion Monitor Events	Journal_IM
Journal	Invalid Sign-on Attempts	Journal_PW
Journal	Job Changes	Journal_JS
Journal	Job Descriptions – USER Parameter Changes	Journal_JD
Journal	Job Descriptions that Contain User Profile Names were Restored	Journal_RJ

Collector Category	Collector Name	Collector ID
Journal	Key Ring File Changes	Journal_KF
Journal	LDAP Operations	Journal_DI
Journal	Network Attribute Changes	Journal_NA
Journal	Network Authentication Events	Journal_X0
Journal	Network Log On and Off Events	Journal_VN
Journal	Network Password Errors	Journal_VP
Journal	Network Profile Changes	Journal_VU
Journal	Network Resource Accesses	Journal_VR
Journal	Object Auditing Attribute Changes	Journal_AD
Journal	Object Changes	Journal_ZC
Journal	Object Management Changes	Journal_OM
Journal	Object Ownership Changes	Journal_OW
Journal	Object Reads	Journal_ZR
Journal	Objects Restored	Journal_OR
Journal	OfficeVision Mail Services Actions	Journal_ML
Journal	Optical Volume Accesses	Journal_O3
Journal	Ownership Changes for Restored Objects	Journal_RO
Journal	Primary Group Changes	Journal_PG
Journal	Primary Group Changes for Restored Objects	Journal_RZ
Journal	Printer Output Changes	Journal_PO
Journal	Program Changes to Adopt Owner Authority	Journal_PA
Journal	Programs Restored that Adopt Owner Authority	Journal_RP
Journal	Programs that Adopt Authority were Executed	Journal_AP
Journal	PTF Object Changes	Journal_PU
Journal	PTF Operations	Journal_PF
Journal	Row and Column Access Control	Journal_AX
Journal	Secure Socket Connections	Journal_SK
Journal	Server Security User Information Actions	Journal_SO
Journal	Server Sessions Started or Ended	Journal_VS
Journal	Service Status Change Events	Journal_VV
Journal	Service Tools Actions	Journal_ST
Journal	Single Optical Object Accesses	Journal_O1

Collector Category	Collector Name	Collector ID
Journal	Socket Descriptor Details	Journal_GS
Journal	Spooled File Actions	Journal_SF
Journal	Subsystem Routing Entry Changes	Journal_SE
Journal	Swap Profile Events	Journal_PS
Journal	System Directory Changes	Journal_SD
Journal	System Values Changes	Journal_SV
Journal	Systems Management Changes	Journal_SM
Journal	User Profile Changes	Journal_CP
Log	Job Log Details	Job_Log_Details
Log	Job Log Summary	Job_Log_Summary
Network	Controller Attached Device Information	Controller_Attached_Devices
Network	Controller Description Information	Controller_Description_Data
Network	Device Description APPC Information	Device_Description_APPC
Network	Device Description Information	Device_Description_Data
Network	Line Description Information	Line_Description_Data
Network	Network Attribute Information	Network_Attributes
Network	Network Connections Ipv4 and Ipv6	Network_Connections
Network	Network Interface Data Ipv4	Network_Interface_Ipv4
Network	Network Interface Data Ipv6	Network_Interface_Ipv6
Network	Network Route Data Ipv4	Network_Route_Ipv4
Network	Network Route Data Ipv6	Network_Route_Ipv6
Network	Network Server Description Data	Network_Server_Descriptions
Network	Network Server Encryption Status	Network_Svr_Encrypt_Status
Network	TCP/IP Ipv4 Stack Attributes	Network_TCPIP_Ipv4
Network	TCP/IP Ipv6 Stack Attributes	Network_TCPIP_Ipv6
Object	Authorized Users through Authorization Lists	Auth_Users_via_Auth_Lists
Object	Display Field Level Authorities	Field_Authority
Object	Display Object Authority	Object_Authority
Object	Display Object Details	Object_Details
Object	Message Queue Data Details	Message_Queue_Data
Object	Program Reference Data	Program_Reference_Data
System	Authority List Data	Authority_List

Collector Category	Collector Name	Collector ID
System	Basic Information about a software product	Product_Info
System	Display Exit Point Data	Exit_Points
System	Display System Value Data	System_Values
System	Installed Software Resources Data	Software_Resources
System	Program Temporary Fix Data	PTF_Data
System	Service Tool User Data	Service_Tool_Users
Users	Display User Profile Data	User_Profiles
Users	Programs that Adopt Authority	Program_Adopt
Users	User Profile Object Authorities	User_Object_Authorities