opentext™

NetIQ Security Solutions for IBM i

TGSecure 3.4

User Guide

Revised October 2024

Legal Notice

What's New

Version 3.4 - TGSecure User Guide Revisions
This release includes the following: **Enhancements** • Network Security • File Server collection data - add SSL Flag • User Profile Archive UI to handle Hex data • User Profile Management • Add Report of Users (TGSecure-only licensing) • Command Security • Add the ability to copy in command security rules • Bug Fixes

See also

APPENDIX - TGSecure Revisions

TGSecure Introduction

This section includes the following topics:

- Historical Perspective of Security
- Features
- Rules Decision Algorithm
- Rules Suggestion Engine

See also

Getting Started

Historical Perspective of Security

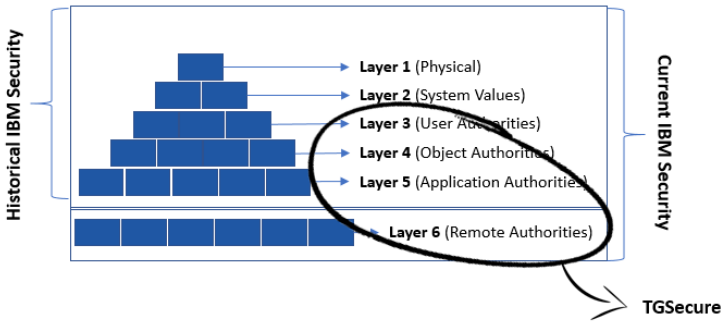
Before we talk about what TGSecure is or does, let's talk about where it fits. When the IBM® AS/400 was introduced in 1988, client/server configurations and Internet-based networks were not widely used. At that time, AS/400 servers were accessed through locally attached terminals. Security was controlled 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 OS/400 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 so has the server. Today, many IBM i systems are accessed via remote connections, which require additional security structure:

- **Remote Authorities** - Restricting remote client access

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

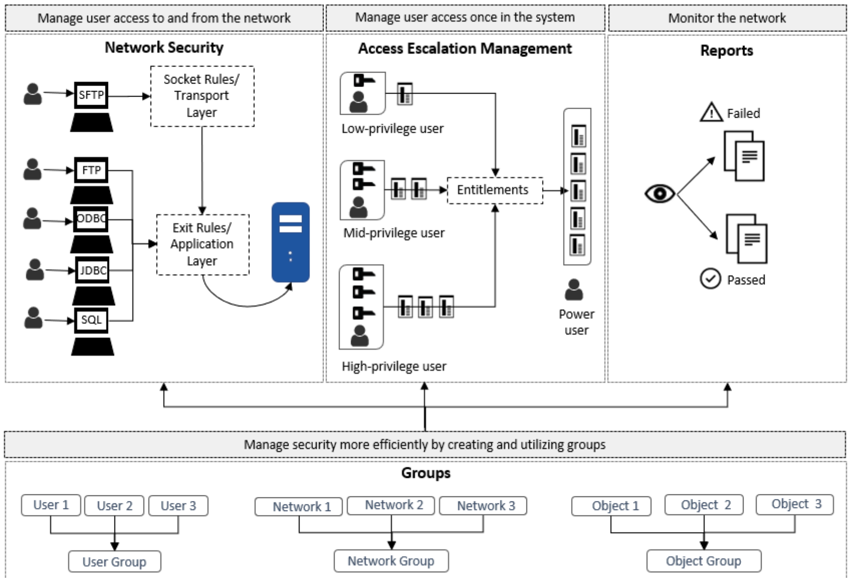


See also

TGSecure Introduction

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 TGSecure 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.

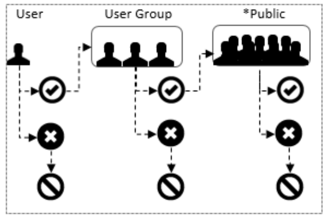
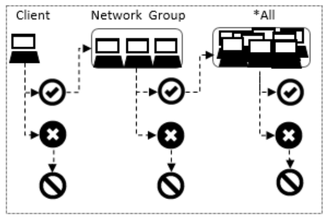
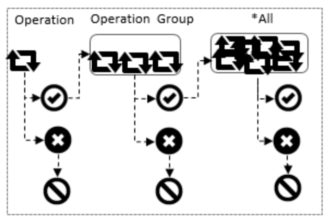
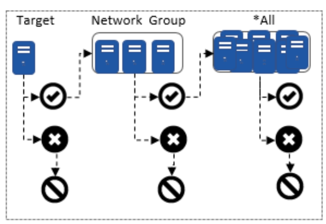
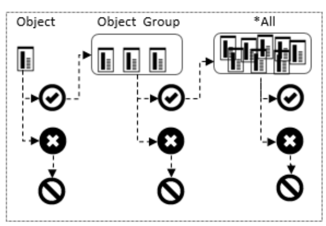
- Manage User Groups
- Manage Network Groups
- Manage Operations Groups
- Manage Object Groups

See also

TGSecure Introduction

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

TGSecure Introduction

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 TGSecure Reports.

Rules Suggestion Engine

Rules (i.e., exit rules or socket rules) are a powerful 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 fulfill a role shared by many. In that case, it would be more efficient to create a role-based rule that could be applied 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

Getting Started

This topic discusses the following:

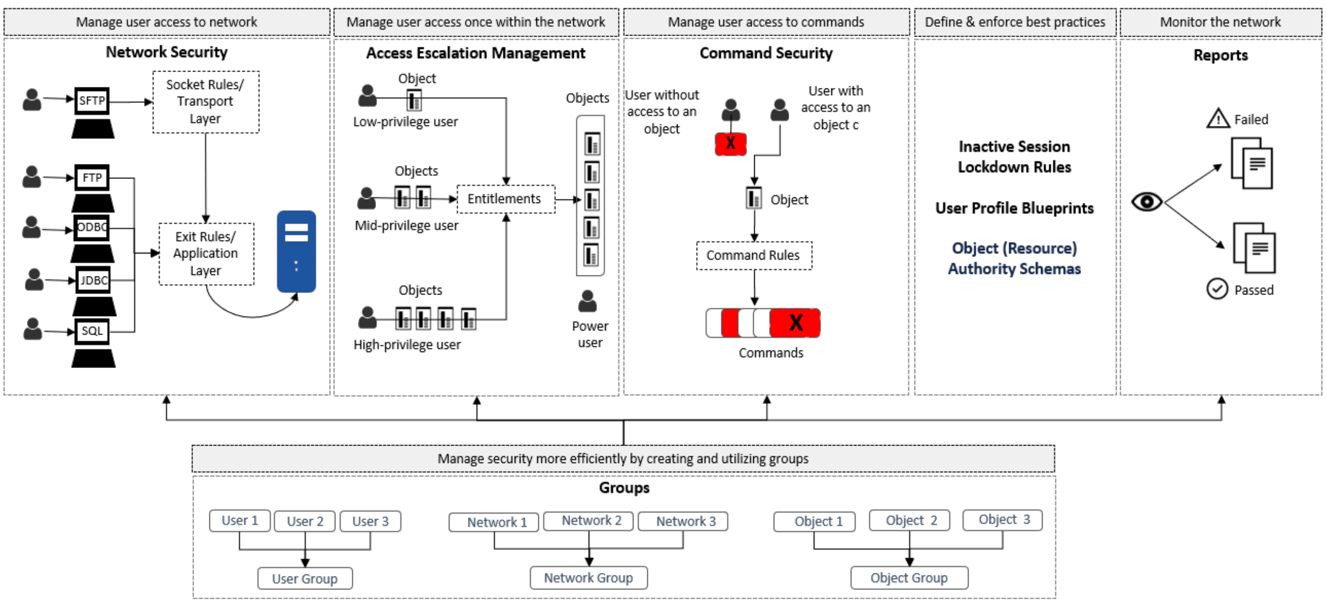
- Actions
- Process Flow
- Implementation Tasks

Actions

The following TGSecure features allow 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
- **Command Security** - Manage access to commands using rules (i.e., command rules)
- **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

Process Flow



Implementation 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.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>Monitor Network Access

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

Incoming Transactions in TGSecure allow you to display the connections requesting access and executing commands on the server.</td></tr>
<tr><td>2</td><td>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 feature of TGSecure allows you to create groups for the following elements:
• Users
• Networks
• Operations
• Objects</td></tr>
<tr><td>3</td><td>Manage Network Access

Once you have a better awareness of who and how your system is accessed and you have created what you think are logical and useful groupings, you can begin limiting network access.</td></tr>
</table>

Step	Description
	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)
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.
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 the security health of your server and system. **Note**: The built-in reports available to you are dependent on your license agreement.

See also

Log Into TGSecure

Features

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**. The **TG - Main** menu is displayed.
4) At the **Selection or command** prompt, enter **2** (TGSecure). The **TGSecure Main** menu is displayed.

See also

Getting Started

Working with TGSecure

Working with TGSecure

Follow these steps:

Step 1: Set up network security

- Working with Network Security Default Settings
- Working with Transactions
- Working with Exit Points
- Working with Socket Rules
- Working with Exit Rules
- Working with Network/Server Groups

Step 2: Set up Access Escalation

- Working with Access Escalation Management Defaults
- Working with Entitlements
- Working with Access Control
- Working with File Editor

Step 3: Set up Inactive Session Lockdown

- Working with Inactive Session Lockdown Defaults
- Working with Inactive Session Rules
- Working with Disconnect Options

Step 4: Set up Resource Manager

- Working with Resource Manager Defaults
- Working with Authority Schemas
- Working with Authority Collections

Step 5: Set up User Profile Manager

- Working with User Profiles
- Working with Blueprints
- Working with User Exclusions
- Working with Archived Profiles
- Working with Inactive Profiles
- Working with User Profiles
- Working with Password Rules

Step 6: Set up Command Security

- Working with Command Security Defaults
- Working with Command Security Rules
- Working with Command Security Reports

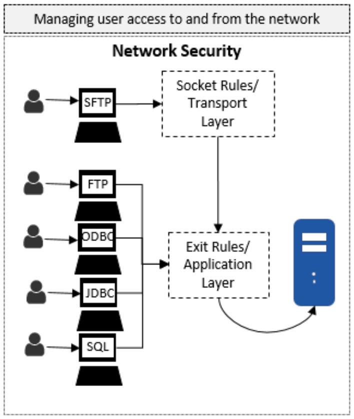
See also

Getting Started

Network Security

Use the **Network Security** feature to monitor and manage your network access. 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 the 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 cleartext. 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.



To access the Network Security interface

1) Log in to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.

Use the **Network Security** interface to do the following:

- Working with Network Security Defaults
- Working with Exit Points
- Working with Socket Rules
- Working with Exit Rules

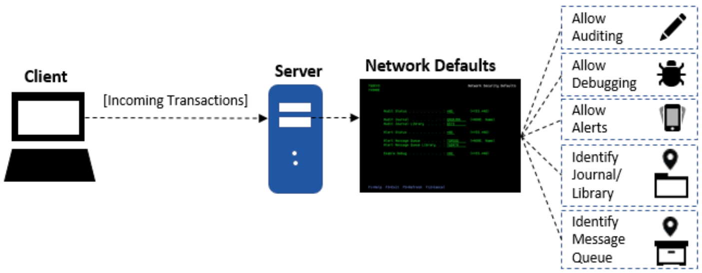
See also

Getting Started

Network Security Defaults

Use the **Network Security Defaults** feature to 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
- Whether a user can inherit privileges from a group



This section includes the following topics:

- Working with Network Security Default Settings
- Display Network Security Defaults
- Manage Network Security Defaults
- Run Network Security Reports

See also

Network Security

Working with Network Security Default Settings

Use the **Network Security Default** settings to do the following:

- Display Network Security Defaults
- Manage Network Security Defaults
- Run Network Security Reports

Note: To work with network security defaults, you must access the **Network Security Defaults** interface.

To access the Network Security Defaults interface

1) Log into to TGSecure. 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**. The **Network Security Defaults** interface is displayed.

See also

Network Security Defaults

Display Network Security Defaults

Use this task to display **Network Security** default settings.

To display the network security defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**. The **Network Security Defaults** interface is displayed.

Field	Description
Audit Status	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	Journal in which to store network security audit data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about network (internal) security changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** to if you plan to run network security change reports. **Note**: There are multiple TGSecure modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.
Alert Status	Whether alerting is enabled globally (for all exit points). Alerting is required if you plan to send alert notifications. ***YES** - Enable alerts for all (PASS and FAIL) connection attempts ***NO** - Disable 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 enabled 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	Queue in which to store alerts **Tip**: You can change the queue if you are using a third-party application for message monitoring.
Alert Message Queue Library	Library in which the queue is located
TELNET AutoSignon Allowed	Whether auto signon is enabled ***YES** - Enabled auto signon ***NO** - Disable auto signon ***ENCPWD** - Enable auto sign and encrypt password ***PWDRQD** - Enable auto signon
Primary Group Inheritance	Whether to allow primary group inheritance ***YES** - Enable profile primary group inheritance ***NO** - Disable profile primary group inheritance **Note**: The primary group is the user ID entered in the **Group** profile field when using command **CHGUSRPRF**. The primary group is the first ID from which a user inherits privileges.
Supplemental Group Inheritance	Whether to allow supplemental group inheritance ***YES** - Enable supplemental group inheritance ***NO** - Disable supplemental group inheritance **Note**: The supplemental groups are user IDs entered in the **Supplemental** group field when using command **CHGUSRPRF**. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.

Field	Description
Enable Debug	Whether to collect data for a debug log ***YES** - Enable debug log ***NO** - Disable debug log **Note**: The debug log is not required but might help with troubleshooting issues.

See also

Working with Network Security Default Settings

Manage Network Security Defaults

Use this task to manage the **Network Security** default settings.

- Access the Network Security Defaults Interface
- Enable Network Security Auditing
- Enable Network Security Change Auditing
- Enable Network Security Alerts
- Enable Network Security Debug Log
- Enable TELNET Auto Signon
- Enable Group Profile Inheritance

> **Note**: To manage network defaults, access the **Network Security Defaults** interface.

Access the Network Security Defaults Interface

To access the with Network Security Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**. The **Network Security Defaults** interface is displayed.

Enable Network Security Auditing

Use this task to enable network security auditing.

> **Tip**: Auditing is required if you plan to run network security reports.

> **Note**: 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 network security auditing

1) Access the **Network Security Defaults** interface.
2) In the **Audit Status** field, enter ***YES**.
3) In the **Audit Journal** field, enter the name of the journal in which to store the auditing data.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter**. The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Enable Network Security Change Auditing

Use this task to enable tracking of network security configuration changes.

> **Tip**: Tracking is required if you plan to run network security change reports.

To enable network security configuration change tracking

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

> **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.

Enable Network Security Alerts

Use this task to enable network security alerts.

Tip: Alerting is required if you plan to send alert notifications.

Note: If alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled 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 network security alerts

1) Access the **Network Security Defaults** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

Enable Network Security Debug Log

Use this task to enable the network security debugging log.

Note: The debug log is not required but might help with troubleshooting issues.

To enable network security debugging log

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

Enable TELNET Auto Signon

Use this task to enable TELNET auto signon.

Warning: This feature must be maintained and monitored properly to avoid any security issues.

Enabling TELNET auto signon is a three-step process:

Step 1. Update the **QRMTSIGN** system value to enable TELNET auto signon

Step 2. Update the **Network Security Defaults** to enable TELNET auto signon

Step 3. Update the **Network Security Configuration** to include the TELNET exit program

Step 1: To update the QRMTSIGN system value for TELNET auto signon

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **WRKSYSVAL QRMTSIGN**.
3) Press **Enter**. The **Work with System Values** interface is displayed.
4) In the **Option** column beside the **QRMTSIGN** system value, enter **2** (Change).
5) Press **Enter**. The **Change System Value** interface is displayed.
6) In the **Remote sign-on control** field, enter ***VERIFY**.
7) Press **Enter** twice.

Step 2: Update the Network Security Defaults for TELNET auto signon

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**. The **Network Security Defaults** interface is displayed.
6) In the **Telnet AutoSignon Allowed** field, enter ***YES**.
7) Press **Enter**.

Step 3: Update the Network Security Configuration for TELNET auto signon

1) Access the **Main** menu.

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

3) Press **Enter**. The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).

5) Press **Enter**. The **Network Security Configuration** interface is displayed.

2) In the **OPT** column beside the ***TELNET** network server, enter **11** (Add Exit Program).

3) Press **Enter**. Once an exit program is installed, you will see ***YES** in the **Exit Inst?** column for the exit point.

Enable Group Profile Inheritance

Use this task to enable users to inherit privileges as defined in their IBM profile. In other words, if an IBM user profile is a member of group (as defined by the **Group profile** and/or **Supplemental group** profile parameters), then you can use the following instruction to ensure that rules (socket rules, exit rules, etc.) created in TGSecure consider the privileges inherited by users when the system is enforcing rules.

Here is a usage example. There are two IBM users: User AAA (higher privilege user) and user BBB (lower privilege user). An IBM user administrator decides to allow user BBB to inherit the privileges from user AAA. To do this, the IBM user administrator uses the command CHGUSRPR, and then enters AAA in the **Group profile** or **Supplemental group** parameter. By taking this action, the user administrator is allowing user BBB to inherit the privileges as user AAA. Now if you want the inherited privileges granted by the IBM user administrator to be considered in TGSecure when evaluating rules, then you must enable group profile inheritance in TGSecure.

To enable group profile inheritance

1) Access the **Network Security Defaults** interface.

2) In the **Primary Group Inheritance** field, enter ***YES**.

> **Note**: The primary group is the user ID entered in the **Group profile** field when using command CHGUSRPRF. The primary group is the first ID from which a user inherits privileges.

3) In some cases, a user might inherit privileges from multiple users. In such a case, enter ***YES** in **Supplemental Group Inheritance** field.

> **Note**: Supplemental groups are user IDs entered in the **Supplemental group** field when using command CHGUSRPRF. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.

4) Press **Enter**.

> **Tip**: Refer to the IBM knowledge base for additional information regarding primary and secondary group inheritance.

See also

Working with Network Security Defaults

Run Network Security Reports

Use this task to generate the **Network Security** reports.

> **Note**: Refer to the TGSecure Report Reference for a complete list of report definitions.

To run the Network Security Reports

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 the category of the report type you want to run.

Category	Type of Report
1	Transaction Reports
2	Summary Reports
3	Configuration Reports
4	Configuration Reports

> **Note**: See the TGSecure Report Reference for a description of each available report.

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

See also

Working with Network Security Default Settings

Exit Point Configuration

This section describes how to work with **Exit Points**. At 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 the 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

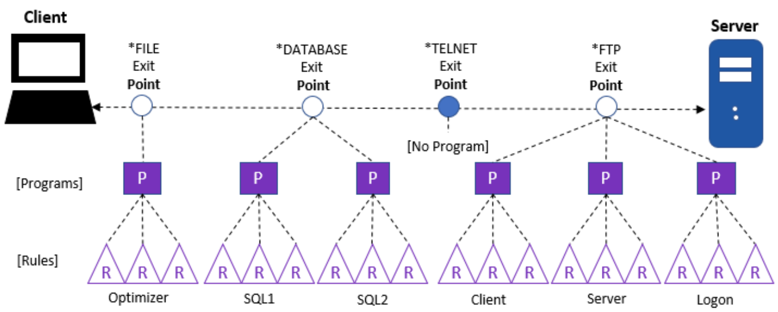
The prior paragraph uses a lot of jargon, so here is an analogy to help you conceptualize what an exit point represents. Say that your IBM server is a building. In the past, if someone wanted to access your building, they would just walk to it. Then, at some point, people started riding horses, and then 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 the 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).



Tip: 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.

Note: To work with exit points, you must access the **Network Security Configuration** interface.

This section includes the following topics:

- Working with Exit Points
- Display List of Exit Points
- Manage Exit Points
- Run Exit Points Report

See also

Network Security

Working with Exit Points

Use the **Exit Points** feature to do the following:

- Display List of Exit Points
- Manage Exit Points
- Run Exit Points Report

> **Note**: To work with exit points, you must access the **Network Security Configuration** interface.

To access the Network Security Configuration interface

1) Log into to TGSecure. The **TGSecure Main** menu appears.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**. The **Network Security Configuration** interface is displayed.

See also

Exit Point Configuration

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**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**. 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.

Field	Description
Network Server	Name of the server type
Audit Status	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 enabled 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. **Note**: See Manage Network Security Defaults for information about enabling/disabling auditing globally.
Sec Status	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	Whether alerting is 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 enabled 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. **Note**: See Manage Network Security Defaults for information about enabling/disabling alerting globally.
Smart Mode	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.
Collector Status	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
Function Usage	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
Exit Inst?	Whether the exit point is installed on the server *YES - Exit points are installed and ready for use *NO - Exit points are not installed **Note**: The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to ***YES**.
Network Description	A short description of the network

See also

Working with Exit Point

Manage Exit Points

Use this task to manage exit points.

- Access the Work with Network Security Configuration Interface
- Display Exit Point Details
- Enable Exit Point Auditing
- Enable Exit Point Security
- Enable Exit Point Alerts
- Enable Exit Point Collection
- Add Exit Program to Exit Point
- Add Exit Programs to Exit Points (Mass Update)
- Remove Exit Programs from Exit Points (Mass Update)
- Cycle Server
- Cycle Servers (Mass Update)
- Update all Exit Points (Mass Update)

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

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**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**. The **Network Security Configuration** interface is displayed.

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 ***YES** - Exit points are installed and ready for use ***NO** - Exit points are not installed **Note**: The exit rules associated with the exit point are not applied until the exit point is installed and the Security Status is set to *YES.
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 enabled at the exit point (secondary) level. The module-level setting takes precedence.

Field	Description
	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. **Note**: 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 enabled 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.
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

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.

> **Note**: 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**.

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.

> **Note**: 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**.

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.

Note: 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**.

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**.

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 exit point, enter **11** (Add Exit Program).
3) Press **Enter**. Once an exit program is installed at an exit point, you will see *__YES__ in the **Exit Inst?** column for the exit point.

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 program to exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F20** (Add Exit Programs) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F20, you must hold down the **Shift** key and F8.

3) Enter *__All__ to add all exit points to an exit program or enter a specific server type.
4) Press **Enter**.

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 exit point, enter **12** (Remove Exit Program).
3) Press **Enter**.

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 program from exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F21** (Remove Exit Programs) function key.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F21, you must hold down the **Shift** key and F9.

3) Enter ***All** to remove all exit programs or enter a specific server type.
4) Press **Enter**.

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 exit 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 the queue (run as part of a job queue)
6) Press **Enter**.

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.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F19, you must hold down the **Shift** key and F7.

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**.

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. ***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**.

See also

Working with Exit Point

Run Exit Points Report

Use this task to generate the following exit point reports:

- Access the Network Reports Interface
- Run Exit Point Configuration Report
- Run Exit Point Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with exit point reports, access from the **Network Reports** interface.

Access the Network Reports Interface

To access the Access Escalation Reports interface

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**. The **Network Reports** interface is displayed.

Run Exit Point Configuration Report

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

To run the Exit Point Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

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

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**. The status of the report is displayed at the bottom of the screen.

Run Exit Point Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.

To run the Exit Point Configuration Change Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

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**. The status of the report is displayed at the bottom of the screen.

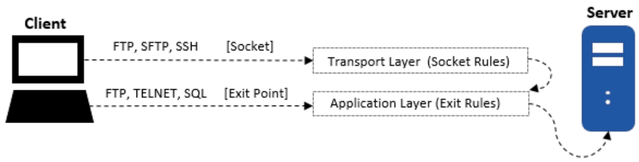
See also

Working with Exit Points

Incoming Transactions

This section describes how to work with **Incoming 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 the 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.



This section includes the following topics:

- Working with Transactions
- Display List of Incoming Transactions
- Manage Incoming Transactions
- Run Transactions (*TRN) Report
- Run Socket Transaction (*SOC) Reports

See also

Network Security

Working with Transactions

Use the **Transaction** feature to do the following:

- Display List of Incoming Transactions
- Manage Incoming Transactions
- Run Transactions (*TRN) Report
- Run Socket Transaction (*SOC) Reports

Note: To work with incoming transactions, you must access the **Incoming Transactions** interface.

To access the Incoming Transactions interface

1) Log into to TGSecure. The **Main** menu appears.

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

3) Press **Enter**. The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Incoming Transactions).

5) Press **Enter**. The **Incoming Transactions** interface is displayed.

See also

Incoming Transactions

Display List of Incoming Transactions

Use this task to display incoming transactions.

- Display List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of incoming transactions.

To display the list of incoming transactions

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Incoming Transactions).
5) Press **Enter**. The **Incoming Transactions** interface is displayed.

Field	Description
Tran Type	There are two types of transactions: ***TRN** - Transaction coming through an exit point ***SOC** - Transaction coming through a socket
User	User who initiated the transaction
Server	Type of server
Function	Function being executed
SSL?	Whether SSL is enabled: ***YES** - SSL enabled ***NO** - SSL disabled ***N/A** - SSL Communication is not applicable
Client IP	IP address of the server initiating the transaction
Tran. 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.
Object Details	Object affected by the transaction
Timestamp	Time at which the transaction was received

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.

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

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Transactions

Manage Incoming Transactions

Use this task to manage incoming transactions.

- Access the Incoming Transactions Interface
- Display Incoming Transaction Details
- Delete Incoming Transaction
- Archive Incoming Transactions
- Create a Rule-Based on a Transaction
- Create an Exit Point Transaction Rule
- Create a Socket Transaction Rule
- Accept a Rule Suggestion

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

Access the Incoming Transactions Interface

To access the Incoming Transactions interface

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 **1** (Incoming Transactions).
5) Press **Enter**. The **Incoming Transactions** interface is displayed.

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: ***YES** - SSL is enabled ***NO** - SSL is disabled ***N/A** - SSL Communication is not applicable
Operation Server	Type of server
Function	Function being executed
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 affected by the transaction

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**.

Archive Incoming Transactions

Use this task to delete (cleanup) incoming 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 transactions 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 help show this.

To archive incoming transactions

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

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F16, you must hold down the **Shift** key and F4.

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

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

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

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 transactions, 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
> - TRN = exit point transaction
>
> The screen that 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.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F23, you must hold down the **Shift** key and F11.

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).

Create an Exit Point Transaction Rule

Use this task to create an exit point transaction rule.

To create an exit point transaction rule

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

Note: The **Tran Type** field identifies the type of transaction:

- SOC = socket level transaction
- TRN = exit point transaction

3) Press **Enter**.
4) Complete the following fields:

Field	Description
User Name	User/user group to which the rule applies
Operation/Port	Operation server or port to which the rule applies
Client IP	IP address to which the rule applies
Calendar	Calendar that defines when the rule is applicable
Swap User	Swap user to which the rule applies
Alert Status	Whether to send a notification when the rule is triggered
Action	Flag indicating when the rule is triggered ***EXITLVL**- Triggered rule for exit level pass ***FAIL** - Triggered rule on exit level fail
Rule Description	Short description of the rule
Delete Transaction	Flag indicating whether to delete the transaction

5) Press the **F23** (Accept Rule) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F23, you must hold down the **Shift** key and F11.

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).

Create a Socket Transaction Rule

Use this task to create a socket transaction rule.

To create a socket transaction rule

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

> **Note**: The **Tran Type** field identifies the type of transaction:
>
> - SOC = socket level transaction
> - TRN = exit point transaction

3) Press **Enter**.

4) Complete the following fields:

Field	Description
User Name	User/user group to which the rule applies
Client IP	IP address to which the rule applies
Oper. Server	Operation server to which the rule applies
Function	Function to which the rule applies
Calendar	Calendar that defines when the rule is applicable
Swap User	Swap user to which the rule applies
Alert Status	Whether to send a notification when the rule is triggered
Action	Flag indicating when the rule is triggered ***PASS** - Triggered rule on pass ***FAIL** - Triggered rule on fail
Rule Desc.	Short description of the rule
Delete Trans.	Flag indicating whether to delete the transaction
Type of Object	Type of object to which the rule applies
Object Name	Name of the object to which the rule applies
Object Library	Library in which the rule applies
Object Type	Type of object to which the rule applies

5) Press the **F23** (Accept Rule) function key.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F23, you must hold down the **Shift** key and F11.

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).

Accept a Rule Suggestion

Use this task to accept a suggestion made by the Rules Suggestion Engine. The intelligence engine provides suggestions 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 referenced 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	In the **Opt** column, enter **1** beside the suggestion you feel is the most appropriate for your situation,

Situation	If...	Then...
	client IP to a network group, or you could add the server name to a network group. In addition, for exit rules, the operation can be added to operation groups, and the object can be added to object groups.	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 your selection. Once you exit the session (press **F3** or **F12**), the ability to undo a suggestion is lost.

See also

Working with Transactions

Rules Suggestion Engine

Rules Decision Engine

Run Transactions (*TRN) Report

Use this task to generate the following incoming transaction reports:

- Access the Network Reports Interface
- Run Incoming Transaction Details
- Run Transaction Summary by Server Report
- Run Transaction Summary by User Report
- Run Network Transaction Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with exit point reports, access from the **Network Reports** interface.

Access the Network Reports Interface

To access the Access Escalation Reports interface

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**. The **Network Reports** interface is displayed.

Run Incoming Transaction Details

Use this report to display incoming transaction details.

To run the Incoming Transactions Details Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Transaction Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Incoming Transactions Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary. 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.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Transaction Summary by Server Report

Use this report to display incoming transaction details by server.

To run the Transaction Summary by Server Report

1) Access the Network Reports interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Transaction Summary by Server).
5) Press **Enter**.
6) Modify the report run criteria as necessary. 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.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Transaction Summary by User Report

Use this report to display incoming transaction details by user.

To run the Transaction Summary by User Report

1) Access the Network Reports interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Transaction Summary by User).
5) Press **Enter**.
6) Modify the report run criteria as necessary. 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.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Network Transaction Report

Use this report to display network transactions.

To run the Network Transaction Report

1) Access the Network Reports interface.
2) At the **Selection or command** prompt, enter **1** (Transaction Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Network Transaction Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary. 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.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Transactions

Run Socket Transaction (*SOC) Reports

Use this task to generate the following socket transaction reports:

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with socket transaction reports, access from the **Network Reports** interface.

Access the Network Reports Interface

To access the Access Escalation Reports interface

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**. The **Network Reports** interface is displayed.

Run Socket Transaction Report

Use this report to display the socket transaction details.

To run the Socket Transaction Report

1) Access the Network Reports interface.
2) At the **Selection or command** prompt, enter **1** (Transaction Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Transactions Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Socket Summary by Server Report

Use this report to display socket transaction details by server.

To run the Socket Summary by Server Report

1) Access the Network Reports interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Socket Summary by Server).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Transaction Summary by User Report

Use this report to display socket transaction details by user.

To run the Transaction Summary by User Report

1) Access the Network Reports interface.

2) At the **Selection or command** prompt, enter **2** (Summary Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **2** (Socket Summary by User).

5) Press **Enter**.

6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

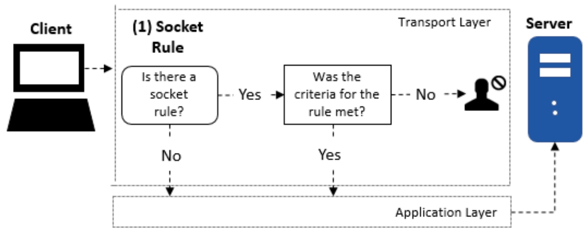
See also

Working with Transactions

Socket Rules

This section describes how to work 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).



This section includes the following topics:

- Working with Socket Rules
- Display List of Socket Rules
- Manage Socket Rules
- Run Socket Rule Reports

See also

Network Security

Working with Socket Rules

The **Socket Rule** feature allows you to do the following:

- Display List of Socket Rules
- Manage Socket Rules
- Run Socket Rule Reports

> **Note**: To work with socket rules, you must access the **Work with Socket Rules** interface.

To access the Work with Socket Rules interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**. The **Work with Socket Rules** interface is displayed.

See also

Socket Rules

Display List of Socket Rules

Use this task to display socket rules.

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of socket rules.

To display the list of socket rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**. The **Work with Socket Rules** interface is displayed.

Field	Description
User	User or user group to which the rule applies
Operation Port	Port to which the rule applies
Client IP	IP address to which the rule applies
Calendar	Applicable calendar **Note**: the calendar limits when the rule is applicable.
Alert Status	Whether alerting is enabled: *__YES__ - Alerts enabled *__NO__ - Alerts disabled
Action	The level at which action was taken: *__EXITLVL__ - Exit point level **Note**: If the action failed, you will see *__FAIL__ in this column.

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.

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

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Socket Rules

Manage Socket Rules

Use this task to manage socket rules.

- Access the Work with Socket Rules Interface
- Add Socket Rule
- Edit Socket Rule
- Copy Socket Rule
- Delete Socket Rule
- Display List of Users in a Group
- Display List of Clients in a Group
- Display List of Servers in a Group
- Display List of Operations in a Group

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

Access the Work with Socket Rules Interface

To access the Work with Socket Rules interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**. The **Work with Socket Rules** interface is displayed.

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) Complete the following fields:

Field	Description
User Name	Enter the user or user group to which the rule applies
Operation/Port	Enter the operation or port to which the rule applies
Client IP	Enter the IP address to which the rule applies
Calendar	Enter the applicable calendar **Note**: the calendar limits when the rule is applicable.
Alert Status	Identify whether to enable alerting: ***YES** - Alerts enabled ***NO** - Alerts disabled
Action	Enter the level at which to execute the action: ***EXITLVL** - Exit point level **Note**: If the action failed, you will see ***FAIL** in this column.
Rule Description	Enter a short description that describes the purpose of the rule.

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.

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 socket 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.

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 socket 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**.

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 socket rule, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter**.

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 socket 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.

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 socket 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.

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 socket 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.

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 socket 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.

See also

Working with Socket Rules

Run Socket Rule Reports

Use this task to generate the following socket rule reports:

- Access the Network Reports Interface
- Run Socket Rule Configuration Report
- Run Socket Rule Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with socket rule reports, access from the **Network Reports** interface.

Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**. The **Network Reports** interface is displayed.

Run Socket Rule Configuration Report

Use this report to display socket rule configuration details.

To run the Socket Rule Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Rules Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Socket Rule Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.

To run the Socket Rule Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Rules Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Socket Rules

Exit Rules

This section describes how to work with **Exit Rules**. Exit rules control network traffic associated with a specific application-level communication protocol (i.e., FTP, TELNET, and ODB).

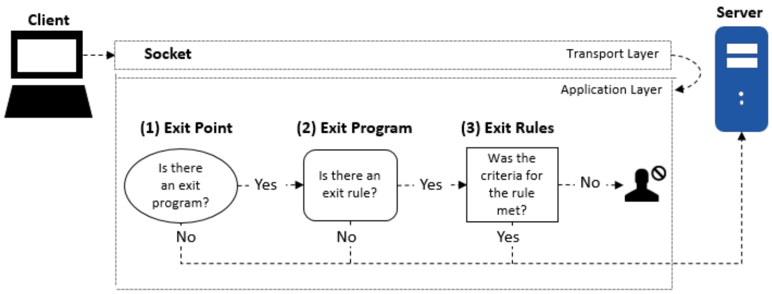
Example Usage: You might need a rule to reject all incoming transactions (connection) initiated by a specific user or member of a user group.

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 program can be created for each type of network communication (FTP, ODBC, JDBC, SQL, etc.). Exit programs control the 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.



This section includes the following topics:

- Working with Exit Rules
- Display List of Exit Rules
- Manage Exit Rules
- Run Exit Rule Reports

See also

Network Security

Working with Exit Rules

Use the **Exit Rule** feature to do the following:

- Display List of Exit Rules
- Manage Exit Rules
- Run Exit Points Report

> **Note**: To work with exit rules, you must access the **Work with Exit Rules** interface.

To access the Work with Exit Rules interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**. The **Work with Exit Rules** interface is displayed.

See also

Exit Rules

Display List of Exit Rules

Use this task to display exit rules.

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of exit rules.

To display the list of exit rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**. The **Work with Exit Rules** interface is displayed.

Field	Description
User	User or user group to which the rule applies
Server	Server on which the rule applies
Function	Function to which the rule applies
Client IP	IP address to which the rule applies
Calendar	Applicable calendar **Note**: the calendar limits when the rule is applicable.
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Action	The level at which action is taken: ***EXITLVL** - Exit point level **Note**: If the action failed, you will see ***FAIL** in this column.
Object Details	Short description of the object to which access was attempted

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.

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

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Exit Rules

Manage Exit Rules

Use this task to manage exit rules.

- Access the Work with Exit Rules Interface
- Add Exit Rule
- Edit Exit Rule
- Copy Exit Rule
- Delete Exit Rule
- Display List of Users
- Display List of Clients
- Display List of Servers
- Display List of Operations
- Display List of Objects

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

Access the Work with Exit Rules Interface

To access the Work with Exit Rules interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**. The **Work with Exit Rules** interface is displayed.

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) Complete the following fields:

Field	Description
User Name	Enter the user or user group to which the rule applies
Client IP	Enter the IP address to which the rule applies
Operation Server	Enter the operation server to which the rule applies
Calendar	Enter the applicable calendar **Note**: the calendar limits when the rule is applicable.
Alert Status	Identify whether to enable alerting: ***YES** - Alerts enabled ***NO** - Alerts disabled
Action	Enter the level at which to execute the action: ***EXITLVL** - Exit point level **Note**: If the action failed, you will see ***FAIL** in this column.
Rule Description	Enter a short description that describes the purpose of the rule.
Type of object	Enter the object to which the rule applies ***QSYS** - limit the rule to QSYS objects ***IFS** - limit the rule to IFS objects ***NONE** - include both QSYS and IFS objects

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**.
5) Complete the following additional fields based on your object type selection:

If	Then
you selected *__QSYS__ as the object type	Complete the following additional fields: **Object Name** - Name of QSYS object to which the rule applies **Object Library** - Name of the QSYS library to which the rule applies **Object Type** - Type of QSYS object to which the rule applies **Tip**: You will receive a warning message if you enter a name/library/type combination that does not currently exist on the server. If this is your intention (e.g., you are creating a rule for future use or you are creating a generic rule that you plan to implement across multiple servers), then ignore the warning by clicking **Enter**. If it was not your intention to create a rule that cannot be applied on the current server, then make any necessary corrections at this time.
you selected *__IFS__ as the object type	If you select *__IFS__ as your object type, complete the following additional field: **IFS Object** - Enter the file path to the IFS object
you selected *__NONE__	No addition fields are required

6) 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.

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 exit rule, enter **2** (Edit).

3) Press **Enter**.

4) Modify the parameters as necessary:

5) Press **Enter**.

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 exit 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**.

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 exit rule, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct rule.

5) Press **Enter**.

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 exit rule, enter **6** (User Grp).
3) Press **Enter**.
4) Review the list of users.

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 exit rule, enter **7** (Client Grp).
3) Press **Enter**.
4) Review the list of clients.

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 exit rule, enter **8** (Server Grp).
3) Press **Enter**.
4) Review the list of servers.

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 exit rule, enter **9** (Opr. Grp).
3) Press **Enter**.
4) Review the list of operations.

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 exit rule, enter **10** (Obj. Grp).
3) Press **Enter**.
4) Review the list of operations.

See also

Working with Exit Rules

Run Exit Rule Reports

Use this task to generate the following exit rule reports:

- Access the Network Reports Interface
- Run Exit Rule Configuration Report
- Run Exit Rule Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with exit rule reports, access from the **Network Reports** interface.

Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**. The **Network Reports** interface is displayed.

Run Exit Rule Configuration Report

Use this report to display exit rule configuration details.

To run the Exit Rule Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Remote Exit Rules Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Exit Rule Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.

To run the Exit Point Configuration Changes Report

1) Access the Network Reports interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Remote Exit Rules Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Exit Rules

AI Rules

This section describes how to work with **AI Rules**. Use an AI rule to override a default rule.

This section includes the following topics:

- Working with AI Rules
- Display List of AI Rules
- Manage AI Rules

See also

Network Security

Working with AI Rules

Use the **AI Rule** feature to do the following:

- Display List of AI Rules
- Manage AI Rules

> ⓘ **Note**: To work with exit rules, you must access the **Work with AI Rules** interface.

To access the Work with AI Rules interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (AI Rules).
5) Press **Enter**. The **Work with AI Rules** interface is displayed.

See also

AI Rules

Display List of AI Rules

Use this task to display AI rules:

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of AI rules.

To display the list of AI rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (AI Rules).
5) Press **Enter**. The **Work with AI Rules** interface is displayed.

Field	Description
Rule Type	Type of AI rule: ***PRE** - Check AI rule before exit point rules ***POST** - Check AI rule after regular exit point rules
User	User or user group to which the rule applies
Client IP	IP address to which the rule applies
Operation Server	Remote server to which the rule applies
Function	Function to which the rule applies
Calendar	Applicable calendar **Note**: the calendar limits when the rule is applicable.
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Action	The action taken when this rule matches an incoming transaction: ***AIFAIL** ***AIPASS** ***TRUSTED**
Object Details	Short description of the object to which access was attempted

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 AI 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.

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

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with AI Rules** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

See also

Working with AI Rules

Manage AI Rules

Use this task to manage AI rules.

Note: To manage AI rules, access the **Work with AI Rules** interface.

Access the Work with AI Rules Interface

To access the Work with AI Rules interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Network Security** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (AI Rules).
5) Press **Enter**. The **Work with AI Rules** interface is displayed.

Add AI Rule

Use this task to add an AI rule.

To add an AI rule

1) Access the **Work with AI Rules** interface.
2) Press the **F6** (Add) function key.
3) Complete the following fields:

Field	Description
Rule Type	Enter the rule type: *__PRE__ - Check AI rule before exit point rules *__POST__ - Check AI rule after regular exit point rules
User Name	Enter the user or user group to which the rule applies
Client IP	Enter the IP address to which the rule applies
Operation Server	Enter the operation server to which the rule applies
Calendar	Enter the applicable calendar **Note**: the calendar limits when the rule is applicable.
Alert Status	Identify whether to enable alerting: *__YES__ - Alerts enabled *__NO__ - Alerts disabled
Action	Enter the level at which to execute the action: *__EXITLVL__ - Exit point level
Number of Transactions	Enter the number of transactions required to trigger the rule 1-999999
Event Frequency	Enter the number of events required to trigger the rule 1-999999
Rule Description	Enter a short description that describes the purpose of the rule.

Field	Description
Type of object	Enter the object to which the rule applies ***QSYS** - limit the rule to QSYS objects ***IFS** - limit the rule to IFS objects ***NONE** - include both QSYS and IFS objects

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**.

5) Complete the following additional fields based on your object type selection:

If	Then
you selected ***QSYS** as the object type	Complete the following additional fields: **Object Name** - Name of QSYS object to which the rule applies **Object Library** - Name of the QSYS library to which the rule applies **Object Type** - Type of QSYS object to which the rule applies **Tip**: You will receive a warning message if you enter a name/library/type combination that does not currently exist on the server. If this is your intention (e.g., you are creating a rule for future use or you are creating a generic rule that you plan to implement across multiple servers), then ignore the warning by clicking **Enter**. If it was not your intention to create a rule that cannot be applied on the current server, then make any necessary corrections at this time.
you selected ***IFS** as the object type	If you select ***IFS** as your object type, complete the following additional field: **IFS Object** - Enter the file path to the IFS object
you selected ***NONE**	No additional fields are required

6) 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.

Edit AI Rule

Use this task to edit an existing AI rule.

To edit an AI rule

1) Access the **Work with AI Rules** interface.

2) In the **OPT** column for the desired **AI** rule, enter **2** (Edit).

3) Press **Enter**.

4) Modify the parameters as necessary:

5) Press **Enter**.

Copy AI Rule

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

To copy an AI rule

1) Access the **Work with AI Rules** interface.

2) In the **OPT** column for the desired AI 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**.

Delete AI Rule

Use this task to delete an AI rule.

To delete an AI rule

1) Access the **Work with AI Rules** interface.

2) In the **OPT** column for the desired AI rule, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter**.

Display List of Users

Use this task when the AI 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 AI** interface.
2) In the **OPT** column for the desired AI rule, enter **6** (User Grp).
3) Press **Enter**.
4) Review the list of users.

Display List of Clients

Use this task when the AI 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 AI Rules** interface.
2) In the **OPT** column for the desired AI rule, enter **7** (Client Grp).
3) Press **Enter**.
4) Review the list of clients.

Display List of Servers

Use this task when the AI 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 AI Rules** interface.
2) In the **OPT** column for the desired AI rule, enter **8** (Server Grp).
3) Press **Enter**.
4) Review the list of servers.

Display List of Operations

Use this task when the AI 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 AI Rules** interface.
2) In the **OPT** column for the desired AI rule, enter **9** (Opr. Grp).
3) Press **Enter**.
4) Review the list of operations.

Display List of Objects

Use this task when the AI 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

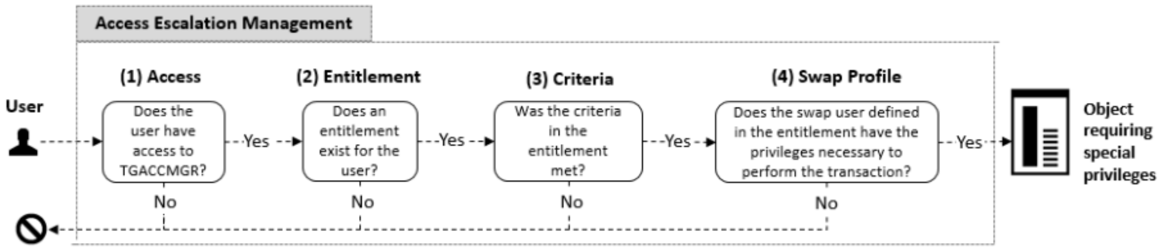
1) Access the **Work with AI Rules** interface.
2) In the **OPT** column for the desired AI rule, enter **10** (Obj. Grp).
3) Press **Enter**.
4) Review the list of operations.

See also

Working with AI Rules

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).



To access the Access Escalation Management interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.

Use the **Access Escalation Management** interface to do the following:

- Work with Access Escalation Management Defaults
- Work with Entitlements
- Work with Access Control
- Work with File Editor

See also

Getting Started

Access Escalation Defaults

Use the **Access Escalation Defaults** (AEM) feature to define the following:

- Default swap user
- How long an AEM session will last before requiring the user to reenter a password
- Journal in which to store AEM changes
- Library in which to store AEM changes
- Whether to enable auditing of AEM changes
- Queue in which to store AEM user alerts
- Queue library in which to store AEM user alerts

ⓘ **Note**: Access Escalation Management defaults apply to all entitlements unless otherwise defined.

The section includes the following topics:

- Working with Access Escalation Management Defaults
- Display Access Escalation Defaults
- Manage Access Escalation
- Run Access Escalation Report

See also

Access Escalation Management

Working with Access Escalation Management Defaults

Use the **Access Escalation Management Defaults** feature to do the following:

- Display Access Escalation Defaults
- Manage Access Escalation
- Run Access Escalation Report

> **Note**: To use the access escalation manager, you must access the **Work with Access Escalation** interface.

To access the Work with Access Escalation interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**. The **Work with Access Escalation** interface is displayed.

See also

Access Escalation Management

Display Access Escalation Defaults

Use this task to display the **Access Escalation** default settings.

> **Note**: These defaults apply to all entitlements unless otherwise defined.

To display Access Escalation defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**. The **Work with Access Escalation** interface is displayed.

Field	Description
Default Swap User	The default swap user (if one is not identified)
Authentication Timeout	Number of minutes the AEM session will remain enabled before requiring the user to reenter a password
Transaction Journal	Journal in which to store journal data
Transaction Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about AEM changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: This flag must be set to **Y** to if you plan to run access escalation change reports. **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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue

See also

Working with Access Escalation Management Defaults

Manage Access Escalation

Use this task to manage **Access Escalation** options.

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

Access the Access Escalation Interface

To access the Work with Access Escalation interface

1) Access the TGSecure **Main** menu.

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

3) Press **Enter**. The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).

5) Press **Enter**. The **Work with Access Escalation** interface is displayed.

Modify Access Escalation 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 escalation 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.

Enable Access Escalation Change Auditing

Use this task to enable tracking of access escalation configuration changes.

> **Tip**: Tracking is required if you plan to run access escalation change reports.

To enable access escalation configuration change tracking

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.

> **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see *__ALL__, this indicates that configuration changes are being tracked in all modules.

See also

Working with Access Escalation Management Defaults

Run Access Escalation Report

Use this task to generate the **Access Escalation** report.

> **Note**: Refer to the TGSecure Report Reference for a complete list of report definitions.

To run the Access Escalation Reports

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the category of the report type you want to run.

Category	Type of Report
1	Access Escalation Usage Report
2	Access Escalation Configuration Report
3	Access Escalation Change Report

> **Note**: See the TGSecure Report Reference for a description of each available report.

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

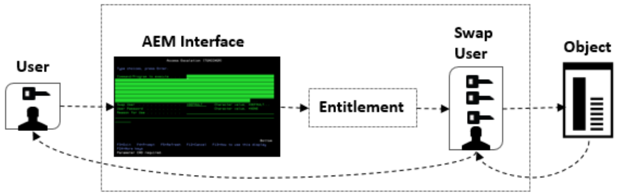
See also

Working with Access Escalation Management Defaults

Entitlements

Use the **Entitlements** feature to allow users 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.

This section contains the following topics:

- Working with Entitlements
- Display List of Entitlements
- Manage Entitlements
- Run Entitlement Reports

See also

Access Escalation Management

Working with Entitlements

Use the **Entitlements** feature to do the following:

- Display List of Entitlements
- Manage Entitlements
- Run Entitlement Reports

Note: In order to work with entitlements, you must access the **Work with Entitlements** interface.

To access the Work with Entitlements interface

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

To access the AEM interface

1) At the **Selection or command** prompt, enter **TGACCMGR**.
2) Press **Enter**. The **AEM** interface is displayed.

See also

Entitlements

Display List of Entitlements

Use this task to display entitlements.

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of entitlements.

To display the list of entitlements

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Entitlements).
5) Press **Enter**. The **Work with Entitlements** interface is displayed.

Field	Description
Enable Status	Whether the entitlement is enabled: **Y** - Enabled **N** - Disabled
User	User or user group to which the entitlement applies
Object	Object or object group to which the entitlement applies
Library	Library in which the object resides
Type	Type of object ***PMG** - Program ***CMD** - Command ***File** - Database file
Swap User	Swap profile whose privileges will be used to execute the entitlement
Aut Req?	Whether the user must enter a password (authenticate) in order to use the entitlement **Y** - Password required **N** - No password required
Alr Req?	Whether an alert is sent to the alert queue when an attempt is made to use the entitlement **Y** - Alert enabled **N** - Alert Disabled
Entitlement Description	Short description identifying the purpose of the entitlement

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.

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

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Entitlements

Manage Entitlements

Use this task to manage entitlements.

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

Access the Work with Entitlements Interface

To access the Work with Entitlements interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Entitlements).
5) Press **Enter**. The **Work with Entitlements** interface is displayed.

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 resides
Object Type	Type of object ***PMG** - Program ***CMD** - Command ***File** - Database 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	Whether the entitlement is enabled: **Y** - Enabled **N** - Disabled
Authentication?	Whether the user must enter a password (authenticate) in order to use the entitlement **Y** - Password required **N** - No password required
Alerting?	Whether an alert is sent to the alert queue when an attempt is made to use the entitlement **Y** - Alert enabled **N** - Alert Disabled
Entitlement Description	Short description identifying the purpose of the entitlement

4) Press **Enter** twice.

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 entitlement, 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.

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 entitlement, 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**.

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**.

See also

Working with Entitlements

Run Entitlement Reports

Use this task to generate the following entitlement reports:

- Access the Access Escalation Reports Interface
- Run Entitlement Usage Report
- Run Entitlement Configuration Report
- Run Entitlement Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with entitlement reports, access from the **Access Escalation Reports** interface.

Access the Access Escalation Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**. The **Access Escalation Reports** interface is displayed.

Run Entitlement Usage Report

Use this report to display entitlement usages details.

To run the Entitlement Usage Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **5** (Entitlement Usage).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports .

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**. The status of the report is displayed at the bottom of the screen.

Run Entitlement Configuration Report

Use this report to display entitlement configuration details.

To run the Entitlement Configuration Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Entitlements).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports .

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**. The status of the report is displayed at the bottom of the screen.

Run Entitlement Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Enable AEM Change Auditing for additional information.

To run the Entitlement Configuration Changes Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Entitlements Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports .

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**. The status of the report is displayed at the bottom of the screen.

See also

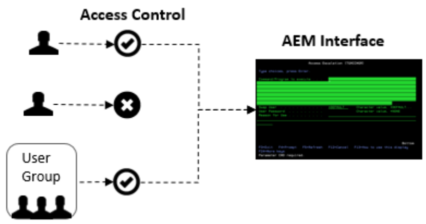
Working with Entitlements

Access Control

Use the **Access Control** feature 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.



This section contains the following topics:

- Working with Access Control
- Display Who Has Access to the AEM Interface
- Manage Access Control
- Run Access Control Reports

See also

Access Escalation Management

Working with Access Control

Use the **Access Control** feature to do the following:

- Display Who Has Access to the AEM Interface
- Manage Access Control
- Run Access Control Reports

> **Note**: To work with access controls, you must access the **Work with Access Control** interface.

To access the Work with Access Control interface

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

See also

Access Control

Display Who Has Access to the AEM Interface

Use this task to display access control options.

Display List

Use this task to display the list of users (including user groups) who have access control.

To display the list of users who have access control

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

Field	Description
User	User or user group to which the entitlement applies
Client IP	IP address from which the transaction was initiated

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.

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

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
>
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
>
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
>
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Access Control

Manage Access Control

Use this task to manage access control options.

- Access the Work with Access Control Interface
- Add Access Control
- Edit Access Control
- Copy Access Control
- Delete Access Control

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

Access the Work with Access Control Interface

To access the Work with Access Control interface

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

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 on your keyboard.
3) Enter the parameters necessary to define the control.

Field	Description
User Name	User or user group to which the entitlement applies
Client IP	IP address from which the transaction was initiated

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 of available groups.

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

4) Press **Enter** twice.

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 access control record, 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.

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**.

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**.

See also

Working with Access Control

Run Access Control Reports

Use this task to generate the following access control reports:

- Access the Escalation Reports interface
- Run Access Control Configuration Report
- Run Access Control Change Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with access control reports, access from the **Access Escalation Reports** interface.

Access the Escalation Reports interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**. The **Access Escalation Management** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**. The **Access Escalation Reports** interface is displayed.

Run Access Control Configuration Report

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

To run the Access Control Configuration Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Access Controls).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run 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.

Tip: You must enable auditing to produce change reports. See Enable AEM Change Auditing for additional information.

To run the Access Control Change Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Access Control Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

See also

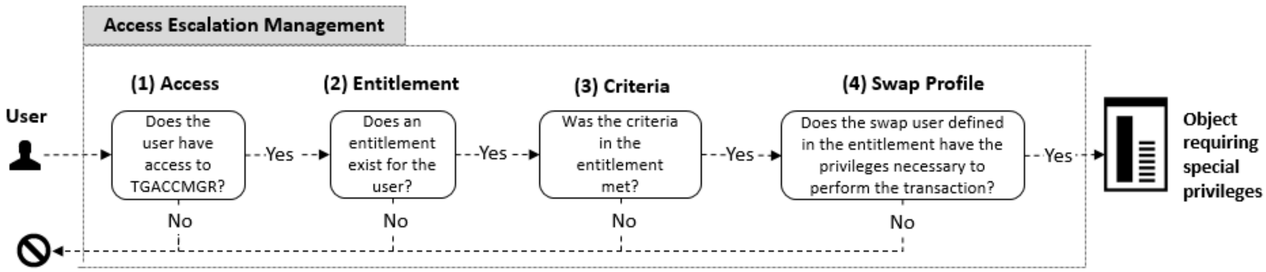
Working with Access Control

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. 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 of why you are performing this task.
7) Press **Enter**.

See also

Working with Access Control

File Editor

The **File Editor** feature provides access to 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.

This section includes the following topics:

- Working with File Editor
- Display List of File Editors
- Manage File Editors
- Run File Editor Reports

See also

Access Escalation Management

Working with File Editor

Use the **File Editor** feature to do the following:

- Display List of File Editors
- Manage File Editors
- Run File Editor Reports

Note: To work with the file editor, you must access the **Work with File Editor** interface.

To access the Work with File Editors interface

1) Log into to TGSecure. 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**. The **Work with File Editors** interface is displayed.

See also

File Editor

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 TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Work with File Editors).
5) Press **Enter**. The **Work with File Editors** interface is displayed.

Field	Description
Editor Command	Command to be executed
Editor Library	Library in which to execute the command
Editor Parameter	Parameter to be executed

See also

Working with File Editor

Manage File Editors

Use this task to manage the following 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 TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Work with File Editors).
5) Press **Enter**. The **Work with File Editors** interface is displayed.

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 on your keyboard.
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.

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 file editor, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

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 file editor, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter**.

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 file editor, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct file editor.
5) Press **Enter**.

See also

Working with File Editor

Run File Editor Reports

Use this task to generate the following file editor reports:

- Access the Access Escalation Reports Interface
- Run File Editors Configuration Report
- Run File Editor Change Report

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with file editor reports, access from the **Access Escalation Reports** interface.

Access the Access Escalation Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**. The **Access Escalation Reports** interface is displayed.

Run File Editors Configuration Report

Use this task to display file editor configuration details.

To run File Editor Report

1) Access the **Access Escalation Reports** interface
2) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
3) Press **Enter**. The **Access Escalation Configuration Reports** interface is displayed
4) At the **Selection or command** prompt, enter **2** (File Editors).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run File Editor Change Report

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

Tip: You must enable auditing to produce change reports. See Enable AEM Change Auditing for additional information.

To run File Editor Change Report

1) Access the Access Escalation Reports interface.
2) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
3) Press **Enter**. The **Access Escalation Change Reports** interface is displayed
4) At the **Selection or command** prompt, enter **2** (File Editors Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

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**. The status of the report is displayed at the bottom of the screen.

See also

Working with File Editor

Inactive Session Lockdown

Use the **Inactive Session Lockdown** (ISL) feature to customize how and when to end a user's session or lock a user's session when the system detects user inactivity for a specified duration (which is defined by an ISL rule). For security purposes, an inactive session has the potential to expose the system to unauthorized access and abuse.

> **Note**: An inactive session is a session in which the user has not interacted with their keyboard or mouse and/or when the system is not pulling resources. For example, if a job or report is running in the background, the system is consuming resources, so even though the user might not interact with their keyboard or mouse (i.e., user inactivity), the session is considered active because of the consumption of resources.

To access the Inactive Session Lockdown interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.

Use the **Inactive Session Lockdown** interface to do the following:

- Working with inactive session lockdown defaults
- Working with inactive session rules
- Working with disconnect options

See also

Getting Started

Inactive Session Lockdown Defaults

This section describes how to work with **Inactivity Session Lockdown** (ISL) **Defaults**. These defaults apply to all ISL rules unless otherwise defined.

Inactive session lockdown defaults allow you to define the following:

- How often the system checks for inactive sessions (e.g., every 30 seconds)
- Whether to track data about sessions disconnected by ISL
- Journal in which to store the data about sessions disconnected by ISL
- Library in which to store the data about sessions disconnected by ISL
- Whether to store changes to ISL rules or defaults
- Queue in which to store ISL admin alerts
- Queue library in which to store ISL admin alerts
- Warning message to share with user before session disconnect
- How often to share warning messages before session disconnect
- Whether to revoke user privileges when at least one of their sessions is in lockdown

This section includes the following topics:

- Working with Inactive Session Lockdown Defaults
- Display Inactive Session Lockdown Defaults
- Manage Inactive Session Lockdown
- Run Inactive Session Lockdown Reports

See also

Inactive Session Lockdown

Working with Inactive Session Lockdown Defaults

Use the **Inactive Session Lockdown** (ISL) **Default** settings to do the following:

- Display Inactive Session Lockdown Defaults
- Manage Inactive Session Lockdown
- Run Inactive Session Lockdown Reports

> **Note**: To work with ISL defaults, you must access the **Work with Inactive Session Lockdown Settings** interface.

To access the Work with Inactive Session Lockdown Settings Interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**. The **Work with Inactive Session Lockdown Settings** interface is displayed.

See also

Inactive Session Lockdown

Display Inactive Session Lockdown Defaults

Use this task to display the **Inactive Session Lockdown** (ISL) default settings.

To display the Interactive Session Lockdown defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**. The **Work with Inactive Session Lockdown Settings** interface is displayed.

Field	Description
Check Interval	How often the system checks for inactive sessions
Audit Status	Whether the system should track (audit) inactive sessions data ***YES** - Enable auditing ***NO** - Disable auditing **Tip**: Set this flag to ***YES** if you plan to run ISL usage reports.
Audit Journal	Journal in which to store ISL usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about ISL configuration changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** to if you plan to run ISL change reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.
Alert Status	Whether alerts are enabled (stored in the alert queue): ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Temporary Disconnect Message	Custom message defined by the administrator and used to inform the user that their session is about to be locked or ended
Temporary Sign on Screen Header	The title assigned to the message screen that notifies the user of an impending disconnect (e.g., company name)
Send Warning	Whether alerts are sent to warn the user of an impending disconnect ***YES** - Warning alert enabled ***NO** - Warning alert disabled
Warning Interval	When to send the user a warning message (seconds before disconnect)
Revoke Authority	Whether to revoke a user's authority when they are locked or their session is ended ***YES** - The user's session is locked or ended, and the user's authority is revoked ***NO** - The user's session is locked or ended, but the user's authority is maintained **Note**: When a user's authority is revoked, the user is prohibited from performing tasks in any concurrent sessions. In other words, the lockdown is not limited to one session; it impacts all sessions associated with a specific user ID. **Warning**: Consider the workflow consequences thoroughly before enabling this feature.

See also

Working with Inactive Session Lockdown

Manage Inactive Session Lockdown

Use this task to manage the **Inactive Session Lockdown** (ISL) default settings.

Note: To manage Interactive Session Lockdown (ISL) defaults, access from the **Work with Inactive Session Lockdown Settings** interface.

Access the Work with Interactive Session Lockdown Settings Interface

To access the Work with Interactive Session Lockdown Settings interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**. The **Work with Inactive Session Lockdown Settings** interface is displayed.

Enable ISL Auditing

Use this task to enable inactive session auditing.

Tip: Auditing is required if you plan to run ISL usage reports .

To enable the ISL auditing

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Audit Status** field, enter ***YES**.
3) In the **Audit Journal** field, enter the name of the journal in which to store the auditing data.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter** twice. The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Enable ISL Change Auditing

Use this task to enable tracking of configuration changes to inactive session defaults.

Tip: Auditing is required if you plan to run ISL change reports.

To enable tracking of configuration changes in the ISL module

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Audit Configuration Changes** field, enter **Y**.
3) Press **Enter** twice.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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.

Enable ISL Alerts

Use this task to enable ISL alerts.

> **Tip**: Alerting is required if you plan to send alert notifications.

To enable ISL alerts

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter** twice.

Set Check Interval

Use this task to determine how often the system checks for inactive sessions.

To set the check interval

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Check Interval** field, enter the desired time interval in seconds.

> **Note**: This value must be less than or equal to the warning interval.

3) Press **Enter** twice.

Set Warning Interval

Use this task to enable ISL warnings and to determine when the system sends out a warning to the user that their inactive session is about to be terminated.

To set the warning interval

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Send Warning** field, enter one of the following:

– {*}**YES** - Enable the warning feature

– {*}**NO** - Disable the warning feature

3) In the **Warning Interval** field, enter the desired time interval in seconds.

> **Note**: This indicates how much time the user has to perform an action before the inactive session is terminated. This value must be greater or equal to the check interval.

4) Press **Enter** twice.

Set Disconnect Message

Use this task to define the message you want to send to the user warning them that their inactive session is about to be terminated.

To set the disconnect message

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Temporary Disconnect Message** field, enter the desired message.
3) In the **Temporary Sign on Screen Header** field, enter the desired disconnect dialog box heading.
4) Press **Enter** twice.

Set Revoke Authority

Use this task to revoke a user's authority to perform system tasks when inactivity triggers a session lockdown.

> **Warning**: When a user's authority is revoked, the user is prohibited from performing tasks in any concurrent sessions. In other words, the lockdown is not limited to one session; it impacts all sessions associated with a specific user ID.

> **Tip**: Revoking a user's authority can have a serious impact on workflow, depending on the user's level of responsibility and access, so consider the downstream consequences of enabling this feature.

To set the revoke authority

1) Access the **Work with Inactive Session Lockdown Settings** interface.

2) In the **Revoke Authority** field, enter on of the following:

– {*}**YES** - Enable the revoke feature

– {*}**NO** - Disable the revoke feature

3) Press **Enter** twice.

Start Monitor

Use this task to start ISL monitoring.

> **Note**: Once started, the monitor status (which appears in the upper right corner of the screen) should display a status of ***ACTIVE**.

To monitor status

1) Access the **Work with Inactive Session Lockdown Settings** interface.

2) Press F22 (**Start monitor**) function key on your keyboard.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F22, you must hold down the **Shift** key and F10.

3) Press **Enter**.

End Monitor

Use this task to end ISL monitoring.

Note: Once ended, the monitor status (which appears in the upper right corner of the screen) should show status of ***INACTIVE**.

To monitor status

1) Access the **Work with Inactive Session Lockdown Settings** interface.

2) Press F23 (**Stop monitor**) function key on your keyboard.

> **Tip**: For function keys higher than F12, you must use a combination of the Shift key and the appropriate function key. For example, to select F23, you must hold down the Shift key and F11.

3) Press **Enter**.

Check Monitor Status

Use this task to check the status of the monitor. This might be useful during troubleshooting.

To monitor status

1) Access the **Work with Inactive Session Lockdown Settings** interface.

2) Press F21 (**Monitor status**) function key on your keyboard.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F21, you must hold down the **Shift** key and F9.

3) Press **Enter**.

See also

Working with Inactive Session Lockdown

Run Inactive Session Lockdown Reports

Use this task to generate the following **Inactive Session Lockdown** (ISL) reports:

- Run Inactivity Disconnect Report
- Run Inactivity Session Configuration Settings Report
- Run Inactivity Session Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with ISL reports, access from the **Inactivity Session Reports** interface.

To access the Inactivity Session Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Inactive Session Reports).
5) Press **Enter**. The **Inactivity Session Reports** interface is displayed.

Run Inactivity Disconnect Report

Use this report to display the list of instances that triggered a disconnection due to user inactivity.

Tip: ISL monitoring must be started for data to be present in this report. See Manage Inactive Session Lockdown for additional information.

To run the Inactivity Disconnect report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Inactivity Session Usage Reports).
3) Press **Enter**. The **Inactivity Session Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Inactivity Disconnect Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Inactivity Session Configuration Settings Report

Use this report to view the ISL configuration settings.

Tip: You must enable auditing to produce change reports. See Manage Inactive Session Lockdown for additional information.

To run the Inactivity Session Configuration Settings report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
3) Press **Enter**. The **Inactivity Session Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Inactivity Session Configuration Settings).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Inactivity Session Configuration Changes Report

Use this report to view the changes made to the ISL configuration settings.

Tip: ISL Change auditing must be enabled for data to be present in this report. See Manage Inactive Session Lockdown for additional information.

To run the Inactivity Session Configuration Changes report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Changes Reports).
3) Press **Enter**. The **Inactivity Session Changes Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Inactivity Session Configuration Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Inactive Session Lockdown Defaults

Inactive Session Rules

This section describes how to work with **Inactive Session Rules**. Inactive session rules allow you to define when a user is automatically logged out of the system after a period of inactivity. For example, if a user forgets to log out of the system before leaving for lunch, a meeting, or at the end of the day, you can establish an inactivity session rule that will log the user out.

Tip: Any unattended workstations present a security vulnerability. Users should never leave active sessions unattended.

This section includes the following topics:

- Working with Inactive Session Rules
- Display Inactive Session Rules
- Manage Inactive Session Rules
- Run Inactive Session Rules Reports

See also

Inactive Session Lockdown

Working with Inactive Session Rules

Use the **Inactive Session Rules** feature to do the following:

- Display Inactive Session Rules
- Manage Inactive Session Rules
- Run Inactive Session Rules Reports

> **Note**: To work with inactive session rules, you must access the **Working with Inactive Session Rules** interface.

To access the Work with Inactive Session Rules interface

1) Log into to TGSecure. The **Main** menu appears.

2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).

3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Inactive Session Rules).

5) Press **Enter**. The **Work with Inactive Session Rules** interface is displayed.

See also

Inactive Session Rules

Display Inactive Session Rules

Use this task to display inactive session rules.

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of inactive session rules.

To display the list of inactive session rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with Inactive Session Rules).
5) Press **Enter**. The **Work with Inactive Session Rules** interface is displayed.

Field	Description
Rule Type	The type of rule: ***PGM** - Rule that affects a program ***WRKSTN** - Rule that affects a workstation ***SBSD** - Rule that affects a subsystem (e.g., country, region, department, etc.) ***CTL** - Rule that affects a controller ***USER** - Rule that affects a user **Note**: If ***USER** is specified, then the user name or user group should appear in the **Object** field.
Object	Object name or object group to which the rule applies
Library	Library in which the object resides
Calendar	Applicable calendar **Note**: the calendar limits when the rule is applicable.
Disconnect Option	The disconnect option used when the rule is applicable
Rule Action	Whether the rule should be used to include or exclude ***INCLUDE** - Who and what is affected by a rule ***EXCLUDE** - Who and what is not affected by a rule
Rule Description	A short description of the rule

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Inactive Session 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.

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 Inactive Session 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.

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Inactive Session 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.

See also

Working with Inactive Session Rules

Manage Inactive Session Rules

Use this task to manage inactive session rules.

> **Note**: To manage ISL rules, access the **Work with Inactive Session Rules** interface.

Access the Work with Inactive Session Interface

To access the Work with Inactive Session interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Inactive Session Rules).
5) Press **Enter**. The **Work with Inactive Session Rules** interface is displayed.

Add Inactive Session Rule

Use this task to add an inactive session rule.

To add an inactive session rule

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

Field	Description
Rule Type	Enter the type of rule: ***PGM** - Rule that affects a program ***WRKSTN** - Rule that affects a workstation ***SBSD** - Rule that affects a subsystem (e.g., country, region, department) ***CTL** - Rule that affects a controller ***USER** - Rule that affects a user **Note**: If ***USER** is specified, then enter user name or user group the **Object** field.
Object	Enter the object name or object group to which the rule is applicable **Tip**: Enter ***ALL** to apply the rule to all objects, except when **Rule Type** is defined as ***USER**.
Library	Enter the name of the library to which the rule is applicable **Tip**: Leave the field blank to apply to all libraries.
Calendar	Enter the name of the calendar that defines when the rule is applicable **Tip**: Enter ***NONE** if no calendar is applicable.
Disconnect Option	Enter the disconnect option to use when the rule is applicable
Rule Action	Identify whether the rule includes or excludes **{}**INCLUDE* - Who and what is affected by a rule **{}**EXCLUDE* - Who and what is not affected by a rule
Rule Description	Enter a description of the rule

> **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** twice.

Edit Inactive Session Rule

Use this task to edit an existing ISL rule.

To edit an inactive session rule

1) Access the **Work with Inactive Session 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.

Copy Inactive Session Rule

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

To copy an inactive session rule

1) Access the **Work with Inactive Session 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** twice.

Delete Inactive Session Rule

Use this task to delete an ISL k rule.

To delete an inactive session rule

1) Access the **Work with Inactive Session 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** twice.

See also

Working with Inactive Session Rules

Run Inactive Session Rules Reports

Use this task to generate the following inactive session reports:

- Access the Inactive Sessions Report Interface
- Run Inactivity Session Inclusion Exception Rules Report
- Run Inactivity Session Rules Change Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with ISL reports, access from the **Inactive Session Reports** interface.

Access the Inactive Sessions Report Interface

To access the Inactive Sessions Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactive Session Reports).
5) Press **Enter**. The **Inactivity Session Reports** interface is displayed.

Run Inactivity Session Inclusion Exception Rules Report

Use this report to view the list of inclusion exception rules.

Tip: ISL auditing must be enabled to run ISL reports. See Manage Inactive Session Rules for additional information.

To run the Inactivity Session Inclusion Exception Rules report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
3) Press **Enter**. The **Inactivity Session Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Inactivity Session Inclusion Exception Rules).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Inactivity Session Rules Change Report

Use this report to view the changes made to ISL rules.

Tip: You must enable auditing to produce change reports. See Manage Inactive Session Rules for additional information.

To run the Inactivity Session Rules Change report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Changes Reports).
3) Press **Enter**. The **Inactivity Session Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Inactivity Session Rule Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Inactive Session Rules

Disconnection Options

This section describes how to work with **Disconnection Options**. Disconnection options define the methods used to disconnect a user when the user's session is deemed inactive and therefore, vulnerable to attack.

You have choices (and therefore decisions to make) regarding how to disconnect a user when the user's session is deemed to be inactive:

- Disconnect (pause) the job
- Hold (freeze) the job (only an admin can unfreeze a job)
- End the job (user remains logged into the server, but the user must restart the job)
- End the session (user is logged off the server, and the user must restart the session and job)

This section includes the following topics:

- Working with Disconnect Options
- Display Disconnect Options
- Manage Disconnect Options
- Run Disconnect Option Reports

See also

Inactive Session Lockdown

Working with Disconnect Options

Use the **Disconnect Options** feature to do the following:

- Display Disconnect Options
- Manage Disconnect Options
- Run Disconnect Option Reports

> **Note**: To work with disconnect options, you must access the **Working with Disconnect Options** interface.

To access the Work with Disconnect Option interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **3** (Interactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Work with Disconnect Options).
5) Press **Enter**. The **Work with Disconnect Options** interface is displayed.

See also

Disconnection Options

Display Disconnect Options

Use this task to display disconnect options.

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of disconnect options.

To display the list of disconnect options

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Work with Disconnect Options).
5) Press **Enter**. The **Work with Disconnect Options** interface is displayed.

Field	Description
Disconnect Option	Name assigned to the disconnect option
Time Limit	Time the system must remain inactive to trigger the disconnect
Disconnect Type	The type of disconnect: **ENDJOB** - End the job (user must restart their job) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - End the session (user must restart their session and job) **Tip**: If **TGDSCJOB** is defined as the disconnect type, ensure that program **ISL80001P** in library **TGPROD** is defined as the user's initial. To see which program is defined as the initial program for the user, at the **Selection or command** prompt, enter **DSPUSRPRF**. Enter the desired user in the **User Profile** field. Press **Enter**. Page down until you see **Initial Program** and **Library** entries. if ISL80001P is not defined as the initial program, you must either use a different disconnect type or change the user's initial program.

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Disconnect Options** 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.

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 Disconnect Options** 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.

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Disconnect Options** 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.

See also

Working with Disconnect Options

Manage Disconnect Options

Use this task to manage disconnect options.

- Add Disconnect Option
- Edit Disconnect Option
- Copy Disconnect Option
- Delete Disconnect Option

Note: To manage disconnect options, access the **Work with Disconnect Options** interface.

To access the Work with Disconnect Options interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).

3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Work with Disconnect Options).

5) Press **Enter**. The **Work with Disconnect Options** interface is displayed.

Add Disconnect Option

Use this task to add a disconnect option.

To add a disconnect option

1) Access the **Work with Disconnect Options** interface.

2) Press the **F6** (Add) function key on your keyboard.

3) Define the disconnect option using the fields provided.

Field	Description
Disconnect Option	Enter the name you want to assign the disconnect option
Time Limit	Enter the time the system must remain inactive to trigger the disconnect option
Disconnect Type	Enter one of the following: **ENDJOB** - End the job (user must start the job over) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - Signoff from the server **Warnings**: Do not select **HLDJOB** if a trained admin will not be available to unfreeze the job. **Tip**: If you select **TGDSCJOB**, ensure that program **ISL80001P** in library **TGPROD** is defined as the user's initial program. To see which program is defined as the initial program for the user, at the **Selection or command** prompt, enter **DSPUSRPRF**. Enter the desired user in the **User Profile** field. Press **Enter**. Page down until you see **Initial Program** and **Library** entries. if ISL80001P is not defined as the initial program, you must either use a different disconnect type or change the user's initial program.

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** twice.

Edit Disconnect Option

Use this task to edit an existing disconnect option.

To edit a disconnect option

1) Access the **Work with Disconnect Options** 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.

Copy Disconnect Option

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

To copy a disconnect option

1) Access the **Work with Disconnect Options** 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** twice.

Delete Disconnect Option

Use this task to delete a disconnect option.

To delete a disconnect option

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

See also

Working with Disconnect Options

Run Disconnect Option Reports

Use this task to generate the following disconnection option reports:

- Access the Inactive Session Reports Interface
- Run Inactivity Session Disconnect Option Report
- Run Inactivity Session Disconnect Option Change Report

Tips: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with ISL reports, access from the **Inactive Session Reports** interface.

Access the Inactive Session Reports Interface

To access the Inactive Sessions Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**. The **Inactive Session Lockdown** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Inactive Session Reports).
5) Press **Enter**. The **Inactivity Session Reports** interface is displayed.

Run Inactivity Session Disconnect Option Report

Use this report to view the list of disconnect options.

Tip: ISL auditing must be enabled to run ISL reports. See Manage Inactive Session Lockdown for additional information.

To run the Inactivity Session Disconnect Option report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
3) Press **Enter**. The **Inactivity Session Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Inactivity Session Disconnect Options).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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.

Run Inactivity Session Disconnect Option Change Report

Use this report to view changes made to ISL disconnection options.

Tip: You must enable auditing to produce change reports. See Manage Inactive Session Lockdown for additional information.

To run the Inactivity Session Disconnect Option Change report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Changes Reports).
3) Press **Enter**. The **Inactivity Session Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Inactivity Session Disconnect Option Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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.

See also

Working with Disconnect Options

Resource Manager

Use the **Resource Manager** feature to manage object-level security using authority schemas. Think of an authority schema as a template that defines authority best practices. Once you create an authority schema, you can use it to evaluate and modify the authority levels of multiple users.

To access the Resource Manager interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Use the **Resource Manager** interface to do the following:

- Working with Resource Manager Defaults
- Working with Authority Schemas
- Working with Authority Collections

See also

Getting Started

Resource Manager Defaults

This section describes working with **Resource Manager** defaults.

Resource Manager defaults allow you to define the following:

- Whether to send resource change alerts
- Whether to track resource changes (required if you plan to run reports)
- Journal in which to store resource changes
- Library in which to store resource changes
- Queue in which to store resource alerts
- Queue library in which to store resource alerts

This section includes the following topics:

- Working with Resource Manager Defaults
- Display Resource Manager Defaults
- Manage Resource Manager Defaults
- Run Resource Manager Reports

See also

Resource Manager

Working with Resource Manager Defaults

Use the **Resource Manager Defaults** settings to do the following:

- Display Resource Manager Defaults
- Manage Resource Manager Defaults
- Run Resource Manager Reports

> **Note**: To work with the Resource Manager, you must access the **Resource Manager Defaults** interface.

To access the Resource Manager interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**. The **Resource Manager Defaults** interface is displayed.

See also

Resource Manager Defaults

Display Resource Manager Defaults

Use this task to display the **Resource Manager** default settings.

To display the Resource Manager defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**. The **Resource Manager Defaults** interface is displayed.

Field	Description
Audit Journal	Journal in which to store resource manager usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library. **Tip**: The Audit Journal and Library fields must be filled with a valid value if you plan to run Resource Manager usage reports.
Audit Journal Library	Library in which the audit journal resides
Audit Configuration Changes	Whether to collect data about resource changes: **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run the Resource Manager change reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue

See also

Working with Resource Manager Defaults

Manage Resource Manager Defaults

Use this task to manage the **Resource Manager** default settings.

- Access the Resource Manager Defaults Interface
- Enable Resource Change Auditing
- Enable Resource Change Alerts

Note: To manage Resource Manager defaults, access the **Resource Manager Defaults** interface.

Access the Resource Manager Defaults Interface

To access the Resource Manager Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**. The **Resource Manager Defaults** interface is displayed.

Enable Resource Change Auditing

Use this task to enable resource change auditing.

Tip: Auditing is required if you plan to run resource manager change reports .

To enable the resource auditing

1) Access the **Resource Manager Defaults** interface.
2) In the **Audit Configuration Change** field, enter **Y**.
3) In the **Audit Journal** field, enter the name of the journal in which to store changes.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter**.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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

Enable Resource Change Alerts

Use this task to enable inactive session alerts.

Tip: Alerting is required if you plan to send alert notifications.

To enable resource alerts

1) Access the **Resource Manager Defaults** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

See also

Working with Resource Manager Defaults

Run Resource Manager Reports

Use this task to generate the following **Resource Manager** reports:

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Resource Manager reports, access from the **Resource Manager Reports** interface.

Access the Resource Manager Reports Interface

To access the Resource Manager Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**. The **Resource Manager Reports** interface is displayed.

Run Resource Manager Configuration Report

Use this report to view the Resource Manager configuration details.

To run the Resource Manager Configuration Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Resource Manager Configuration).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Resource Manager Configuration Change Report

Use this report to view changes made to the Resource Manager configuration details.

Tip: You must enable auditing to produce change reports. See Manage Resource Manager Defaults for additional information.

To run the Resource Manager Configuration Change Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**. The **Resource Manager Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Resource Manager Configuration Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

Run Resource Manager Out of Compliance Data

Use this report to view user authorities that are deemed out of compliance based on a defined authority schema.

To run the Resource Manager Out of Compliance Report

1) Access the **Resource Manager Reports** interface.

2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).

3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Out of Compliance Data).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

Run Resource Manager Out of Compliance Data Changes Report

Use this report to view changes made to user authorities that are deemed out of compliance based on a defined authority schema.

To run the Resource Manager Out of Compliance Data Changes Report

1) Access the **Resource Manager Reports** interface.

2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).

3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Out of Compliance Data Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

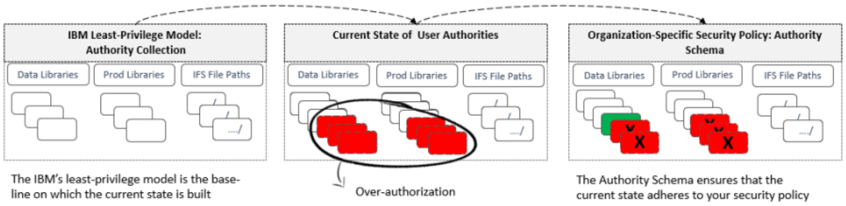
See also

Working with Resource Manager Defaults

Authority Schemas

Use the **Authority Schemas** feature to define an architecture (template) for granting user authorities. Each authority scheme is the ideal model of how your organization should implement user authorities. Therefore, each authority schema should be unique to an organization and be based on a well-defined security policy.

The following is the process used to define and implement authorities schemas:



This section includes the following topics:

- Working with Authority Schemas
- Display Authority Schemas
- Manage Authority Schemas
- Run Authority Schema Reports

See also

Resource Manager

Working with Authority Schemas

Use the **Authority Schemas** feature to do the following:

- Display Authority Schemas
- Manage Authority Schemas
- Run Authority Schema Reports

> **Note**: To work with authority schemas, you must access the **Working with Authority Schemas** interface.

To access the authority schemas interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (**Authority Schema Configuration**).
5) Press **Enter**. The **Work with Authority Schemas** interface is displayed.

See also

Authority Schemas

Display Authority Schemas

Use this task to display the authority schemas.

Display List of Schemas

Use this task to display the list of available authority schemas.

To display the list of authority schemas

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**. The **Work with Authority Schemas** interface is displayed.

Field	Description
Schema ID	ID assigned to the schema
Compliances	Date and time at which the last check for authority schema compliance was performed
Enforcement	Date and time at which user authorities were compared to the authority schema and compliance with the schema was enforced
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alerts) ***NO** - Disable alerts
Schema Description	Description of the authority schema
Compliance Status	Whether the current authority levels comply with the schema ***PASS** - User authorities comply with the current authority scheme ***FAIL** - User authorities do not comply with the current authority scheme **Note**: See Manage Authority Scheme for instruction on enforcing an authority schema.

Sort List of Schemas

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

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

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

Move to Position in List of Schemas

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 Authority Schemas** 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.

Filter List Schemas

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

> **Tip**: Use wildcard asterisk to help define your subset.
>
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
>
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
>
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Authority Schemas** interface.
2) Press the **F8** (Subset) function key on your keyboard.
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.

Display List of Schemas Details

Use this task to display the list of available schema details and exceptions.

To display the list of authority schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**. The **Work with Authority Schema Details** interface is displayed.

Field	Description
File Sys	File system to monitor
Path or ASP	File path or ASP to monitor
Library	Library to monitor
Object Name	Object name to monitor
Object Type	Object type to monitor
Object Owner	Name of the object owner
Auth List	Name of the authority list **Note**: An authority list displays the users who have authority to specific objects.
User Object	Name of the user (or group) that has access to the object
Auth	User or group authority level: ***ALL** - All authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Change authority ***EXCLUDE** - Prohibit the user from performing operations on the object ***USE** - Allow the user to use the object (but not change it) ***AUTL** - Default level of authority defined for public users (*PUBLIC)
Exception	Whether excepts are defined ***YES** - This entry is an exception to the default rules for this schema ***NO** - This entry is a default rule for this schema **Note**: Exceptions are defined as schema details.

Sort List of Schemas Details

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

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

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

Move to Position in List of Schemas Details

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 Authority Schemas** 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.

Filter List Schemas Details

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 Authority Schemas** interface.
2) Press the **F8** (Subset) function key on your keyboard.
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.

See also

Working with Authority Schemas

Manage Authority Schemas

Use this task to manage authority schemas.

- Access the Work with Authority Schema Interface
- Add Authority Schema
- Edit Authority Schema
- Copy Authority Schema
- Delete Authority Schema
- Enabling Authority Schema Alerting
- Disable Authority Schema Alerting
- Limit Scope of Authority Schema to System Libraries (SYS)
- Limit Scope of Authority Schema to Integrated File System (IFS)
- Change Scope of Authority Schema (Object or IFS)
- Add Schema Details
- Edit Schema Details
- Copy Schema Detail
- Delete Schema Detail
- Display Authority Schema Compliance Issues
- Enforce Authority Schema

Note: To manage authority schemas, access the **Work with Authority Schemas** interface.

Access the Work with Authority Schema Interface

To access the Work with Authority Schemas interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**. The **Work with Authority Schemas** interface is displayed.

Add Authority Schema

Use this task to add an authority schema.

To add an authority schema

1) Access the **Work with Authority Schemas** interface.
2) Press the **F6** (Create) function key on your keyboard.
3) Complete the following fields.

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.

Field	Description
Schema ID	ID you want to assign to the schema
Schema Description	Text describing the purpose of the schema
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alerts) ***NO** - Disable alerts
Include IFS or Library Object	Which structures to check: ***SYS** - Enable check only in system libraries ***IFS** - Enable check only in Integrated File System (IFS). **Note**: IFS is a newer file management structure that supports stream input/output and is similar to the structure used by personal computers and UNIX operating systems. For more information about IBM file systems, refer to the IBM Knowledge Center. ***ALL** - Enable check-in (both SYS and IFS) ***NO** - Disable check-in

Field	Description
Filter Details	Whether data is filtered: ***NONE** - Data is not filtered **Filter name** - Enter the filter name or press F4 to select from a list.
IFS Depth	Depth of IFS Folder to include: 00-99 - Depth level **Tip:** Enter 00 to include only the IFS Scope directory level.

4) Define the object scope for library (SYS) objects by completing the following fields:

> **Note**: The values you enter in the following fields limit the scope of the schema to a single object or an object group.

Field	Description
Object Name	Enter a specific object name or object group to which this schema applies You can also choose one of the following options: ***NONE** - No objects ***ALL** - All objects **Tip:** You can skip this field for IFS files.
Object Library	Enter the name of the library to which this authority schema applies or enter ***ALL** to include all libraries **Tip:** You can skip this field for IFS files.
Object Type	Enter the object type to which this authority schema applies or enter ***ALL** to include all object types **Tip:** You can skip this field for IFS files.
Path or ASP Name	Do one of the following: – Enter the file path for the IFS or – Enter the ASP (Auxiliary Storage Pool) for the system libraries **Note**: If you enter ***SYSBAS**, the system ASP and all basic user ASPs are included.

5) Define the authorities by completing the following fields:

> **Note**: The values you enter in the following fields define the recommended object authority settings for the object or object group associated with the schema.

Field	Description
Object Owner	Enter the name of the object owner
Authorization List	Enter the name of the authority list to which this authority schema applies, or enter ***NONE** if not applicable **Note**: An authority list displays the users who have the authority to access a specific object.
Object Primary Group	Enter the name of the primary group to which the object belongs or enter ***NONE** if not applicable
Adopt User Profile	Enter the name of the user profile to adopt when the schema is enforced
Adopt Authority	Whether to allow the ability to adopt authority: ***YES** - Enable the program to adopt the authorities from the previous program ***NO** - Disable the program from adopting the authorities from the previous program

6) Define the user authorities by completing the following fields:

> **Note**: The values you enter in the following fields define the recommended user authority settings for the user or user group associated with the schema.

Field	Description
User Name	Enter the user's name
*Public Authority	Enter the authority level you want to assign to public users (*Public): **Note:** Public users do not have the following: – They do not have specific authority to use the function – They do not appear on the authorization list – They are not members of a user group that has specific authority to the object Select the level of authority you want to grant public users: ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant public users change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object) ***AUTL** - Grant public users the default level of authority specified for the authority list

7) Press **Enter** twice.

Edit Authority Schema

Use this task to edit an existing authority schema.

To edit an authority schema

1) Access the Work with Authority Schemas interface.
2) In the **OPT** column for the desired schema, 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.

Copy Authority Schema

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

To copy an authority schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, 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**.

Delete Authority Schema

Use this task to delete an authority schema.

To delete an authority schema

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

Enabling Authority Schema Alerting

Use this task to enable alerting.

To enable/disable authority schema alerting

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter ***YES** to enable alerting.

Disable Authority Schema Alerting

Use this task to disable alerting.

To enable/disable authority schema alerting

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter ***NO** to disable alerting.

Limit Scope of Authority Schema to System Libraries (SYS)

Use this task to limit the scope of an authority schema to only address system libraries (SYS).

To limit the scope of the schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Include IFS or Library Object** field, enter ***SYS**.

Limit Scope of Authority Schema to Integrated File System (IFS)

Use this task to limit the scope of an authority schema to only address the Integrated File System (IFS).

To limit the scope of the schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Include IFS or Library Object** field, enter ***IFS**.

Change Scope of Authority Schema (Object or IFS)

Use this task to change the scope of an authority schema.

To change the scope of the schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **12** (Edit).
3) Press **Enter**. The **Change Scope (Object or IFS)** interface is displayed.
4) Updated the following fields as necessary:

Field	Description
File Type	Enter the appropriate file type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center.
Object Name	Enter a specific object name or object group to which this schema applies You can also choose one of the following options: ***NONE** - No objects ***ALL** - All objects **Tip:** You can skip this field for IFS files.
Object Type	Enter the object type to which this authority schema applies, or enter ***ALL** to include all object types **Tip:** You can skip this field for IFS files.
Object Library	Enter the name of the library to which this authority schema applies, or enter ***ALL** to include all libraries **Tip:** You can skip this field for IFS files.
ASP Name	Do one of the following: – Enter the file path for the IFS or – Enter the ASP (Auxiliary Storage Pool) for system libraries **Note**: If you enter ***SYSBAS**, the system ASP and all basic user ASPs are included.

Add Schema Details

Use this task to add an authority schema details. The details are the exceptions that are allowed.

To add an authority schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**. The **Work with Authority Schema Details** interface is displayed.
4) Press the **F6** (Create) function key on your keyboard.
5) Complete the following fields.

Field	Description
Schema ID	ID assigned to the schema (not editable)
Schema Description	Text describing the purpose of the schema (not editable)
File Type	Enter the appropriate file type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center.
Object Owner	Enter the name of the object owner
Authorization List	Enter the name of the authority list to which this authority schema applies, or enter ***NONE** if not applicable
Object Primary Group	Enter the name of the object primary group to which this authority schema applies or enter ***NONE** if not applicable
User Name	Enter the name of the user (or group) to which the exception applies or enter ***PUBLIC** to apply to all users.
Object Authority	Enter the authority level: ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant public users change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (changes to object not allowed) ***AUTL** - Grant public users the public authority specified in the authority list

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.

6) Press **Enter** twice.

Edit Schema Details

Use this task to edit schema details.

To edit schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**. The **Work with Authority Schema Details** interface is displayed.
4) In the **OPT** column for the desired schema, enter **2** (Edit).
5) Press **Enter**.
6) 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.

7) Press **Enter** twice.

Copy Schema Detail

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

To copy schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**. The **Work with Authority Schema Details** interface is displayed.
4) In the **OPT** column for the desired schema, enter **3** (Copy).
5) Press **Enter**.
6) 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.

7) Press **Enter**.

Delete Schema Detail

Use this task to delete a schema detail.

To delete a schema detail

1) Access the **Work with Authority Schemas** interface.

2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).

3) Press **Enter**. The **Work with Authority Schema Details** interface is displayed.

4) In the **OPT** column for the desired schema, enter **4** (Delete).

5) Press **Enter**.

6) Review the record to ensure you are deleting the correct schema.

7) Press **Enter** twice.

Display Authority Schema Compliance Issues

Use this task to display authority schema compliance issues.

Tip: Run this task before you attempt to enforce authority schema to determine if exceptions (details) are required (see Add Schema Details).

To display authority schema compliance issues

1) Access the **Main** menu.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).

5) Press **Enter**.

6) Complete the following fields.

Field	Description
Scheme ID	ID assigned to the scheme you want to analyze for compliance
Audit report	Enter *__YES__ to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter *__NO__ to display only (not enforce) compliance issues **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: *__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) Press **Enter**.

Enforce Authority Schema

Use this task to enforce an authority schema.

Tip: Before enforcing an authority schema, first identify where non-compliance is occurring (see Display Authority Schema Compliance Issues). In some cases, an issue of non-compliance might identify an exception (authority detail) that must be added. In other words, you might need to update the scheme.

To enforce authority schemas

1) Access the **Main** menu.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).

5) Press **Enter**.

6) Complete the following fields.

Field	Description
Scheme ID	ID assigned to the scheme you want to analyze for compliance
Audit report	Enter *__YES__ to enable auditing (tracking)
Enforcement	Enter *__YES__ to enforce the schema
Run interactively	Whether to run interactively or add to batch: *__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) Press **Enter**.

See also

Working with Authority Schemas

Run Authority Schema Reports

Use this task to generate the following authority schema reports:

- Access the Resource Manager Reports Interface
- Run Resource Manager Schema Details Report
- Run Resource Manager Schema Details Changes Report
- Run Resource Manager Schema Header Changes Report
- Run Authority Schema Compliance Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Resource Manager reports, access from the **Resource Manager Reports** interface.

Access the Resource Manager Reports Interface

To access the Inactive Sessions Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**. The **Resource Manager Reports** interface is displayed.

Run Resource Manager Schema Details Report

Use this report to view the list of details (exceptions) associated with each authority schema.

To run the Resource Manager Schema Details Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Resource Manager Schema Details Changes Report

Use this report to view the list of changes made to the details (exceptions) associated with each authority schema.

Tip: You must enable auditing to produce change reports. See Manage Resource Manager Defaults for additional information.

To run the Resource Manager Schema Details Changes Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Resource Manager Schema Header Report

Use this report to display the list of schema headers.

To run the Resource Manager Schema Header Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Resource Manager Schema Header Changes Report

Use this report to display the list of changes to schema headers.

To run the Resource Manager Schema Header Changes Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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**. The status of the report is displayed at the bottom of the screen.

Run Authority Schema Compliance Report

Use this task to display authority schema compliance issues.

Tip: Run this task before you attempt to enforce an authority schema to determine if exceptions (details) are required (see Add Schema Details).

To run the authority schema compliance report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).
5) Press **Enter**.
6) Complete the following fields.

Field	Description
Scheme ID	ID assigned to the scheme you want to analyze for compliance
Audit report	Enter ***YES** to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***NO** to display (not enforce) compliance issues. **Tip**: Always display and investigate before enforcing.

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) Press **Enter**.

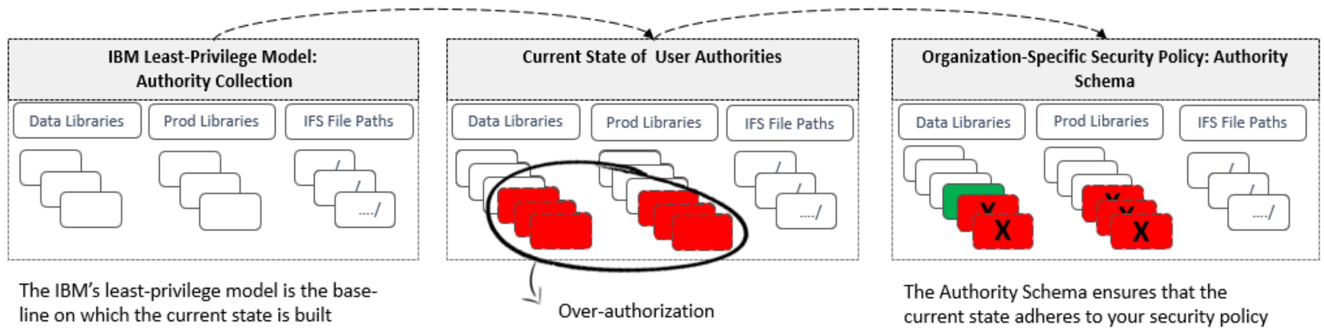
See also

Working with Authority Schemas

Authority Collections

This section describes working with the authority collections to compare IBM's least-privileges model with your current authority state in order to help define an authority schema that best meets the security needs of your organization.

Tip: It's good practice is to compare IBM's least privilege model with your current authority state to determine if a user has been granted more authority than necessary. This helps you to eliminate unnecessary over-authorization.



This section includes the following topics:

- Working with Authority Collections
- Display Authority Collection Configuration
- Manage Authority Collection Configuration
- Run Authority Collection Reports

See also

Resource Manager

Working with Authority Collections

Use the **Authority Collection** feature to do the following:

- Display Authority Collection Configuration
- Manage Authority Collection Configuration
- Run Authority Collection Reports

Note: To work with authority collections, you must access the **Work with Authority Collection Configuration Users** interface.

To access the Work with Authority Collection Configuration Users interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**. The **Work with Authority Collection Configuration Users** interface is displayed.

See also

Authority Collections

Display Authority Collection Configuration

Use this task to display the authority collection configuration details.

- Display List of Authority Collections
- Display Authority Collection Details

Display List of Authority Collections

Use this task to display the list of authority collections.

Important: Authority collection is only available with OS IBM i 7.3. or higher.

To display the list of authority collections

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**. The **Work with Authority Collection Configuration Users** interface is displayed.

Field	Description
User	Name of the user
Collection Active	Whether user authority data is collected: **YES** - Collection enabled (started) **NO** - Collection disabled (ended)
Repository Exists	Whether a repository exists for the storage of authority data: **YES** - Repository exists **NO** - Repository does not exist

Display Authority Collection Details

To display the authority collection configuration details

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Authority Collection Configuration).
5) Press **Enter**. The **Work with Authority Collection Configuration** interface is displayed.
6) In the **OPT** column for the desired authority collection, enter **5** (Display Collection Details).
7) Press **Enter**. The **Display Collection Details** interface is displayed.

Field	Description
User profile	Name of the user for which authority data is being collected
Library	Name of the library monitored, or one of the following: ***NONE** - Exclude libraries ***ALL** - Include all libraries
ASP Device	Name of the ASP device or ***SYBAS**
Object	Name of the object or one of the following: generic* - First few letters of an object name followed by an asterisk (wildcard) This indicates that all object that begins with the letters identified are to be included. ***ALL** - Include all objects
Object type	Name of the object type or one of the following: ***ALL** - Include all object types
Include DLO	Identifies the document libraries to include: ***NONE** - Exclude document library objects ***ALL** - Include all document library objects (*DOC and *FLR) ***DOC** - include only documents ***FLR** - Include only folders

Field	Description
Include file system objects	Identifies the file system objects to include: ***NONE** - Exclude file system objects ***ALL** - Include all file system objects ***BLKSF** - Include only block files ***CHRSF** - Include only character files ***DIR** - Include only directories ***FIFO** - Include only first-in-first-out special files ***SOCKET** - Include only socket files ***STMF** - Include only steam files ***SYMLNK** - Include only symbolic links
Delete collection	Whether to store or dispose of the collection ***NO** - Dispose ***YES** - Store
Detail	What level of detail should be collected ***OBJINF** - Collect authority details for each unique instance of the object-level information ***OBJJOB** - Collect authority details for each unique instance of the object-level information and each unique instance of the job

See also

Working with Authority Collection

Manage Authority Collection Configuration

Use this task to manage the authority collection configuration details.

- Access the Authority Collection Users Interface
- Start Authority Collection
- End Authority Collection
- Delete Authority Collection

ⓘ **Note**: To manage authority collections, access the **Work with Authority Collection Users** interface.

Access the Authority Collection Users Interface

To access the Work with Authority Collection Users interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**. The **Work with Authority Collection Users** interface is displayed.

Start Authority Collection

Use this task to add an authority collection.

To add an authority collection

1) Access the **Work with Authority Collections Users** interface.
2) Press the **F6** (Start Collection) function key on your keyboard.
3) Complete the following fields.

Field	Description
User profile	Name of the user for which you want to begin collecting authority data
Library	Name of the library you want to monitor or enter one of the following: ***ALL** - Include all libraries ***NONE** - Exclude all libraries
ASP Device	Name of the ASP device or ***SYSBAS**
Object	Name of the object or one of the following: generic* - First few letters of an object name followed by an asterisk (wildcard). This indicates that all objects that begin with the letters identified are to be included. ***ALL** - Include all objects
Object type	Name of the object type or one of the following: ***ALL** - Include all object types
Include DLO	Identifies the document libraries to include: ***ALL** - Include all document library objects (*DOC and *FLR) ***DOC** - include only documents ***FLR** - Include only folders ***NONE** - Exclude document library objects
Include file system objects	Identifies the file system objects monitored: ***ALL** - Include all file system objects ***BLKSF** - Include only block files ***CHRSF** - Include only character files ***DIR** - Include only directories ***FIFO** - Include only first-in-first-out special files ***SOCKET** - Include only socket files ***STMF** - Include only steam files ***SYMLNK** - Include only symbolic links ***NONE** - Exclude file system objects
Delete collection	Whether to store or dispose of the collection ***NO** - Dispose ***YES** - Store
Detail	What level of detail should be collected ***OBJINF** - Collect authority details for each unique instance of the object-level information ***OBJJOB** - Collect authority details for each

Field	Description
	unique instance of the object-level information and each unique instance of the job

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** twice.

End Authority Collection

Use this task to end an authority collection.

To edit an authority collection

1) Access the **Work with Authority Collections Users** interface.
2) In the **OPT** column for the desired schema, enter **3** (End Collection).
3) Press **Enter**.
4) Review the record to ensure you are ending the correct collection.

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.

Delete Authority Collection

Use this task to delete an authority collection.

To delete an authority collection

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

See also

Working with Authority Collection

Run Authority Collection Reports

Use this task to generate the following authority configuration reports:

- Access the Resource Manager Reports Interface
- Run Authority Compliance Report (Single Schema)
- Run Authority Compliance Report (All Schemas)
- Run Authority Collection Report (QSYS)
- Run Authority Collection Report (IFS)

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with authority collection reports, access from the **Resource Manager Reports** interface.

Access the Resource Manager Reports Interface

To access the Resource Manager Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**. The **Resource Manager Reports** interface is displayed.

Run Authority Compliance Report (Single Schema)

Use this report to identify compliance issues with your authority schema(s). You can use this report to identify two states:

- Instances in which your authority scheme is being enforced (i.e., in compliance with your schema)
- Instances in which your authority scheme is not being enforced (i.e., out of compliance with your schema)

To run the Authority Compliance report for all schemas

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**. The **Resource Manager** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**. The **Work with Authority Schemas** interface is displayed.
6) In the **OPT** column for the desired schema, enter **22** (Run Compliance Report).
7) Press **Enter**.
8) In the **Audit report** field, enter ***YES**.
9) Enter the desired output format in the **Report output type** field.
10) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Authority Compliance Report (All Schemas)

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

Use this report to identify compliance issues with your authority schema(s). You can use this report to identify two states:

- Instances in which your authority scheme is being enforced (i.e., in compliance with your schema)
- Instances in which your authority scheme is not being enforced (i.e., out of compliance with your schema)

To run the Authority Compliance report for all schemas

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).
3) Press **Enter**. The **Resource Manager Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Authority Compliance Report).
5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

Run Authority Collection Report (QSYS)

Use this task to generate the authority collection report for QSYS.

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

To run the Authority Collection report (QSYS)

1) Access the **Resource Manager Reports** interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **3** (Authority Collection Report - QSYS).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

Run Authority Collection Report (IFS)

Use this task to generate the authority collection report for the Integrated File System (IFS).

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

To run the Authority Collection report (IFS)

1) Access the **Resource Manager Reports** interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **2** (Authority Collection Report - IFS).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Authority Collection

User Profile Management

Use the **User Profile Management** feature to manage user profiles using blueprints. Think of a blueprint as a template that defines user profile best practices. Once you create a blueprint, you can use it to evaluate, create, or modify user profiles.

To access the User Profile Manager interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Manager).
3) Press **Enter**.

Use the **User Profile Management** interface to do the following:

- Work with profile manager defaults
- Work with blueprints
- Work with user exclusions
- Work with archived profiles
- Work with inactive profiles
- Work with user profiles
- Work with password rules

See also

Getting Started

Profile Management Defaults

This section describes how to work with **User Profile Management Defaults**.

User Profile Manager defaults allow you to define the following:

- Whether to send profile change alerts
- Whether to track profile changes (required if you plan to run reports)
- Journal in which to store profile changes
- Library in which to store profile changes
- Queue in which to store profile alerts
- Queue library in which to profile alerts

This section includes the following topics:

- Display User Profile Management Defaults
- Manage User Profile Management Defaults
- Run User Profile Management Reports
- Working with User Profile Management Defaults

See also

User Profile Management

Working with User Profile Management Defaults

Use the **Profile Manager Defaults** interface to do the following:

- Display User Profile Management Defaults
- Manage User Profile Management Defaults
- Run User Profile Management Reports

Note: To work with profile manager defaults, you must access the **Profile Management Defaults** interface.

To access the User Profile Management Defaults interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **7** (User Profile Management Defaults).
5) Press **Enter**. The **User Profile Manager Defaults** interface is displayed.

See also

User Profile Management

Display User Profile Management Defaults

Use this task to display the **User Profile Management** default settings.

To display the User Profile Manager defaults

1) Access the TGSecure **Main** menu.

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

3) Press **Enter**. The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Profile Manager Defaults).

5) Press **Enter**. The **User Profile Management Defaults** interface is displayed.

Field	Description
Audit Journal	Journal in which to store profile manager usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Indicates whether to track profile changes: **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run usage reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules
Alerting Status	Indicates whether alerts are enabled: ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Archive User Profile	Indicates whether to archive inactive profiles: ***YES** - Create an archive ***NO** - Do not create an archive **Tip**: For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met: a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.) b. The user profile is associated with a blueprint c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion
Archive Profiles Retention (Days)	Number of days an archived profile is retained by the system
Exit Programs Installed	Indicates whether the exit programs necessary for profile management (including archiving) are installed: ***YES** - The exit programs that support user profile management are installed ***NO** - The exit programs that support user profile management are uninstalled **Note**: See Manage Profile Manager Defaults for instruction on adding exit programs.

See also

Working with User Profile Management Defaults

Manage User Profile Management Defaults

Use this task to manage the **User Profile Management** default settings.

ⓘ **Note**: To manage Profile Manager defaults, access the **User Profile Management Defaults** interface.

Accessing the User Profile Management Defaults Interface

To access the User Profile Management Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **7** (User Profile Management Defaults).
5) Press **Enter**. The **User Profile Management Defaults** interface is displayed.

Edit User Profile Manager Settings

Use this task to edit profile auditing settings

To edit profile manager settings

1) Access the **User Profile Management Defaults** interface.
2) Modify the following fields as necessary.

Field	Description
Audit Journal	Journal in which to store profile manager usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Indicates whether to track profile changes: **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run usage reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules
Alerting Status	Indicates whether alerts are enabled: ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Archive User Profile	Indicates whether to archive inactive profiles: ***YES** - Create an archive ***NO** - Do not create an archive **Tip**: For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met: a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.) b. The user profile is associated with a blueprint c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion

Field	Description
Archive Profiles Retention (Days)	Number of days an archived profile is retained by the system
Archive Method	Indicates the method used to archive inactive profiles: ***SAVSEC** - Save user profile data using SAVSECDTA command ***SAVPRF** - Save user profile data to a database file **Tip**: Using ***SAVSEC** option is slower, restore from archive option will run **RSTUSRPRF** command, whereas using ***SAVPRF** is faster, restore option will run **CRTUSRPRF** command.
Exit Programs Installed	Indicates whether the exit programs necessary for profile management (including archiving) are installed: ***YES** - The exit programs that support user profile management are installed ***NO** - The exit programs that support user profile management are uninstalled **Note**: See Manage Profile Manager Defaults for instruction on adding exit programs.

3) Press **Enter**.

Enable Profile Auditing

Use this task to enable profile change auditing.

> **Tip**: Auditing is required if you plan to run profile change reports.

To enable profile auditing

1) Access the **User Profile Management Defaults** interface.
2) In the **Audit Journal** field, enter the name of the journal in which to store changes.
3) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
4) In the **Audit Configuration Change** field, enter **Y**.
5) Press **Enter**.

> **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules

Enable Profile Alerts

Use this task to enable profile change alerts.

> **Tip**: Alerting is required if you plan to send alert notifications.

To enable profile alerts

1) Access the **User Profile Management Defaults** interface.
2) In the **Alerting Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

Enable Profile Archiving

Use this task to enable archiving of inactive user profiles.

> **Tip**: The exit programs are required (must be installed) if you plan to use the Program Manager feature.

To enable profile archiving

1) Access the **User Profile Management Defaults** interface.
2) In the **Archive User Profile** field, enter ***YES**.
3) In the **Archive Profiles Retention** field, enter the number of days the archived should be retained.
4) Press **Enter**.

Add Profile Exit Programs

Use this task to add (install) the User Profile Management exit program.

Tip: This exit program is required to enable Program Manager features.

To add Profile Manager exit programs

1) Access the **User Profile Management Defaults** interface.
2) Press the **F20** (Add Exit Program) function key on your keyboard.

Remove Profile Exit Programs

Use this task to remove (uninstall) the User Profile Management exit program.

Tip: The exit program is required to enable Program Manager features.

To remove profile exit programs

1) Access the **User Profile Management Defaults** interface.
2) Press the **F21** (Remove Exit Program) function key on your keyboard.

See also

Working with User Profile Management Defaults

Display User Profile Management Defaults

Run User Profile Management Reports

Use this task to generate the following **User Profile Manager** reports:

- Access the User Profile Reports Interface
- Run User Profile Management Defaults Report
- Run User Profile Management Defaults Changes Report

Tip: You can schedule the Profile Manager Default reports (like all other reports) to run when most convenient.

Note: To work with Profile Manager Default reports, access from the **User Profile Reports** interface.

Access the User Profile Reports Interface

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**. The **User Profile Reports** interface is displayed.

Run User Profile Management Defaults Report

To run the User Profile Manager Default Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Profile Manager Defaults).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run User Profile Management Defaults Changes Report

Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the Profile Manager Default Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **11** (Profile Manager Defaults Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

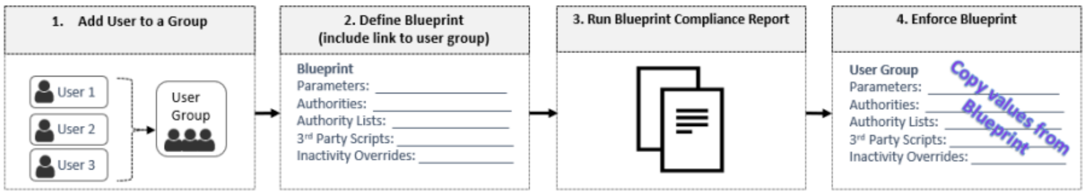
See also

Working with User Profile Management Defaults

Blueprints

This section describes how to work with **Blueprints**. Blueprints allow you to design a 'template' by which to create new user profiles. In addition, you can use a blueprint to perform a mass update to all profiles assigned to a specific user group. To determine if the profiles within a user group conform to a blueprint, run the blueprint compliance report. The report identifies any discrepancies. You can then enforce a blueprint to eliminate the discrepancies (modify the user profiles within a group to 'match' the blueprint).

The following is the process used to define and implement blueprints:



This section includes the following topics:

- Working with Blueprints
- Display Blueprints
- Manage Blueprints
- Run Blueprint Reports

See also

User Profile Management

Working with Blueprints

Use the **Blueprint** feature to do the following:

- Display Blueprints
- Manage Blueprints
- Run Blueprint Reports

> **Note**: To work with blueprints, you must access the **Work with Blueprints** interface.

To access the Work with Blueprint interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Blueprints).
5) Press **Enter**. The **Work with Blueprints** interface is displayed.

See also

Blueprints

Display Blueprints

Use this task to display blueprints.

- Display List of Blueprints
- Sort List of Blueprint
- Move to Position in List of Blueprints
- Filter List Blueprint

Display List of Blueprints

Use this task to display the list of available blueprints.

To display the list of blueprints

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Blueprints).
5) Press **Enter**. The **Work with Blueprints** interface is displayed.

Field	Description
Blueprint ID	ID assigned to the blueprint
User Group	Name of user group to which the blueprint applies
Prf Parm	Whether parameters are defined: ***YES** - One or more profile parameters are defined for the blueprint ***NO** - No profile parameters are defined
Prf Auth	Whether object authorities are defined: ***YES** - One or more object authorities are defined for the blueprint ***NO** - No object authorities are defined
Auth List	Whether authority lists are defined: ***YES** - One or more authority lists are defined for the blueprint ***NO** - No object authorities are defined
3rd Party	Whether 3rd party scripts are defined: ***YES** - One or more 3rd party scripts are defined for the blueprint ***NO** - No 3rd party scripts are defined
Alt Sts	Whether alerts are enabled: ***YES** - Alerts enabled (create admin alerts) ***NO** - Alerts disabled
Compliance Date	Date on which blueprint compliance and profile inactivity check was last performed
Compliance Time	Time at which blueprint compliance and profile inactivity check was last performed
Inact Ovr	Whether inactivity overrides are enabled: ***YES** - Overrides are enabled ***NO** - Overrides disabled
Inact Prf?	Whether inactive profiles exist (according to last report run): **Y** - Inactive profile were found (consider running enforcement) **N** - Inactive profiles were not found
Comp Status	Whether the current authority levels comply with the blueprint **PASS** - User authorities comply with the current blueprint **FAIL** - User authorities do not comply with the current blueprint
Blueprint Description	Description of the blueprint

Sort List of Blueprint

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Blueprint** 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.

Move to Position in List of Blueprints

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

Filter List Blueprint

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Blueprint** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

See also

Working with Blueprints

Manage Blueprints

Use this task to generate the following blueprint reports:

> **Note**: To manage blueprints, access the **Work with Blueprints** interface.

Access the Work with Blueprints Interface

To access the Work with Blueprints interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Blueprints).
5) Press **Enter**. The **Work with Blueprints** interface is displayed.

Add Blueprint

Use this task to add a blueprint. There a number of details that need to be included in each blueprint, so a wizard has been designed to help you complete this multi-step process.

> **Tip**: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 1: Add Blueprint Details

To add blueprint details

1) Access the **Work with Blueprints** interface.
2) Press the **F6** (Add Wizard) function key on your keyboard. The **Blueprint - Add** interface is displayed.
3) Complete the following fields.

Field	**Description**
Blueprint ID	ID you want to assign to the blueprint
Blueprint Description	Text describing the purpose of the blueprint
Alert Status	Indicates whether alerts are enabled: ***YES** - Enable alerts (create admin alerts) ***NO** - Disable alerts
User Scope	Enter the user group you want to associate with the blueprint. **Note**: If you create a new profile based on this blueprint, the group you enter in this field will be the user group to which you can add new profiles. This is also the user group whose members are updated when a blueprint is enforced. (See Manage User Profiles, for information about adding a user profile based on an existing blueprint.)
Inactivity until User Profile is disabled (days)	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Inactivity until User Profile is deleted (days)	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Object owner for objects owned by deleted profiles	Name of the user who should take over ownership of objects when/if a profile is disabled or deleted **Note**: *DFT (Default) indicates that the standard owner defined by IBM should be applied

4) Press **Enter**. The **User Profile Parameter Settings** interface is displayed.

> **Tip**: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 2: Add Profile Parameters to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add profile parameters to your blueprint

1) Do one of the following:

If	Then
If you want to see all available parameters	Press the **F6** (Add All) function key, go to Step 2 **Note**: This option adds all available profile parameters (and their associated default values). You can edit the default value if necessary. **Tip**: *ANY is not a valid parameter value. If ***ANY** is the default value, you will be required to enter a specific value before you can save the blueprint.
If you want to see only the system-suggested parameters	Press the **F7** (Add Suggested) function key, skip to Step 4 **Note**: This option adds only the profile parameters suggested by the intelligence engine.
If you want to add all default parameters	Press the **F8** (Add All Default) function key, skip to Step 4

Note: The **Parameter Selection** dialog appears.

2) In the **Sel** column, enter **1** beside the parameter(s) you want to add.

Tip: To make no selections, press the **F12** (Cancel) function key to return to the previous screen.

3) Press **Enter** to add the selected parameters and return to the **User Profile Parameter Settings** interface.

4) Press **Enter**. The **User Profile Object Authority** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 3: Add Object Authorities to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add object authorities to your blueprint

1) In the ***USRPRF Object** area, complete the following fields:

Field	Description
Object Owner	Enter one the following: Name - Enter the user name you want to assign as the owner of user profile objects ***DFT** - Assign user profile object ownership to the default (IBM) user ***USRPRF** - Assign user profile object ownership to the user running the program **Note**: If *DFT appears in this column, the two fields below should be left blank.
Owner Authority	Enter the authority level you want to assign the object owner: ***ALL** - Grant owner all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant owner change authority ***EXCLUDE** - Prohibit owner from performing operations on the object ***USE** - Grant access to the object attributes and allow the owner to use of the object (but not change the object)
*PUBLIC Authority	Enter the authority level you want to assign to public users (*Public): ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***AUTL** - Grant public users the default level of authority specified by the authority list ***CHANGE** - Grant public users change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object)

2) In the ***MSGQ Object** area, complete the following fields:

Field	Description
Object Owner	Enter one the following: Name - Enter the user name you want to assign as the owner of message queue objects ***DFT** - Assign message queue object ownership to the default (IBM) user ***USRPRF** - Assign message queue object ownership to the user running the program **Note**: If *DFT appears in this column, the two fields below should be left blank.
Owner Authority	Enter the authority level you want to assign the object owner: ***ALL** - Grant owner all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant owner change authority

	*EXCLUDE - Prohibit owner from performing operations on the object *USE - Grant access to the object attributes and allow the owner to use of the object (but not change the object)
*PUBLIC Authority	Enter the authority level you want to assign to public users (*Public): ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***AUTL** - Grant public users the default level of authority specified by the authority list ***CHANGE** - Grant public users change authority ***USE** - Grant access to the object attributes and allow public users to use the object (but not change the object)

3) Press **Enter**. The **Authority List Settings** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 4: Add Authority List Settings to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add authority list settings to your blueprint

1) Press the **F6** (Add) function key on your keyboard. The **Authority List Settings** interface is displayed.

2) Complete the following fields:

Field	Description
Authority List	Enter the name of the authority list to which this blueprint applies **Note**: An authority list displays the users who have the authority to access a specific object.
Authority Value	Enter the authority level you want to assign users who are members of the authority list: ***ALL** - Grant users all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant users change authority ***EXCLUDE** - Prohibit uses from performing operations on the object ***USE** - Grant access to the object attributes and allow users to use the object (but not change the object)

3) Press **Enter** to add the authority list and return to the User **Authority List Settings** interface.

4) Press **Enter**. The **3rd Party Integration** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 5: Add 3rd Party Scripts to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add 3rd party scripts to your blueprint

1) Press the **F6** (Add) function key on your keyboard. The **3rd Party Integration** interface is displayed.

2) Complete the following fields:

Field	Description
Script Type	Type of the third-party script
Script Statement	3rd party script text

4) Press **Enter**.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 6: Add Permissions to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add permissions to a blueprint

1) Press the **F6** (Add) function key on your keyboard. The **Blueprint Permissions** interface is displayed.

2) Complete the following fields:

Field	Description
User/Group	User or user group that has permission to use the blueprint to create and change user profiles **Tip**: Press the F4 (List) function key to see a list of available options.
Create Permission	Whether the user/user group has permission to create new user profiles based on the blueprint *YES - Enable create *NO - Disable create
Change Permission	Whether the user/user group has permission to change user profiles based on blueprint *YES - Enable change *NO - Disable change

3) Press **Enter**.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Copy Blueprint

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

To copy a blueprint

1) Access the **Work with Blueprint** interface.
2) In the **OPT** column for the desired blueprint, 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** twice.

Delete Blueprint

Use this task to delete a blueprint.

To delete a blueprint

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

Display Blueprint Details

Use this task to display blueprint details.

To display blueprint details

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **5** (Display).
3) Press **Enter**.

Field	Description
Blueprint ID	ID assign to the blueprint
Blueprint Description	Text describing the purpose of the blueprint
Alert Status	Whether alerts are enabled *YES - Enable alerts (create admin alerts) *NO - Disable alerts

User Scope	User group to which the blueprint applies
Inactivity until User Profile is disabled (days)	Number of days a profile must remain inactive before it is disabled **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Inactivity until User Profile is deleted (days)	Number of days a profile must remain inactive before it is deleted **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Object owner for objects owned by deleted profiles	Name of the user who should take over ownership of objects when a profile is disabled or deleted **Note**: All objects must be assigned an owner.

Display Inactivity Overrides

Use this task to display inactivity overrides. When you create a blueprint, you have the option to use the default (*DFT) IBM policy to determine when an inactive user profile is disabled or deleted (and to whom object ownership should be transferred in such a case).

To display inactive overrides

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **14** (Inactivity Overrides).
3) Press **Enter**.

Field	Description
Inactivity until User Profile is disabled (days)	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Inactivity until User Profile is deleted (days)	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Object owner for objects owned by deleted profiles	Name of the user who should take over ownership of objects when a profile is disabled or deleted

Edit Blueprint Details

Use this task to edit the details of an existing blueprint.

To edit blueprint details

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

Edit Blueprint Profile Parameters

Use this task to edit the profile parameters for an existing blueprint.

To edit blueprint profile parameters

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **10** (Profile Parameters).
3) Press **Enter**.
4) Modify the parameters as necessary. You also have the ability to add and delete parameters.
5) Press **Enter** twice.

Edit Blueprint Profile Authorities

Use this task to edit the profile authorities for an existing blueprint.

To edit blueprint profile authorities

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

2) In the **OPT** column for the desired blueprint, enter **11** (Profile Authorities).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete profile authorities.

5) Press **Enter** twice.

Edit Blueprint Authority Lists

Use this task to edit the authority list for an existing blueprint.

To edit blueprint authority list

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

2) In the **OPT** column for the desired blueprint, enter **12** (Authority Lists).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete authority lists.

5) Press **Enter** twice.

Edit Blueprint 3rd Party Scripts

Use this task to edit 3rd party scripts associated with an existing blueprint.

To edit blueprint 3rd party scripts

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

2) In the **OPT** column for the desired blueprint, enter **13** (3rd Party).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete 3rd party scripts.

5) Press **Enter** twice.

Edit Blueprint Permissions

Use this task to manage who can use a blueprint (as a template) to create and change user profiles.

To edit blueprint permissions

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

2) In the **OPT** column for the desired blueprint, enter **30** (Blueprint Permissions).

3) Press **Enter**.

4) Modify the following fields as necessary.

Field	Description
User/Group	User or user group who has permission to use the blueprint to create and change user profile **Tip**: Press the F4 (List) function key to see of a list of available options.
Create Permission	Whether the user/user group has create permission ***YES** - Enable create ***NO** - Disable create
Change Permission	Whether the user/user group has change permission ***YES** - Enable change ***NO** - Disable change

5) Press **Enter** twice.

Add Blueprint User

Use this task to add a user (member) to a blueprint user group.

To add blueprint user

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

2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).

3) Press **Enter**. The **Work with Users** interface is displayed.

4) Press the **F6** (Add) function key on your keyboard. The **Work with Users - Add Record** interface is displayed.

5) Complete the following fields.

Field	Description
User Name	Name of user
User Description	Description of user

6) Press **Enter**.

> **Note**: If the system locates the user on the server, then a ***YES** appears in the **Exists on Server** field.

Edit Blueprint User

Use this task to edit the user details of a user (member) assigned to a blueprint group.

To edit a blueprint user

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

2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).

3) Press **Enter**. The **Work with Users** interface is displayed.

4) In the **OPT** column for the desired user, enter **2** (Edit).

5) Press **Enter**.

6) 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.

7) Press **Enter** twice.

Delete Blueprint User

Use this task to delete a user (member) from a blueprint group.

To delete a blueprint user

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

2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).

3) Press **Enter**. The **Work with Users** interface is displayed.

4) In the **OPT** column for the desired user, enter **4** (Delete).

5) Press **Enter**.

6) Review the record to ensure you are deleting the correct blueprint.

7) Press **Enter** twice

Display Blueprint Compliance Issues

Use this task to display blueprint compliance issues. This is another way of running the blueprint compliance report.

To display blueprint compliance issues

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

2) In the **OPT** column for the desired blueprint, enter **22** (Run Compliance Report).

3) Press **Enter**.

4) Complete the following fields.

Field	Description
Component	Name of blueprint
Audit report	Enter *YES to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***NO** to display only (not enforce them) compliance issues **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***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.

5) Press **Enter**.

Display List of Non-Compliant Profiles

Use this task to display blueprint compliance issues identified when the blueprint compliance report was the last run.

Tip: Before you can display compliance issues you must run the blueprint compliance report.

To display blueprint compliance issues

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

2) In the **OPT** column for the desired blueprint, enter **20** (Non-Compliant).

3) Press **Enter**.

Field	Description
User Name	Name of the user
Violation	How the user's profile is in violation of the blueprint: **Category** - Category of violation **Keyword** - Parameter that is in violation **Description** - Description of object in violation
Blueprint Value	Parameter value defined in the blueprint
Actual Value	Parameter value defined in the user profile

Enforce Blueprint

Use this task to enforce a blueprint.

Tip: Before enforcing a blueprint, first display the blueprint compliance issues to identify where non-compliance is occurring. In some cases, an issue of non-compliance might identify the need for an exclusion to be added. In other words, you might need to update the blueprint.

To enforce authority blueprint

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

2) In the **OPT** column for the desired blueprint, enter **24** (Run Enforcement).

3) Press **Enter**.

4) Complete the following fields:

Field	Description
Component	Name of blueprint
Audit report	Enter ***YES** to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***YES** to enforce the blueprint **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***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.

5) Press **Enter**.

See also

Working with Blueprints

Run Blueprint Reports

Use this task to generate the following blueprint reports:

- Access the User Profile Interface
- Run Blueprint Compliance Report (TGPRFCMP)
- Run Blueprint Master Report
- Run Blueprint Permission File Report
- Run Blueprint Parameter File Report
- Run Blueprint Object Authority File Report
- Run Blueprint Authority List Settings Report
- Run Blueprint Non-Compliance User Profiles Report
- Run Blueprint 3rd Party Integration File Report
- Run Blueprint Master Change Report
- Run Blueprint Permission File Change Report
- Run Blueprint Parameter File Change Report
- Run Blueprint Object Authority File Change Report
- Run Blueprint Authority List Settings Change Report
- Run Blueprint Non-Compliance User Profiles Change Report
- Run Blueprint 3rd Party Integration File Change Report

Tip: You can schedule the blueprint reports (like all other reports) to run when most convenient.

Note: To work with blueprint reports, access from the **User Profile Reports** interface.

Access the User Profile Interface

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**. The **User Profile Reports** interface is displayed.

Run Blueprint Compliance Report (TGPRFCMP)

Use this task to run the blueprint compliance issues report. This report lists the users whose profile authorities do not meet blueprint requirements.

Tip: Run this task before you attempt to enforce a blueprint to determine if exclusions are required (see Manage User Exclusions).

To run the Blueprint Compliance Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Blueprint Compliance Report).
5) Press **Enter**.
6) Complete the following fields.

Tip: To see the complete list of available parameters, press the **F9** function key.

Field	Description
Component	Enter *BLUEPRINT
Audit report	Enter *YES to enable auditing (tracking)
Users	User profile to include in the report

Field	Description
Days for disable user profile	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Days for delete user profile	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
File to receive output	Name of file to receive report output
Library	Library in which the file resides
Replace or add records	Whether to replace or append records to the file
Enforcement	Enter ***NO** to display only (not enforce) compliance issues **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to run when most efficient for the system.
Job queue	If you want to include the report in a batch, enter job queue
Library	Library in which job queue resides
Schedule?	Whether the report is scheduled

7) Press **Enter**.

Run Blueprint Master Report

Use this task to display the list of blueprints.

To run the Blueprint Master Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Blueprint Master).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Permission File Report

Use this task to display permissions associated with blueprints. Permissions determine who can use a blueprint to create or modify user profiles.

To run the Blueprint Permission File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Blueprint Permission File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Parameter File Report

Use this task to display parameters associated with blueprints. For a user profile to be in compliance with a blueprint, the parameter values in the blueprint must match the parameter values in the associated user profile.

To run the Blueprint Parameter File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Object Authority File Report

Use this task to display object authorities associated with blueprints.

To run the Blueprint Object Authority File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Authority List Settings Report

Use this task to display the authority list associated with blueprints.

To run the Blueprint Authority List Settings Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **5** (Blueprint Authority List Settings).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**.

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

Run Blueprint Non-Compliance User Profiles Report

Use this task to display a list of user profiles that are not compliant with blueprints.

To run the Blueprint Non-Compliance User Profiles Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (Blueprint Non-Compliance User Profiles).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint 3rd Party Integration File Report

Use this task to display 3rd party scripts associated with blueprints.

To run the Blueprint 3rd Party Integration File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Master Change Report

Use this task to display changes made to the blueprint master.

> **Tip**: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the Blueprint Master Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Blueprint Master Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Permission File Change Report

Use this task to display changes made to blueprint permissions. Permissions determine who can use a blueprint to create or modify user profiles.

To run the Blueprint Permission File Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Blueprint Permission File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Parameter File Change Report

Use this task to display changes made to blueprint parameters.

To run the Blueprint Parameter File Change Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Object Authority File Change Report

Use this task to display changes made to blueprint object authorities.

To run the Blueprint Object Authority File Change Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Authority List Settings Change Report

Use this task to display changes made to blueprint authority lists.

To run the Blueprint Authority List Settings Change Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Blueprint Authority List Settings Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint Non-Compliance User Profiles Change Report

Use this task to display changes made to non-compliant user profiles.

To run the Blueprint Non-Compliance User Profiles Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (Blueprint Non-Compliance User Profiles Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Blueprint 3rd Party Integration File Change Report

Use this task to display changes made to 3rd party scripts.

To run the 3rd Party Integration File Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Blueprints

User Exclusions

This section describes how to work with **User Exclusions**.

This section includes the following topics:

See also

User Profile Management

Working with User Exclusions

Use the **User Exclusion** feature to do the following:

- Display User Exclusions
- Manage User Exclusions
- Run User Exclusion Reports

Note: To work with user exclusions, you must access the **Work with User Exclusions** interface.

To access the Work with User Exclusions interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Work with User Exclusions).
5) Press **Enter**. The **Work with User Exclusions** interface is displayed.

See also

User Exclusions

Display User Exclusions

Use this task to display user exclusions.

- Display List of User Exclusions
- Sort List of User Exclusions
- Move to Position in List of User Exclusions

Display List of User Exclusions

Use this task to display the list of available user exclusions.

To display the list of user exclusions

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Work with User Exclusions).
5) Press **Enter**. The **Work with User Exclusions** interface is displayed.

Field	Description
User Group	Name of the user group to which exclusions apply
Exclusion Type	Type of exclusion ***ALL** - All types ***ACTIVITY** - Exclude the user group from inactivity check ***SYNC** - Exclude the user group from synchronization with other iSeries systems

Sort List of User Exclusions

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with User Exclusion** 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.

Move to Position in List of User Exclusions

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 Exclusion** 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.

Filter List User Exclusions

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with User Exclusion** 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.

See also

Working with User Exclusions

Manage User Exclusions

Use this task to manage user exclusions.

- Access the Working with User Exclusions Interface
- Add Exclusion
- Edit Exclusion
- Copy Exclusion
- Delete Exclusion

Note: To manage user exclusions, access the Work with User Exclusions interface.

Access the Working with User Exclusions Interface

To access the Work with User Exclusions interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Work with User Exclusions).
5) Press **Enter**. The **Work with User Exclusions** interface is displayed

Add Exclusion

Use this task to create a new user exclusion.

To copy an exclusion

1) Access the **Work with User Exclusions** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Press **Enter**. The **Work with User Exclusion - Add** interface is displayed.
3) Complete the following fields.

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

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.

Tip: If you want to exclude generic user profiles, create a TG user group, and then use the group to exclude the generic users.

5) Press **Enter** twice.

Edit Exclusion

Use this task to edit an existing user exclusion.

To edit an exclusion

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, 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.

Copy Exclusion

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

To copy an exclusion

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, 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** twice.

Delete Exclusion

Use this task to delete an exclusion.

To delete an exclusion

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

See also

Working with User Exclusions

Run User Exclusion Reports

Use this task to generate the following user exclusion reports:

- Access the User Profile Report Interface
- Run User Profile Exclusions Report
- Run User Profile Exclusions Changes Report

Tip: You can schedule the user exclusion reports (like all other reports) to run when most convenient.

Note: To work with user exclusion reports, access from the **User Profile Reports** interface.

Access the User Profile Report Interface

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**. The **User Profile Reports** interface is displayed.

Run User Profile Exclusions Report

Use this report to view the list of user profile exclusions.

To run the User Profile Exclusions Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **8** (User Profile Exclusions).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run User Profile Exclusions Changes Report

Use this report to view the changes made to user profile exclusions.

Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the User Profile Exclusions Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **8** (User Profile Exclusions Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with User Exclusions

Archived Profiles

This section describes how to work with **Archived Profiles**.

This section includes the following topics:

- Working with Archived Profiles
- Display Archived Profiles
- Manage Archived Profiles
- Run Archived Profile Reports

See also

User Profile Management

Working with Archived Profiles

Use the **Archived Profiles** feature to do the following:

- Display Archived Profiles
- Manage Archived Profiles
- Run Archived Profile Reports

Note: To work with archived profiles, you must access the **Work with Archived Profiles** interface.

To access the Work with Archived Profiles interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Work with Archived Profiles).
5) Press **Enter**. The **Work User Archived Profiles** is displayed.

See also

Archived Profiles

Display Archived Profiles

Use this task to display archived profiles.

- Display List of Archived Profiles
- Clean up Profile Archive Data
- Sort List of Archived Profiles
- Move to Position in List of Archived Profiles
- Filter List Archived Profiles

Display List of Archived Profiles

Use this task to display the list of available archived profiles.

To display the list of archived profiles

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Work with Archived Profiles).
5) Press **Enter**. The **Work with Archived Profiles** is displayed.

Field	Description
User Name	Name of the user whose profile has met inactivity limits and should, therefore, be disabled or deleted
Archived Date	Date on which the user profile was archived
User Description	Description of the user
Arch Available	Where archive is available
Archived Library	Name of the archive library
Archived File	Name of the archive file

Clean up Profile Archive Data

Use this task to delete previously archived profile data.

To clean up profile data

1) Access the **Profile Archive Cleanup** interface.
2) Press the **F16** (Profile Archive Cleanup) function key on your keyboard.

Tip: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F24**, you must hold down the **Shift** key and **F12**. The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

Sort List of Archived Profiles

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

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

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

Move to Position in List of Archived Profiles

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 Archived Profiles** 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.

Filter List Archived Profiles

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

> **Tip**: Use a wildcard asterisk to help define your subset.
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
> – Add an asterisk after the text (e.g., report*) to find list items that start with specific text.
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Archived Profiles** interface.
2) Press the **F8** (Subset) function key on your keyboard.
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.

See also

Working with Archived Profiles

Manage Archived Profiles

Use this task to manage archived profiles.

- Access the Work with Archived Profiles Interface
- Reactivate Profile
- Delete Archived File

Note: To manage archived profiles, access the **Work with Archived Profiles** interface.

Access the Work with Archived Profiles Interface

To access the Work with Archived Profiles interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Work with Archived Profiles).
5) Press **Enter**. The **Work with Archived Profiles** is displayed.

Reactivate Profile

Use this task to reactivate a profile.

Note: Profiles are archived (retired from the system and stored in an archive file) once they meet the inactivity requirements set in the Manage Inactive Profiles.

To reactivate a profile

1) Access the **Work with Archived Profiles** interface.
2) In the **OPT** column for the desired profile, enter **6** (Reactivate Profile).
3) Press **Enter**.

Delete Archived File

Warning: Before deleting an archive file, ensure you have a back-up of the file.

Use this task to delete an archive file, which contains multiple archived user profiles.

To delete an archive file

1) Access the **Work with Archived Profiles** interface.
2) In the **OPT** column for the desired archive file, enter **9** (Delete Archive File).
3) Press **Enter** twice.

See also

Working with Archived Profiles

Run Archived Profile Reports

Use this task to generate the following archived profile reports:

- Run User Profile Archive Report
- Run User Profile Archive Changes Report

Tip: You can schedule the archived profile reports (like all other reports) to run when most convenient.

Note: To work with archived profile reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**. The **User Profile Reports** interface is displayed.

Run User Profile Archive Report

Use this report to view the list of archived profiles.

To run the User Profile Archive Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **9** (User Profile Archive).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run User Profile Archive Changes Report

Use this report to view the list of changes made to archived profiles.

Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the User Profile Archive Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **9** (User Profile Archive Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Archived Profiles

Inactive Profiles

This section describes how to work with **Inactive Profiles**.

This section includes the following topics:

- Working with Inactive Profiles
- Display Inactive Profile Settings
- Manage Inactive Profiles
- Run Inactive Profile Reports

See also

User Profile Management

Display Inactive Profile Settings

Use this task to display the inactive profile settings.

To display Inactive profile settings

1) From the TGSecure **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **5** (Profile Inactivity Settings).
5) Press **Enter**. The **Profile Inactivity Settings** interface is displayed.

Field	Description
Inactivity until user profile is disabled	Number of days before an inactive user profile is disabled
Inactivity until user profile is deleted	Number of days before an inactive user profile is deleted
Delete profiles with password of *NONE	Whether to delete profiles that do not have an assigned password ***YES** - Delete the profiles ***NO** - Keep the profiles
Object owner for objects owned by deleted profiles	The name of the user who will inherit ownership of objects for deleted user profiles
Remove deleted profiles from TG user group	Whether to remove deleted profiles from TG user groups ***YES** - Delete the user profile from TG groups ***NO** - Keep the user profile as a member of TG groups
Remove deleted profiles from TG rules	Whether to remove deleted profiles from TG rules. ***YES** - Delete the user profile from rule definition ***NO** - Keep the user profile as part of rule definition
Alert when inactivity found	Whether to send an alert to the admin when inactive profiles are detected ***YES** - Enable alerts ***NO** - Disable alerts

See also

Working with Inactive Profiles

Manage Inactive Profiles

Use this task to manage inactive profiles.

Note: To manage Profile Manager defaults, access the **Profile Inactivity Settings** interface.

Access the Profile Inactivity Settings Interface

To access the Profile Inactivity Settings interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **5** (Profile Inactivity Settings).
5) Press **Enter**. The **Profile Inactivity Settings** interface is displayed.

Edit Inactive Profile Settings

To display Inactive profile settings

1) Access the **Profile Inactivity Settings** interface.
2) Modify the necessary parameters:

Field	Description
Inactivity until user profile is disabled	Number of days before an inactive user profile is flagged as needing to be disabled
Inactivity until user profile is deleted	Number of days before an inactive user profile is flagged as needing to be deleted
Delete profiles with password of *NONE	Whether to delete profiles with the password value of *NONE ***YES** - Delete the profiles ***NO** - Keep the profiles
Object owner for objects owned by deleted profiles	The name of the user who will inherit ownership of objects from deleted or disabled user profiles **Note**: All objects must be assigned an owner.
Remove deleted profiles from TG user group	Whether to remove deleted profiles from TG user groups ***YES** - Delete the user profile from TG groups ***NO** - Keep the user profile as a member of TG groups
Remove deleted profiles from TG rules	Whether to remove rules that are no longer associated with a user because the user profile for which the rule was defined is no longer present in the system ***YES** - Delete the rule ***NO** - Keep the rule
Alert when inactivity found	Whether to send an alert to the admin when inactive profiles are detected ***YES** - Enable alerts ***NO** - Disable alerts

3) Press **Enter** twice.

Display the List of Inactive Profiles

Use this task to display the list of user profiles that the system (based on the inactive profile settings) has deemed as inactive.

To display the list of inactive user profiles

1) Access the **Profile Inactivity Settings** interface.
2) Press the **F22** (Run Inactive Report) function key on your keyboard.

Tip: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F24**, you must hold down the **Shift** key and **F12**.

3) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

Enforce Inactive Profile Rules

Use this task to enforce the inactive profile rules.

> **Note**: Whether a profile is disabled or deleted during enforcement is based on the inactive profile settings.

To enforce profile inactivity rules

1) Access the **Profile Inactivity Settings** interface.
2) Press the **F23** (Run Inactivity Enforcement) function key on your keyboard.

> **Tip**: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F23**, you must hold down the **Shift** key and **F11**.

3) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Inactive Profiles

Run Inactive Profile Reports

Use this task to generate the following inactive profile reports:

> **Tip**: You can schedule the Archived Profile reports (like all other reports) to run when most convenient.

> **Note**: To work with Archived Profile reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**. The **User Profile Reports** interface is displayed.

Run Inactivity Compliance Report (TGPRFCMP)

Use this report to display the list of inactive profiles.

To run the Inactivity Compliance Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Inactivity Compliance Report).
5) Press **Enter**.
6) Complete the following fields:

> **Tip**: To see the complete list of available parameters, press the **F9** function key.

Field	**Description**
Component	Enter ***INACTIVITY**
Audit report	Enter ***YES** to enable auditing (tracking)
Users	User profile to include in the report
Days for disable user profile	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Days for delete user profile	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
File to receive output	Name of file to receive report output
Library	Library in which the file resides
Replace or add records	Whether to replace or append records to the file
Enforcement	Enter ***NO** to display only (not enforce) compliance issues **Tip**: Always display (run the report) and analyze before enforcing.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to run when most efficient for the system.
Job queue	If you want to include the report in a batch, enter job queue
Library	Library in which job queue resides

Schedule?	Whether the report is scheduled

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Profile Inactivity Settings Report

Use this report to view the list of profile inactivity settings.

To run the Profile Inactivity Settings Report

1) Access the **User Profile Reports** interface.

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

3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Profile Inactivity Settings).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Profile Inactivity Settings Changes Report

Use this report to view the list of changes made to the profile inactivity settings.

Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the Profile Inactivity Settings Changes Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Profile Inactivity Settings Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Inactive Profiles

User Profiles

This section describes how to work with **User Profiles**.

This section includes the following topics:

- Working with User Profiles
- Manage User Profiles
- Run User Profile Reports

See also

User Profile Management

Working with User Profiles

Use the **User Profile** feature to do the following:

- Manage User Profiles
- Run User Profile Reports

> **Note**: To work with user profiles, you must access the **TG User Profile Manager** interface.

To access the TG User Profile Manager interface

1) Log into to TGSecure. The **Main** menu appears.

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

3) Press **Enter**. The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Create/Change User Profile - TGUSRMGR).

5) Press **Enter**. The **TG User Profile Manager** interface is displayed.

See also

User Profiles

Manage User Profiles

Use this task to manage user profiles.

- Access the TG User Profile Manager Interface
- Create User Profile Based on a Blueprint
- Change User Profile Based on a Blueprint

Note: To manage user profiles using blueprints, access the **TG User Profile Manager** interface.

Access the TG User Profile Manager Interface

To access the TG User Profile Manager interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **4** (Create/Change User Profile - TGPRFMGR).
5) Press **Enter**. The **TG User Profile Manager** interface is displayed.

Create User Profile Based on a Blueprint

Use this task to create a user profile based on a blueprint.

Tip: Ensure you have permission to use the blueprint to create profiles before attempting this task.

To create a user profile based on a blueprint

1) Access the **TG User Profile Manager** interface.
2) In the **Action type** field, enter ***CRT**.
3) Press Enter.
4) Complete the following fields:

Field	Description
Blueprint ID	Name of the blueprint on which to base the user profile
User Name	Name of the user or user group
User Description	Description of the user
Add to Blueprint user group	Whether to add the user to the user group associated with the named blueprint ***YES** - Add the user to the blueprint user group ***NO** - Base the user profile on the blueprint only, but do not add the user to the blueprint user group

5) Press **Enter**.

Change User Profile Based on a Blueprint

Use this task to change a user profile based on a blueprint.

Tip: Ensure you have permission to use the blueprint to change profiles before attempting this task.

To change a user profile based on a blueprint

1) Access the **TG User Profile Manager** interface.
2) In the **Action type** field, enter ***CHG**.
3) Press **Enter**.
4) Complete the following fields:

Field	Description
Blueprint ID	Name of the blueprint on which to base the user profile
User Name	Name of the user

Field	Description
User Description	Description of the user
Add to Blueprint user group	Whether to add the user to the user group associated with the named blueprint ***YES** - Add the user to the blueprint user group ***NO** - Based the user profile on the blueprint only, but do not add the user to the blueprint user group

5) Press **Enter**.

See also

Working with User Profiles

Run User Profile Reports

Use this task to run the following user profile reports:

- Run User Profile Create/Change via Blueprint
- Run User Profile Activity Report
- Run User Profile Changes Report
- Run Invalid Sign-on Attempts Report
- Run Authority Failures For User Report

Tip: You can schedule the user profile reports (like all other reports) to run when most convenient.

Note: To work with user profile reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**. The **User Profile Reports** interface is displayed.

Run User Profile Create/Change via Blueprint

Use this report to view the profiles either created or changed using the profile manager feature.

To run the User Profile Create/Change via Blueprint Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (User Profile Create/Change via Blueprint).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run User Profile Activity Report

Use this report to view modifications made to user profiles. The information is presented in two-row partners. The first row shows the previous state and the second row shows the change state.

Tip: This report has numerous columns. If you are interested in only a subset of user profile parameters, consider creating a custom report based on this built-in report.

To run the User Profile Activity Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **4** (User Profile Activity).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

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) Press **Enter**.

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

Run User Profile Changes Report

Use this report to view who has modified user profiles and what they have changed.

Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the User Profile Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (User Profile Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Invalid Sign-on Attempts Report

Use this report to view the list of unsuccessful sign-on attempts.

To run the Invalid Sign-on Attempts Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **5** (Invalid Sign-on Attempts).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Authority Failures For User Report

Use this report to view job failures due to inadequate user authorities.

To run the Invalid Sign-on Attempts Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **7** (Authority Failures For User).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with User Profiles

Password Rules

This section describes how to work with **Password Rules**.

This section includes the following topics:

- Working with Password Rules
- Manage Password Rules

See also

User Profile Management

Working with Password Rules

Use the **Password Rules** feature to do the following:

> ⓘ **Note**: To work with inactive profiles, you must access the **Password Rule Settings** interface.

To access the Password Rules Settings interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (Password Rule Settings).
5) Press **Enter**. The **Password Rules Settings** interface is displayed.

See also

Password Rules

Manage Password Rules

Use this task to manage password rules.

- Access the Work with Password Rules Setting Interface
- Add Password Exit Program
- Remove Password Exit Program
- Edit Password Rules

> **Note**: To manage password rules, access the **Password Rules Setting** interface.

Access the Work with Password Rules Setting Interface

To access the Work **with Password Rules Setting interface**

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**. The **User Profile Management** interface is displayed.
4) At the **Selection or command** prompt, enter **6** (Password Rules Settings).
5) Press **Enter**. The **Password Rules Setting** is displayed.

Add Password Exit Program

Use this task to add (install) the password exit program.

> **Note**: Before using the Profile Manager to modify password rules, you must install the password exit program.

To add password exit programs

1) Access the **Password Rule Settings** interface.
2) Press the **F20** (Add Password Exits) function key on your keyboard.

> **Tip**: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F20**, you must hold down the **Shift** key and **F8**.

Remove Password Exit Program

Use this task to remove the password exit program.

To remove password exit programs

1) Access the **Password Rule Settings** interface.
2) Press the **F21** (Remove Password Exits) function key on your keyboard.

> **Tip**: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F21**, you must hold down the **Shift** key and **F9**.

Edit Password Rules

Use this task to edit password rules.

> **Tip**: Changes made in this interface will not impact password rules unless the password exit program is installed.

> **Note**: IBM provides documentation for all password rule parameters. To access the IBM documentation, enter the following at the **Selection or command** prompt: WRKSYSVAL SYSVAL(QPWDRULES) and then press F1 (Help).

To edit password rules

1) Access the **Password Rules Setting** interface.
2) Complete the following fields:

Field	Description
Current password level (QPWDLVL)	Enter the desired password level
Password rule value set to *PWDSYSVAL	Whether to use default system values or custom rules ***YES** - Use default password system values ***NO** - Allow the admin to customize password rules **Tip**: This value must be set to *NO if you want to use the profile manager feature to update password rules.
Number of mixed case letters (*MIXCASEn)	**[0-9]** - Number of mix-case letters required in the password
Limit repeat characters (*CHRLMTREP)	Whether a password to contain characters that repeat (appears next to each other) **Y** - Disallow consecutive use of characters **N** - Allow consecutive use of characters
Limit same character (*LMTSAMPOS)	Whether characters can be used in the same position as the previous password **Y** - Disallow characters in the same position **N** - Allow characters in the same position
Require upper/lower/digits/special char (*REQANY3)	Whether a password is required to contain the following types of characters: uppercase, lowercase, special characters or digits **Y** - Require character variation **N** - Do not require character variation
Limit profile name (*LMTPRFNAME)	Whether a password can contain the user's profile name. **Y** - Disallow user's profile name in password **N** - Allow user's profile name in password
Password cannot be same as last	**[0-32]** - Number of times before a password can be repeated
Block password change (Hours)	**[1-99]** - Number of hours allowed between password changes **Note**: Enter ***NONE** to ignore this rule.
Password expiration interval (Days)	**[1-366]** - Number of days a password is valid **Note**: Enter ***NOMAX** to ignore this rule.
Password expiration warning (Days)	**[1-99]** - Number of days before a password expiration warning is issued to the user
Limit Adjacent	Whether to allow adjacent elements: **Y** - Disallow adjacent characters, digits, or special characters **N** - Allow adjacent characters, digits, or special characters
Limit First Char	Whether to place limits on the first character **Y** - Disallow password to start with a character, digit, or special character **N** - Allow password to start with a character, digit, or special character
Limit Last Char	Whether to place limits on the last character **Y** - Disallow password to end with a character, digit, or special character **N** - Allow password to end with a character, digit, or special character
Maximum	**[0-9]** - Maximum number of characters, digits, or special characters allowed in the password
Minimum	**[0-9]** - Minimum number of characters, digits, or special characters allowed in the password (0-9)

3) Press the **F8** (Save Settings) function key on your keyboard.

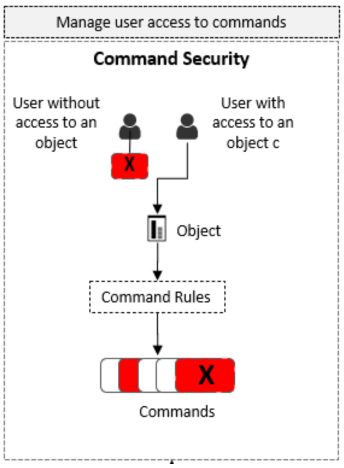
See also

Working with Password Rules

Command Security

Use the **Command Security** feature to add an additional layer of security at the command level. IBM security is based on object-level authorities, which is one level above commands. If a user has access to an object, then they can perform all authorized commands on that object. The **Command Security** feature allows you to limit which commands can be executed, even though the user has permission via Object authority.

Tip: The error message given to the end-user who is blocked from executing a command might be difficult for the user to decode (last request at level [N] ended), but the administrator can see full, clear details about why a user/user group was blocked from executing a command in the job log (dspjoblog).



To access the Command Security interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**.

This section contains the following topics:

- Command Security Defaults
- Command Security Rules
- Command Security Reports

See also

Getting Started

Command Security Defaults

Use the **Command Security Defaults** to define the following:

This section includes the following topics:

- Working with Command Security Defaults
- Display Command Security Defaults
- Manage Command Security Defaults

Note: To manage network defaults, access the **Command Security Defaults** interface.

To access the Command Security Defaults interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **6** (Command Security).

3) Press **Enter**. The **Command Security** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).

5) Press **Enter**. The **Command Security Defaults** interface is displayed.

See also

Command Security

Working with Command Security Defaults

Use the **Command Security Defaults** feature to do the following:

- Display Command Security Defaults
- Manage Command Security Defaults
- Run Command Security Reports

> **Note**: To manage network defaults, access the **Command Security Defaults** interface.

To access the Command Security Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).
5) Press **Enter**. The **Command Security Defaults** interface is displayed.

See also

Command Security

Display Command Security Defaults

Use this task to display network security default settings.

To display the Command Security defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).
5) Press **Enter**. The **Command Security Defaults** interface is displayed.

Field	Description
Audit Status	Whether auditing is enabled globally (for all command security rules). *__YES__ - Record command security changes in the audit journal *__NO__ - Do not command security changes in the audit journal **Tip**: Auditing is required if you plan to run command security reports.
Audit Journal	Journal in which to store command security data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about command security changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run command security change reports. **Note**: There are multiple TGSecure modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see *ALL, this indicates that configuration changes are being tracked in all modules.
Alert Status	Whether alerting is enabled globally (for all command rules). Alerting is required if you plan to send alert notifications. *__YES__ - Enable alerts *__NO__ - Disable alerts **Tip**: If alerts are disabled at the command security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the command rule (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 command rule. See Manage Command Security Rules for information about setting the alert status for an individual exit point.
Alert Message Queue	Queue in which to store alerts **Tip**: You can change the queue if you are using a third-party application for message monitoring.
Alert Message Queue Library	Library in which the queue is located
Primary Group Inheritance	Whether to allow primary group inheritance *__YES__ - Enable profile inheritance for the primary group *__NO__ - Disable profile inheritance for the primary group **Note**: The primary group is the user ID entered in the **Group profile** field when using command **CHGUSRPRF**. The primary group is the first ID from which a user inherits privileges.
Supplemental Group Inheritance	Whether to allow supplemental group inheritance *__YES__ - Enable profile inheritance for supplemental groups *__NO__ - Disable profile inheritance for supplemental groups **Note**: The supplemental groups are user IDs entered in the **Supplemental group** field when using command **CHGUSRPRF**. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.
Command Security	Whether to enable the **Command Security** feature *__YES__ - Enable the Command Security feature *__NO__ - Disable the Command Security feature

See also

Working with Command Security Defaults

Manage Command Security Defaults

Use this task to manage **Command Security** default settings.

- Access the Command Security Defaults Interface
- Enable Command Security (Globally)
- Enable Command Security Auditing
- Enable Command Security Change Auditing
- Enable Command Security Alerts
- Enable Group Profile Inheritance

Note: To manage network defaults, access the **Command Security Defaults** interface.

Access the Command Security Defaults Interface

To access the Command Security Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (Command Security Defaults).
5) Press **Enter**. The **Command Security Defaults** interface is displayed.

Enable Command Security (Globally)

Use this task to enable/disable command security globally (TGCMDSEC).

Alternatively, this same action can be executed by entering ***YES**/***NO** in the **Command Security (Enable/Disable)** field in the **Command Security Defaults** interface.

To enable/disable command security globally

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **2** (Enable/Disable Command Security).
5) Press **Enter**. The **TG Command Security (TGCMDSEC)** interface is displayed.
6) In the Enable Command Security field, enter the desired option:

- ***YES** - Enable the Command Security feature
- ***NO** - Disable the Command Security feature (disregard all command security rules)

Enable Command Security Auditing

Use this task to enable command security auditing.

Tip: Auditing is required if you plan to run network security reports.

Note: If auditing is disabled at the command 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 command rule) if you want to record auditing data for a specific command rule.

To enable command security auditing

1) Access the **Command Security Defaults** interface.
2) In the **Auditing Status** field, enter ***YES**.
3) In the **Audit Journal** field, enter the name of the journal in which to store the auditing data.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter**. The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Enable Command Security Change Auditing

Use this task to enable tracking of command security configuration changes.

Tip: Tracking is required if you plan to run command security change reports.

To enable command security configuration change tracking

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

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.

Enable Command Security Alerts

Use this task to enable command security alerts.

Tip: Alerting is required if you plan to send alert notifications.

Note: If alerts are disabled at the command security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the rule (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 rule.

To enable command security alerts

1) Access the **Command Security Defaults** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

Enable Group Profile Inheritance

Use this task to enable users to inherit privileges as defined in their IBM profile. In other words, if an IBM user profile is a member of a group (as defined by the **Group profile** and/or **Supplemental group** profile parameters), then you can use the following instruction to ensure that rules created in TGSecure consider the privileges inherited by users when the system is enforcing rules.

Here is a usage example. There are two IBM users: User AAA (higher privilege user) and user BBB (lower privilege user). An IBM user administrator decides to allow user BBB to inherit the privileges from user AAA. To do this, the IBM user administrator uses the command CHGUSRPR, and then enters AAA in the **Group profile** or **Supplemental group** parameter. By taking this action, the user administrator is allowing user BBB to inherit the privileges as user AAA. Now if you want the inherited privileges granted by the IBM user administrator to be considered in TGSecure when evaluating rules, then you must enable group profile inheritance in TGSecure.

To enable group profile inheritance

1) Access the **Command Security Defaults** interface.
2) In the **Primary Group Inheritance** field, enter ***YES**.

Note: The primary group is the user ID entered in the **Group profile** field when using command CHGUSRPRF. The primary group is the first ID from which a user inherits privileges.

3) In some cases, a user might inherit privileges from multiple users. In such a case, enter ***YES** in **Supplemental Group Inheritance** field.

Note: Supplemental groups are user IDs entered in the **Supplemental group** field when using command CHGUSRPRF. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.

4) Press **Enter**.

Tip: Refer to the IBM knowledge base for additional information regarding primary and secondary group inheritance.

See also

Working with Command Security Defaults

Command Security Rules

Use **Command Security** rules to implement restrictions on commands.

This section contains the following topics:

- Working with Command Security Rules
- Display List of Command Security Rules
- Manage Command Security Rules

> **Note**: To work with command security rules, access the **Work with Command Security** interface.

To access the Work with Command Security interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **6** (Command Security).

3) Press **Enter**. The **Command Security** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Command Security Rules).

5) Press **Enter**. The **Work with Command Security** interface is displayed.

See also

Command Security

Working with Command Security Rules

Use **Command Security** rules to do the following:

- Display List of Command Security Rules
- Manage Command Security Rules
- Run Command Security Reports

> **Note**: To work with command security rules, access the **Work with Command Security** interface.

To access the Work with Command Security interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Command Security Rules).
5) Press **Enter**. The **Work with Command Security** interface is displayed.

See also

Command Security Rules

Display List of Command Security Rules

Use this task to display **Command Security** rules.

Display List

Use this task to display the list of command security rules.

To display the list of command security rules

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **6** (Command Security).

3) Press **Enter**. The **Command Security** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Command Security Rules).

5) Press **Enter**. The **Work with Command Security** interface is displayed.

Field	Description
Command	Name of command
Library	Library in which command resides
User	User or user group to which the rule applies
Client IP	IP address to which the rule applies
Calendar	Applicable calendar **Note**: the calendar limits when the rule is applicable.
Parm Rest	Whether parameter restrictions are enabled: ***YES** - Parameter restrictions are enabled ***NO** - Parameter restrictions are disabled **Note**: Parameter restrictions limit which parameters a user can enter for a command.
Alert Sts	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Exit Inst	Whether the associated exit point is installed: ***YES** - Exit point installed ***NO** - Exit point not installed
Action	The level at which action was taken: ***EXITLVL** - Exit point level

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 Command Security** 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.

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 Command Security** 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**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
>
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
>
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
>
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Command Security** interface.

2) Press the **F8** (Subset) function key.

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

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

See also

Working with Command Security Rules

Manage Command Security Rules

Use this task to manage **Command Security** rules.

> **Note**: To manage command security rules, access the **Work with Command Security** interface.

Access the Work with Command Security Interface

To access the Work with Command Security interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Command Security Rules).
5) Press **Enter**. The **Work with Command Security** interface is displayed.

Add Command Security Rule

Use this task to add a command security rule.

> **Tip**: You can define a command security rule for groups of users, networks, or operations.

To add a command security rule

1) Access the **Work with Command Security** interface.
2) Press the **F6** (Add) function key.
3) Complete the following fields:

Field	Description
Command Name	Enter the name you want to assign the command rule
Command Library	Enter the library in which the command rule resides
User Name	Enter the user or user group to which the rule applies
Client IP	Enter the IP address to which the rule applies
Enable Status	Identify whether to enable the rule *__YES__ - Rule enabled *__NO__ - Rule disabled
Audit Status	Identify whether to enable auditing *__YES__ - Auditing enabled *__NO__ - Auditing disabled **Note**: Auditing must be enabled to generate reports.
Alert Status	Identify whether to enable alerting: *__YES__ - Alerts enabled *__NO__ - Alerts disabled
Calendar	Enter the applicable calendar **Note**: the calendar limits when the rule is applicable.
Action	Enter the level at which to execute the action: *__EXITLVL__ - Exit point level **Note**: If the action failed, you will see *__FAIL__ in this column.

Parameter Restriction	Identify whether to enable parameter restrictions: ***YES** - Parameter restrictions are enabled ***NO** - Parameter restrictions are disabled **Note**: Parameter restrictions limit which parameters a user can enter for a command.
Exit Installed	Identify whether to install the associated exit point: ***YES** - Exit point installed ***NO** - Exit point not installed

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.

Edit Command Security Rule

Use this task to edit an existing command security rule.

To edit a command security rule

1) Access the **Work with Command Security Rules** interface.

2) In the **OPT** column for the desired command security 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.

Copy Command Security Rule

Use this task to create a new rule by copying a command security rule.

To copy a command security rule

1) Access the **Work with Command Security Rules** interface.

2) In the **OPT** column for the desired command security 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**.

Delete Command Security Rule

Use this task to delete a command security rule.

To delete a command security rule

1) Access the **Work with Command Security Rules** interface.

2) In the **OPT** column for the desired command security rule, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct rule.

5) Press **Enter**.

Create Parameter Restriction

Use this task to create restrictions based on command parameters.

To create a parameter restriction

1) Access the **Work with Command Security Rules** interface.
2) In the **OPT** column for the desired command security rule, enter **2** (Edit).
3) Press **Enter**.
4) In the **Action** field, enter one of the following options:
    - ***PASS** - If the parameter restriction is met, allow the action.
    - ***FAIL** - If the parameter restriction is met, disallow the action.
5) Select ***YES** for the **Parameter Restrictions** field to enable parameter restrictions.
6) Press **Enter** twice.
7) In the **OPT** column for the desired rule, enter **10** (Work with Parameters). The **Work with Command Security - Parameter** interface is displayed.
8) In the **Command Parm. Restriction** field, enter the parameter and the parameter value (in parenthesis) that you want to restrict (pass or fail).
   For example, enter SBS (TGCMN) to restrict the parameter SBS to the parameter value of TGCMN.
9) Press **Enter** twice.

See also

Working with Command Security Rules

Command Security Reports

This section includes the following topics:

- Working with Command Security Reports
- Run Command Security Reports

ⓘ **Note**: To work with command security reports, access from the **Command Security Reports** interface.

To access the Command Security Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**. The **Command Security Reports** interface is displayed.

See also

Command Security

Working with Command Security Reports

Use the **Command Security Reports** interface to do the following:

- Run Command Security Reports

> **Note**: To work with command security reports, access from the **Command Security Reports** interface.

To access the Command Security Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**. The **Command Security Reports** interface is displayed.

See also

Command Security Reports

Run Command Security Reports

Use this task to generate the following **Command Security** reports:

- Access the Command Security Reports Interface
- Run Command Security Activity Reports
- Run Command Security Configuration Reports
- Run Command Security Change Reports

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with command security rule reports, access from the **Command Security Reports** interface.

Access the Command Security Reports Interface

To access the Command Security Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**. The **Command Security Reports** interface is displayed.

Run Command Security Activity Reports

Use this task to run the reports classified as activity reports.

To run the Command Security Activity Reports

1) Access the **Command Security Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Command Security Activity Reports).
3) Press **Enter**. The **Command Security Activity Reports** interface is displayed.
4) Select the desired activity report.
5) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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.

6) Enter the desired output format in the **Report output type** field.
7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Command Security Configuration Reports

Use this task to run the reports classified as configuration reports.

Tip: You must enable auditing to produce change reports. See Manage Command Security Defaults for additional information.

To run the Command Security Configuration Reports

1) Access the **Command Security Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Command Security Configuration Reports).
3) Press **Enter**. The **Command Security Configuration Reports** interface is displayed.
4) Select the desired configuration report.
5) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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.

6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run Command Security Change Reports

Use this task to run the reports classified as change reports.

> **Tip**: You must enable auditing to produce change reports. See Manage Command Security Defaults for additional information.

To run the Command Security Change Reports

1) Access the **Command Security Reports** interface.

2) At the **Selection or command** prompt, enter **3** (Command Security Change Reports).

3) Press **Enter**. The **Command Security Change Reports** interface is displayed.

4) Select the desired change report.

5) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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.

6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Command Security Reports

System Value Management

Use the **System Value Management** feature to manage...

To access the System Value Management interface

1) Log into to TGSecure. The **Main** menu appears.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**.

This section contains the following topics:

- System Value Defaults
- System Values Rules
- System Value Reports

See also

Getting Started

System Value Defaults

Use the **System Value Management Defaults** to define the following:

This section includes the following topics:

- Working with System Value Management Defaults
- Display System Value Defaults
- Manage System Value Defaults

Note: To manage system value defaults, access the **System Value Default** interface.

To access the System Value Default interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **7** (System Value Management).

3) Press **Enter**. The **System Value Management** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (System Value Management Defaults).

5) Press **Enter**. The **System Value Default** interface is displayed.

See also

System Value Management

Working with System Value Management Defaults

Use the **Command Security Defaults** feature to do the following:

- Display System Value Defaults
- Manage System Value Defaults
- Run System Value Management Reports

Note: To manage network defaults, access the **System Default Default** interface.

To access the System Value Default interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Value Management** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (System Value Management Defaults).
5) Press **Enter**. The **System Value Default** interface is displayed.

See also

System Value Management

Display System Value Defaults

Use this task to display **System Value** default settings.

To display the System Value defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Defaults).
3) Press **Enter**. The **System Value Management** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (System Value Defaults).
5) Press **Enter**. The **System Value Default** interface is displayed.

Field	Description
Audit Journal	Journal in which to store command security data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about command security changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run command security change reports. **Note**: There are multiple TGSecure modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see *ALL, this indicates that configuration changes are being tracked in all modules.
Alert Status	Whether alerting is enabled globally (for all command rules). Alerting is required if you plan to send alert notifications. ***YES** - Enable alerts ***NO** - Disable alerts **Tip**: If alerts are disabled at the command security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the command rule (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 command rule. See Manage Command Security Rules for information about setting the alert status for an individual exit point.
Alert Message Queue	Queue in which to store alerts **Tip**: You can change the queue if you are using a third-party application for message monitoring.
Alert Message Queue Library	Library in which the queue is located
Enforcement Enable	Whether to enforce system value rules. ***YES** - Enable enforcement of system value rules ***NO** - Disable enforcement of system value rules

See also

Working with System Value Management Defaults

Manage System Value Defaults

Use this task to manage **System Value** default settings.

- Access the System Value Defaults Interface
- Enable System Value Enforcement
- Enable System Value Auditing
- Enable System Value Change Auditing
- Enable System Value Alerts

Note: To manage network defaults, access the **System Value Defaults** interface.

Access the System Value Defaults Interface

To access the System Value Management Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Value Management** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (System Value Defaults).
5) Press **Enter**. The **System Value Defaults** interface is displayed.

Enable System Value Enforcement

Use this task to enable/disable system value enforcement.

Alternatively, this same action can be executed by entering ***YES**/***NO** in the **Enforcement Enable** field in the **System Value Default** interface.

To enable/disable system value enforcement

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Value Management** interface is displayed.
4) At the **Selection or command** prompt, enter **10** (System Value Defaults).
5) Press **Enter**. The **System Value Default** interface is displayed.
6) In the **Enforcement Enable** field, enter the desired option:

- ***YES** - Enable the enforcement of system values
- ***NO** - Disable the enforcement of system values

Enable System Value Auditing

Use this task to enable system value auditing.

Tip: Auditing is required if you plan to run system value reports.

To enable system value auditing

1) Access the **System Value Default** interface.
2) In the **Audit Status** field, enter ***YES**.
3) In the **Audit Journal** field, enter the name of the journal in which to store the auditing data.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter**. The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Enable System Value Change Auditing

Use this task to enable tracking of system value configuration changes.

Tip: Tracking is required if you plan to run system value change reports.

To enable system value configuration change tracking

1) Access the **System Value Default** interface.
2) In the **Audit Configuration Changes** field, enter **Y**.
3) Press **Enter**.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, 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 tracked in at least one module, but not all modules. If you see *__ALL__, this indicates that configuration changes are being tracked in all modules.

Enable System Value Alerts

Use this task to enable system value alerts.

Tip: Alerting is required if you plan to send alert notifications.

Note: If alerts are disabled at the system value management (module) level, then alerts are not stored in the message queue even if alerts are enabled at the rule (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 rule.

To enable system value security alerts

1) Access the **System Value Default** interface.
2) In the **Alerting Status** field, enter *__YES__.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

See also

Working with System Value Management Defaults

System Values Rules

Use **System Values** rules to establish recommendations for what is expected as the current value.

This section contains the following topics:

- Working with System Values Rules
- Display List of System Value Rules
- Manage System Value Rules

> **Note**: To work with command security rules, access the **Work with System Values** interface.

To access the Work with System Values interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Values Management).
3) Press **Enter**. The **System Values** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with System Values).
5) Press **Enter**. The **Work with System Values** interface is displayed.

See also

System Value Management

Working with System Values Rules

Use **System Values** to do the following:

- Display List of System Value Rules
- Manage System Value Rules
- Run System Value Management Reports

> **Note**: To work with system values, access the **Work with System Values** interface.

To access the Work with System Values interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Values** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with System Values).
5) Press **Enter**. The **Work with System Values** interface is displayed.

See also

System Values Rules

Display List of System Value Rules

Use this task to display the list of **System Values**.

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of system value rules.

To display the list of system values rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Value** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with System Values).
5) Press **Enter**. The **Work with System Values** interface is displayed.

Field	Description
System Value	Name assigned to the system value
Category	System value category
System Value Description	Description of the system value
Alt Sts	Whether alerting is enabled: *__YES__ - Alerts enabled *__NO__ - Alerts disabled
Expected Value	The parameter value expected (recommended)
Current Value	The parameter value currently defined
Compl Sts	Compliance status: ***PASS** - Expected value and current value match ***FAIL** - Expected value and current value differ

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 System Value** 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.

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 System Values** 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**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with System Values** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

See also

Working with System Values Rules

Manage System Value Rules

Use this task to manage **System Values** rules.

- Access the Work with System Values Interface
- Edit System Value Rule
- Change System Value
- Set System Value to Expected Value

Note: To manage system value rules, access the **Work with System Values** interface.

Access the Work with System Values Interface

To access the Work with System Values interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Values** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with System Values).
5) Press **Enter**. The **Work with System Values** interface is displayed.

Edit System Value Rule

Use this task to edit an existing system value rule.

To edit a system value rule

1) Access the **Work with System Values** interface.
2) In the **OPT** column for the desired command security rule, enter **1** (Edit).
3) Press **Enter**.
4) Modify the following fields as necessary:

Field	Description
System Value	Name assigned to the system value
Compliance Status	Flag indicating whether current authority levels defined in the system align with the rule *__FAIL__ - There are discrepancies *__PASS__ - There are no discrepancies (authority levels and schema align)
Category	System value category
Description	Description of the system value
Shipped Value	Parameter defined for the system value at the time the product was shipped (distributed) to the client
TG Recommended	Parameter recommended by Trinity Guard for the system value
Current Value	Current parameter set for the system value
Compliance Cond	The condition/range of parameters acceptable for the current value (in relation to the expected value) to be in compliance (*PASS). **INFO** - **=** - Current value complies if it is equal to the expected value **LIKE** - Current value complies if it is similar to the expected value **NLIKE** - Current value complies if it is not similar to the expected value **<>** - Current value complies if it is not equal to the expected value **<** - Current value complies if it is less than the expected value **>** - Current value complies if it is great than the expected value **<=** - Current value complies if it is less than or equal to the expected value **>=** - Current value complies if it is great than or equal to the expected value
Alert Status	Whether alerting is enabled: *__YES__ - Alerts enabled *__NO__ - Alerts disabled
Expected Value	The expected parameters for system value.

Field	Description
	Note: If the current value does not match the expected value, then compliance status displays as *FAIL.
Password Level	Password encryption level

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.

Change System Value

Use this task to change a system value.

To change a system value

1) Access the **Work with System Values** interface.
2) In the **OPT** column for the desired system value, enter **2** (Change System Value).
3) Press **Enter**.
4) In the **Option** column for the desired system value rule, enter **2** (Change).
5) Press **Enter**.
6) 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.

7) Press **Enter**.

Set System Value to Expected Value

Use this task to set a system value to the expected value.

To set a system value to the expected value

1) Access the **Work with System Values** interface.
2) In the **OPT** column for the desired command security rule, enter **6** (Set to Expected Value).
3) Press **Enter**. You should receive a confirmation or information message at the bottom of the screen.

See also

Working with System Values Rules

System Value Reports

This section includes the following topics:

- Working with System Value Management Reports
- Run System Value Management Reports

Note: To work with command security reports, access from the **System Value Reports** interface.

To access the System Value Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Value Management** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**. The **System Value Reports** interface is displayed.

See also

System Value Management

Working with System Value Management Reports

Use the **Command Security Reports** interface to do the following:

- Run System Value Management Reports

> Note: To work with command security reports, access from the **Command Security Reports** interface.

To access the Command Security Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **6** (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (Command Security Reports).
5) Press **Enter**. The **Command Security Reports** interface is displayed.

See also

System Value Reports

Run System Value Management Reports

Use this task to generate the following **System Value Management** reports:

- Access the System Value Reports Interface
- Run System Value Activity Reports
- Run System Value Configuration Reports
- Run System Value Change Reports

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with command security rule reports, access from the **System Value Management** interface.

Access the System Value Reports Interface

To access the System Value Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Value Management** interface is displayed.
4) At the **Selection or command** prompt, enter **20** (System Value Reports).
5) Press **Enter**. The **System Value Reports** interface is displayed.

Run System Value Activity Reports

Use this task to run the reports classified as activity reports.

To run the System Value Activity Reports

1) Access the **System Value Reports** interface.
2) At the **Selection or command** prompt, enter **1** (System Value Activity Reports).
3) Press **Enter**. The **System Value Activity Reports** interface is displayed.
4) Select the desired activity report.
5) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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.

6) Enter the desired output format in the **Report output type** field.
7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run System Value Configuration Reports

Use this task to run the reports classified as configuration reports.

Tip: You must enable auditing to produce change reports. See Manage System Value Defaults for additional information.

To run the System Value Configuration Reports

1) Access the **System Value Management Reports** interface.
2) At the **Selection or command** prompt, enter **2** (System Value Configuration reports).
3) Press **Enter**. The **System Value Configuration Reports** interface is displayed.
4) Select the desired configuration report.
5) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

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.

6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

Run System Value Change Reports

Use this task to run the reports classified as change reports.

> **Tip**: You must enable auditing to produce change reports. See Manage System Value Defaults for additional information.

To run the System Value Change Reports

1) Access the **System Value Change Reports** interface.

2) At the **Selection or command** prompt, enter **3** (System Value Change Reports).

3) Press **Enter**. The **System Value Change Reports** interface is displayed.

4) Select the desired change report.

5) Modify the report run criteria as necessary.

> **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

> **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.

6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with System Value Reports

Reports

This section describes how to work with **TGSecure reports**. Reports allow you to display and analyze system transactions.

This section includes the following topics:

To access the Reports interface

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

See also

Getting Started

Working with TGSecure Reports

Use the **Reports** feature to do the following:

- Display List of TGSecure Reports
- Run TGSecure Reports
- Create TGSecure Reports
- Manage TGSecure Reports

Tip: See the TGSecure Report Reference for details about a specific report.

Note: To work with built-in 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**.

See also

Reports

Display List of TGSecure Reports

Use this task to do the following:

- Display list
- Sort List
- Move to Location in List
- Filter List

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

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.

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.

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

See also

Working with TGSecure Reports

Run TGSecure Reports

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

Note: See the TGSecure Report Reference for information about individual reports.

- Run Reports with Start and End Time Requirements
- Run Reports without Start and End Time Requirements

Tip: You can schedule reports to run when most convenient.

Run Reports with Start and End Time Requirements

Use these instructions when the report requires the start and end time entries.

Identifying a start and end time helps you filter the data reported and is required for some types of reports that have the potential to contain a huge amount of data.

To run a report with start and end time requirements

1) Access the **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 from which report data is obtained (not an editable field)
Collector Name	Name assigned to the collector (not an editable field)
Report ID	ID assigned to the report you want to run (not an editable field)
User profile	Name of the user or group for which you want to report data **Tip**: Enter ***ALL** to include all users
Starting date	Select from the options available: ***CUR** - Use the current date ***CMS** - Use the current month's start date ***LMS** - Use the last month's start date ***LME** - Use the last month end date ***LYS** - Use the last year's start date ***LYE** - Use the last year's end date ***LWS** - Use the last week's start date (last 7 days) ***LDS** - Use the last day's start date
Starting time	Enter time in the format (hhmmss): hour, minute, second
Ending date	Select from the options available
Ending time	Enter time in the format (hhmmss): hour, minute, second
Override report defaults?	Whether to override report defaults: ***YES** - Ignore run-time collector defaults ***NO** - Apply Run-time collector defaults
Reload collector data	Whether to reload the 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 the data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Run interactively?	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system.

Run Reports without Start and End Time Requirements

Use these instructions when the report does not require a start and end time.

To run a report without start and end time requirements

1) Access the **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)
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	Whether to 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	Whether to reload the 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 the data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Run interactively?	Whether to run interactively or add to batch: *__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**. The status of the report is displayed at the bottom of the screen.

See also

Working with TGSecure Reports

Create TGSecure Reports

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

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

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**.

Step 1: Add Report

To add a Report

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

Step 2: Select Data Source Collector

Use this task to select the data source collector for your custom report. Each report must have a least one source (collector) from which to pull data.

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**.

Step 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.

Step 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 on your keyboard.

To select report fields

1) Press the **F4** (Select Fields) function key on your keyboard.
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

Step 5: Change Order of 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**.

Step 6: 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 on your keyboard.
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.

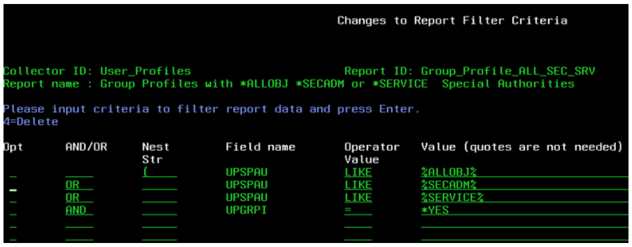


Figure: Build Report Filter Criteria

To delete filter criteria

1) Enter **4** (Delete) in the **Opt** column for the filter criteria you want to delete.

2) Press **Enter**.

Step 7: 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 TGSecure 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**.

Step 8: 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**.

See also

Working with TGSecure Reports

Manage TGSecure Reports

Use this task to do the following:

- Access the Work with Reports Interface
- Edit Report
- Copy Report
- Delete Report
- Enabling Report Alerting

Note: To manage reports, access the **Work with Reports** interface.

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**. The **Work with Reports Interface** is displayed.

Alternatively, at the IBM i command line, enter **TGWRKRPT**, and press **Enter**.

Edit Report

Use this task to edit a custom report.

Tip: You cannot edit built-in reports, but you can create a copy of a built-in report and then edit the copy.

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)
5 (Alerts)	Modify the condition (number of rows returned) that trigger the generation of an alert
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 List)	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 to be applied to the data obtained from the collector **Note**: Modifications cannot be made to built-in reports

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) In the **Opt** column for the report you want to copy, enter **3** (Copy).
3) Enter a unique Report ID and continue customization as desired. Please refer to "Creating Reports" for details.

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) In the **Opt** column for the report you want to delete, enter **4** (Delete).

Enabling Report Alerting

Use this task to enable alerting based on the results (number of rows) produced in a given report. This is useful if you want the system to send a notification when the number of rows in a report exceeds a threshold.

Tip: You can set up alerts for both built-in and custom reports.

To enable report alerting

1) Access the **Work with Reports** interface.
2) In the **Opt** column for the desired report, enter **5** (Alerts).
3) Complete the following fields:

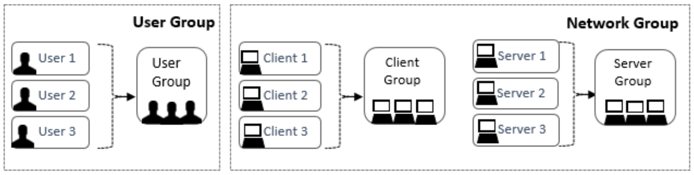
Field	Description
Alert Status	Enter *__YES__ to enable alerts for this specific report (local setting)
Alert Criteria (Condition)	Enter the desired mathematical symbol (<, >, =, etc.)
Alert Criteria (No. of Rows)	Enter the number of rows used in conjunction with a mathematical symbol to determine the threshold used to trigger an alert (e.g., if the number of rows is > 10, then trigger an alert). **Note**: See Set Up Alert Defaults for instructions on defining the action taken when a report triggers an alert.

See also

Working with TGSecure Reports

Groups

This section describes how to work with **Groups**. There are several types of groups that you can create.



This section includes the following topics:

- Working with Groups
- User Groups
- Network Groups
- Operation Groups
- Object Groups

See also

Getting Started

Working with Groups

This section includes the following topics:

- Working with User Groups
- Working with Network/Server Groups
- Working with Object Groups
- Working with Operation Groups

Note: To work with groups, access the **Work with Groups** interface.

To access the Work with Groups interface

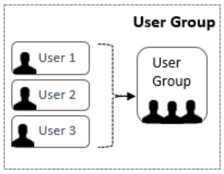
1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**. The **Work with Groups** interface is displayed.

See also

Groups

User Groups

This section describes how to work with **Users** and **User Groups**.



This section includes the following topics:

- Working with User Groups
- Display List of User Groups
- Display List of Users in a Group
- Manage User Groups
- Manage Users in a Group
- Run User Groups Report

See also

Groups

Working with User Groups

> ⓘ **Note**: 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) Do one of the following:

> ⓘ **Note**: User groups are a common feature in multiple TG products.

Product	Step
TGAudit	1. At the **Selection or command** prompt, enter the **3** (Job Activity Monitor). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **11** (Work with User Groups).
TGDetect	At the **Selection or command** prompt, enter **10** (Work with User Groups).
TGEncrypt	1. At the **Selection or command** prompt, enter **4** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).
TGSecure	1. At the **Selection or command** prompt, enter **31** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).

See also

User Groups

Display List of User Groups

Use this task to do the following with user groups:

- Display Lists of User Groups
- Sort List
- Move to Position in List
- Filter List

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

Display Lists of User Groups

Use this task to display the list of user groups.

To display the list of user groups

1) Access the **Main** menu.
2) Do one of the following:

Note: Groups are a common feature used in multiple TG products.

Product	Step
TGAudit	1. At the **Selection or command** prompt, enter the **3** (Job Activity Monitor). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **11** (Work with User Groups).
TGDetect	At the **Selection or command** prompt, enter **10** (Work with User Groups).
TGEncrypt	1. At the **Selection or command** prompt, enter **4** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).
TGSecure	1. At the **Selection or command** prompt, enter **31** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).

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.

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.

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with User Groups

Display List of Users in a Group

Use this task to do the following with user groups:

- Display Lists of User Groups
- Sort List
- Move to Position in List

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

Display Lists of User Groups

Use this task to display the list of user groups.

To display the list of user groups

1) Access the **Main** menu.

2) Do one of the following:

> **Note**: Groups are a common feature used in multiple TG products.

Product	Step
TGAudit	1. At the **Selection or command** prompt, enter the **3** (Job Activity Monitor). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **11** (Work with User Groups).
TGDetect	At the **Selection or command** prompt, enter **10** (Work with User Groups).
TGEncrypt	1. At the **Selection or command** prompt, enter **4** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).
TGSecure	1. At the **Selection or command** prompt, enter **31** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).

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.

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.

See also

Working with User Groups

Manage User Groups

Use this task to do the following with user groups:

- Access the Work with User Group Interface
- Add User Group
- Edit User Group
- Copy User Group
- Delete User Group

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

Access the Work with User Group Interface

To access the Work with User Groups interface

1) Access the **Main** menu.
2) Do one of the following:

Note: Groups are a common feature used in multiple TG products.

Product	Step
TGAudit	1. At the **Selection or command** prompt, enter the **3** (Job Activity Monitor). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **11** (Work with User Groups).
TGDetect	At the **Selection or command** prompt, enter **10** (Work with User Groups).
TGEncrypt	1. At the **Selection or command** prompt, enter **4** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).
TGSecure	1. At the **Selection or command** prompt, enter **31** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).

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.

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.

Copy User Group

Use this task to copy a user group.

To copy user 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) Modify the description as necessary.
5) Press **Enter** twice.

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.

See also

Working with User Groups

Manage Users in a Group

Use this task to do the following with user groups:

- Access the Work with User Group Interface
- Edit a User
- Delete a User

Note: To manage users, access the Work with Users interface.

Access the Work with User Group Interface

To access the Work with User Groups interface

1) Access the **Main** menu.
2) Do one of the following:

Note: Groups are a common feature used in multiple TG products.

Product	Step
TGAudit	1. At the **Selection or command** prompt, enter the **3** (Job Activity Monitor). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **11** (Work with User Groups).
TGDetect	At the **Selection or command** prompt, enter **10** (Work with User Groups).
TGEncrypt	1. At the **Selection or command** prompt, enter **4** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).
TGSecure	1. At the **Selection or command** prompt, enter **31** (Work with Groups). 2. Press **Enter**. 3. At the **Selection or command prompt**, enter the **1** (Work with User Groups).

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**.

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.

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.

See also

Working with User Groups

Run User Groups Report

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

- Run User Group Configuration Report
- Run User Group Configuration Changes Report

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**. The status of the report is displayed at the bottom of the screen.

Run User Group Configuration Changes Report

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

> **Tip**: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

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.

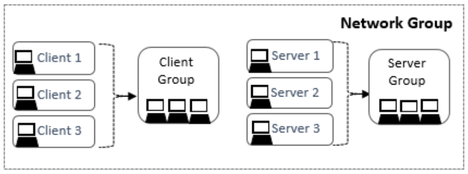
11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with User Groups

Network Groups

This section describes how to work with **Networks** and **Network Groups**.



This section includes the following topics:

- Working with Network/Server Groups
- Display List of Network/Server Groups
- Display List of Networks in a Group
- Manage Network/Server Groups
- Manage Networks in a Group
- Run Network Groups Report

See also

Groups

Working with Network/Server Groups

> **Note**: 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) Do one of the following:

> **Note**: Network/server groups are a common feature in multiple TG products.

Product	Step
TGEncrypt	At the **Selection or command** prompt, enter **4** (Work with Groups).
TGSecure	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**. The **Work with Network Groups** Interface is displayed.

See also

Network/Server Groups

Display List of Network/Server Groups

Use this task to do the following with network groups:

- Display List
- Sort List
- Move to Position in List
- Filter List

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) Do one of the following:

Note: Network/server groups are a common feature in multiple TG products.

Product	Step
TGEncrypt	At the **Selection or command** prompt, enter **4** (Work with Groups).
TGSecure	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**. The **Work with Network Groups** Interface is displayed.

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.

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.

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.

– Add an asterisk after text (e.g., report*) to find list items that start with specific text.

– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Network/Server Groups

Display List of Networks in a Group

Use this task to do the following with network groups:

- Display List
- Sort List
- Move to Position in List

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) Do one of the following:

> **Note**: Network/server groups are a common feature in multiple TG products.

Product	Step
TGEncrypt	At the **Selection or command** prompt, enter **4** (Work with Groups).
TGSecure	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**. The **Work with Network Groups** Interface is displayed.

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.

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

See also

Working with Network/Server Groups

Manage Network/Server Groups

Use this task to do the following with network groups:

- Access the Work with Network Groups Interface
- Add Network Group
- Edit Network Group
- Copy Network Group
- Delete Network Group

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

Access the Work with Network Groups Interface

To access the Work with Network Groups interface

1) Access the **Main** menu.
2) Do one of the following:

Note: Network/server groups are a common feature in multiple TG products.

Product	Step
TGEncrypt	At the **Selection or command** prompt, enter **4** (Work with Groups).
TGSecure	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**. The **Work with Network Groups** Interface is displayed.

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.

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.

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**.

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.

See also

Working with Network/Server Groups

Manage Networks in a Group

Use this task to do the following with network groups:

- Access the Work with Networks Interface
- Add Network
- Edit Network
- Delete Network

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

Access the Work with Networks Interface

To access the Work with Networks interface

1) Access the **Main** menu.

2) Do one of the following:

Note: Network/server groups are a common feature in multiple TG products.

Product	Step
TGEncrypt	At the **Selection or command** prompt, enter **4** (Work with Groups).
TGSecure	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**. The **Work with Networks** interface is displayed.

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.

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.

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.

See also

Working with Network/Server Groups

Run Network Groups Report

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

- Access the Network Reports Interface
- Run Network Group Configuration Report
- Run Network Group Configuration Changes Report

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with Network Group reports, access the **Network Reports** interface.

Access the Network Reports Interface

To access the Network Reports interface

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**. The **Network Reports** interface is displayed.

Run Network Group Configuration Report

Use this task to display user group configuration details.

To run the Network Group Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **5** (Network Groups Report).
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.

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**. The status of the report is displayed at the bottom of the screen.

Run Network Group Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run the Network Group Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **5** (Network Groups Changes Report).
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.

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.

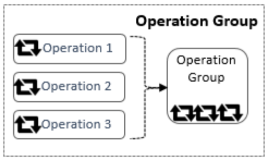
8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Network/Server Groups

Operation Groups

This section describes how to work with **Operations** and **Operation Groups**.



This section includes the following topics:

- Working with Operation Groups
- Display List of Operation Groups
- Display List of Operations in a Group
- Manage Operation Groups
- Manage Operations in a Group
- Run Operation Groups Report

See also

Groups

Working with Operation Groups

Use the **Operation Groups** feature to do the following:

- Display List of Operation Groups
- Display List of Operations in a Group
- Manage Operation Groups
- Manage Operations in a Group
- Run Operation Groups Report

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

See also

Operation Groups

Display List of Operation Groups

Use this task to do the following with operation groups:

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

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.

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.

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
>
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
>
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
>
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Operation Groups

Display List of Operations in a Group

Use this task to do the following with operation groups:

- Display List
- Sort List
- Move to Position in List

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

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.

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.

See also

Working with Operation Groups

Manage Operation Groups

Use this task to do the following with operation groups:

- Add Operation Group
- Edit Operation Group
- Copy Operation Group
- Delete Operation Group

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

Add Operation Group

Use this task to add an operation group.

To add an 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.

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.

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**.

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.

See also

Working with Operation Groups

Manage Operations in a Group

Use this task to do the following with operation groups:

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

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.

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.

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.

See also

Working with Operation Groups

Run Operation Groups Report

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

- Access the Network Reports Interface
- Run Operation Groups Configuration Report
- Run Operation Group Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Network Group reports, access the **Network Reports** interface.

Access the Network Reports Interface

To access the Network Reports interface

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**. The **Network Reports** interface is displayed.

Run Operation Groups Configuration Report

Use this task to display operation group configuration details.

To run the Operation Group Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **6** (Operation Groups Report).
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.

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**. The status of the report is displayed at the bottom of the screen.

Run Operation Group Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run the Operation Group Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **6** (Operation Groups Changes Report).
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.

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.

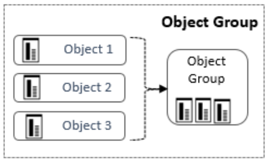
8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

See also

Working with Operation Groups

Object Groups

This section describes how to work with **Objects** and **Object Groups**.



This section includes the following topics:

- Working with Object Groups
- Display List of Object Groups
- Display List of Object in a Group
- Manage Object Groups
- Manage Objects in a Group
- Run Object Groups Report

See also

Groups

Working with Object Groups

Use the **Object Groups** feature to do the following:

- Display List of Object Groups
- Display List of Object in a Group
- Manage Objects in a Group
- Manage Objects in a Group
- Run Object Groups Report

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

See also

Object Groups

Display List of Object Groups

Use this task to do the following with object groups:

- Display List
- Sort List
- Move to a Position in the List

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

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.

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.

Filter List

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

> **Tip**: Use wildcard asterisk to help define your subset.
> – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
> – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
> – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

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

See also

Working with Object Groups

Display List of Object in a Group

Use this task to do the following with object groups:

- Display List
- Sort List
- Move to Position in List

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

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.

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

See also

Working with Object Groups

Manage Object Groups

Use this task to do the following with object groups:

- Add Object Group
- Edit Object Group
- Copy Object Group
- Delete Object Group

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

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.

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.

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**.

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.

See also

Working with Object Groups

Manage Objects in a Group

Use this task to do the following with object groups:

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

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

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.

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.

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 object, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct object.
5) Press **Enter** twice.

See also

Working with Object Groups

Run Object Groups Report

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

- Access the Network Reports Interface
- Run Object Group Configuration Report
- Run Object Group Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Network Group reports, access the **Network Reports** interface.

Access the Network Reports Interface

To access the Network Reports interface

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**. The **Network Reports** interface is displayed.

Run Object Group Configuration Report

Use this task to display operation group configuration details.

To run the Object Group Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (Object Groups Report).
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.

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**. The status of the report is displayed at the bottom of the screen.

Run Object Group Configuration Changes Report

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

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run the Object Groups Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (Object Groups Changes Report).
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.

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**. The status of the report is displayed at the bottom of the screen.

See also

Working with Object Groups

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.).

This section includes the following topics:

- Working with Calendars
- Display List of Calendars
- Manage Calendars
- Manage Calendar Day/Time Access

Troubleshooting

This section provides resources to help you troubleshoot issues:

- TGSecure FAQ
- Error Messages

TGSecure FAQ

This section provides troubleshooting information you can use to resolve issues you might encounter.

Why does my report have no data?

If you generate a report and it contains no data, you need to ensure that auditing has been enabled (see Audit Configuration).

Error Messages

Go here: IBM Errors

Appendices

APPENDIX - TGSecure Revisions

This section includes enhancement by version.

Version 3.4 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

- Network Security
- File Server collection data - add SSL Flag
- User Profile Archive UI to handle Hex data
- User Profile Management
- Add Report of Users (TGSecure-only licensing)
- Command Security
- Add the ability to copy in command security rules
- Bug Fixes

Version 3.3 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

Network Security

- Work with Operations/Ports has been updated to differentiate SSL/TLS secure ports within socket rules
- Incoming Transactions UI now handles hex data
- Incoming Transactions cleanup function enhanced
    - TGNTWCLEAN command now allows End/Start collection and Reorganize Database File

User Profile Manager

- Enhanced TGPRFMGR command to support user profile deletion

Command Security

- Allows ending command when run by non-UIM menus with no call stack entry

Resource Manager

- Enhanced to allow IFS generic exceptions

Version 3.2 - TGSecure User Guide Revisions

Thus release includes the following:

Enhancements

User Profile Management

o Password Rules UI Enhancements

o Added support for Blueprints to allow *LIBL as the Initial Program Library

Version 3.1 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

Access Escalation Management (AEM)

The following new report is now available:

- Access Escalation Activity Details

The following new collector is now available:

- ACCESS_ESCALATION_DETAILS

System Value Management (SVM)

- To support IBM's enhanced password encryption using the QPWDLVL system value, TGSecure now supports the identification of the password level (value 0-4) when defining **System Value** rules.

User Profile Management (PM)

- The value *ANY is now accepted as a **Profile Parameter** when defining a blueprint.
- To support the addition of the MAXSIGN (maximum sign-on attempts allowed per user profile) parameter in IBM i, TGSecure now supports the addition of the MAXSIGN parameter (value 0-5) as one of the **Profile Parameter** you can add when defining a blueprint.

Version 2.5 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

System Value Management (SYS)

- Added support for numeric data

Command Security (CMD)

- Added granular parameter restriction per rule (CMD/Lib/User/IP)
- Added option to use function key F2 to add exits out of sync

Version 2.4 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

System Value Management

The System Value Management feature is now available.

Reports

The following new System Value Management reports are now available:

- All System Values
- Security System Values
- System Value Changes
- System Value Configuration
- System Value Defaults
- System Value Valid Values
- System Value Configuration Changes
- System Value Default Changes
- System Value Valid Value Changes

Collectors

The following new collectors are now available:

- SYS_VAL_CONFIG
- SYS_VAL_DEFAULT
- SYS_VAL_VALID

User Profile Manager

Addition of two new options to archive inactive profiles:

- ***SAVSEC** - Save user profile data using SAVSECDTA command
- ***SAVPRF** - Save user profile data to a database file

Resource Manager

Addition additional support for authority schemas:

- IFS Filter Support
- IFS Depth Support

Version 2.3 - TGSecure User Guide Revisions

This release includes the following:

New Features

- Network Security - Artificial Intelligence (AI) rules engine
- Resource Manager - Schemas filter feature

Enhancements

- Network Security – Database Parser granularity of rules extended to the command level

Version 2.2 - TGSecure User Guide Revisions

This release contains the following:

New Features

Command Security (CMD)

The Command Security feature is now available.

The following new Command Security reports are now available:

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

The following new collectors are now available::

- CMD_SEC_COMMANDS
- CMD_SEC_CONF_SETTINGS
- CMD_SEC_PARAM_LEVEL
- CMD_SEC_RULES

Enhancements

Network Security

- Added support for swap profiles in exit point transaction rule definitions

Job Scheduler

- Added Job Scheduler

User Profile Manager

- Added support of the Initial Menu (INLMENU) special value of *SIGNOFF
- Changed TGPRFCMP command to support generic users in TG user groups
- Changed TGPRFMGR command to support generic users in TG user group
- Changed TGPROFILE - PRF00010D/P to validate objects as per IBM standards

Version 2.1 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

Groups

In the **Network Security Default** settings, you can now do the following:

- Enable group profile inheritance

Exit Program

The following exit program is now available for use:

- Showcase

> **Note**: See Manage Exit Points for instruction on adding (installing) an exit program.

Report

The following report is now available:

- Network Transaction Showcase

> **Note**: See the TGSecure Report Reference Guide for information about individual reports.

APPENDIX - TGSecure Collectors

Collector ID	Collector Name	Collector Category	Platform
ACCESS_ESCAL_ACC_CONTROLS	Access Escalation Access Controls	Network	IBMi
ACCESS_ESCAL_DEFAULTS	Access Escalation Defaults	Network	IBMi
ACCESS_ESCAL_ENTITLEMENTS	Access Escalation Entitlements	Network	IBMi
ACCESS_ESCAL_FILE_EDITORS	Access Escalation File Editors	Network	IBMi
ACCESS_ESCALATION_DETAILS	Access Escalation Details	Network	IBMi
ACCESS_ESCALATION_USAGE	Access Escalation Usage	Network	IBMi
AUTH_USERS_VIA_AUTH_LISTS	Authorized Users through Authorization Lists	Resource	IBMi
AUTHORITY_COL_ALI	Authority Collection Report (*ALL)	Resources	IBMi
AUTHORITY_COL_IFS	Auth Collection For Objects IFS Report	Resources	IBMi
AUTHORITY_COL_OBJECT	Auth Collection For Objects Native Report	Resources	IBMi
AUTHORITY_COLLECTION	Authority Collection Data	Journal	IBMi
AUTHORITY_COMPLIANCE	Authority Compliance	Resource	IBMi
AUTHORITY_LIST	Authority List Data	System	IBMi
BLUEPRINT_3RD_PARTY_FILE	Blueprint 3rd Party Integration File	Profile	IBMi
BLUEPRINT_AUTH_SETTINGS_FILE	Blueprint Authority List Settings File	Profile	IBMi
BLUEPRINT_MASTER	Blueprint Master	Profile	IBMi
BLUEPRINT_NON_COMPLIANCE_USER	Blueprint Non-Compliance User Profiles	Profile	IBMi
BLUEPRINT_OBJECT_AUTH_FILE	Blueprint Object Authority File	Profile	IBMi
BLUEPRINT_PARAMETER_FILE	Blueprint Parameter File	Profile	IBMi
BLUEPRINT_PERMISSION_FILE	Blueprint Permission File	Profile	IBMi
CMD_SEC_COMMANDS	Commands Allowed/Rejected via Command Security	Resources	IBMi
CMD_SEC_CONF_SETTINGS	Command Security Config Settings	Resources	IBMi
CMD_SEC_PARAM_LEVEL	Command Security Parameter Level	Resources	IBMi
CMD_SEC_RULES	Command Security Config Settings	Resources	IBMi
CONTROLLER_ATTACHED_DEVICES	Command Security Parameter Level	Network	IBMi
CONTROLLER_DESCRIPTION_DATA	Controller Description Information	Network	IBMi
DATA_AREA_AUDITING	Audit data area changes	Network	IBMi
DATABASE ACCESS	Database File Access	N/A	IBMi
DATABASE_AUDITING	Monitor Database changes	Network	IBMi
DATABASE_CONTENT	Database Content	Configuration	IBMi
DATABASE_FIELD_ACTIVITY	Database Field Activity	Resources	IBMi
DATABASE_MONITORING	Database Monitoring	Resources	IBMi
DATABASE_OPERATIONS	Database Operations	N/A	IBMi
DET_ACT_HISTORY	Detect Activity History	Network	IBMi
DET_DEFAULTS	Detect Defaults	Configuration	IBMi
DET_CMD_RULES	Command Monitor Rules	Configuration	IBMi
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration	IBMi
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration	IBMi
DET_JRNMON_RULES	Journal Monitor Rules	Configuration	IBMi
DET_MON_MASTER	Monitor Master	Configuration	IBMi

Collector ID	Collector Name	Collector Category	Platform
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration	IBMi
DET_MSQ_RULES	Message Queue Rules	Configuration	IBMi
DET_SEIM_PROVIDERS	SEIM Providers	Configuration	IBMi
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration	IBMi
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network	IBMi
DEVICE_DESCRIPTION_DATA	Device Description Information	Network	IBMi
DTBASE_OPERATIONS_JRN	Database Operations by Journal	N/A	IBMi
ENCRYPT_DATABASE_FIELD	Encryption Database Field Details	Resource	IBMi
ENCRYPT_DATABASE_FILE	Encryption Database File Details	Resource	IBMi
ENCRYPT_DATABASE_FILTER	Encryption Database File Details	Resource	IBMi
ENCRYPT_DATABASE_RULES	Encryption Database Rule Details	Resource	IBMi
ENCRYPTION_DEFAULTS	Encryption Defaults	Resource	IBMi
EXIT_POINTS	Display Exit Point Data	Network	IBMi
FIELD_AUTHORITY	Display Field Level Authorities	Object	IBMi
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource	IBMi
IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource	IBMi
IFS_CONTENT	IFS Content	Configuration	IBMi
IFS_JOURNALING	Display extended journaling information for the IFS object	Resource	IBMi
IFS_STATUS	Display status information about an IFS file	Resource	IBMi
INACTIVITY_DISCONNECTS	Inactivity Disconnections	Configuration	IBMi
INCOMING_TRANSACTIONS	Incoming Transactions	Network	IBMi
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network	IBMi
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network	IBMi
ISL_RULES	ISL Inclusion Exclusion Rules	Network	IBMi
JOB_ACTIVITY_DETAILS	Job Activity Details	Log	IBMi
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log	IBMi
JOB_DATABASE_ACTIVITY	Job and Database Activity	Configuration	IBMi
JOB_DESCRIPTIONS	Job Description Data	Configuration	IBMi
JOURNAL_AD	Object Auditing Attribute Changes	Configuration	IBMi
JOURNAL_AF	Authority Failures	Profile	IBMi
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration	IBMi
JOURNAL_AU	EIM Attribute Changes	Configuration	IBMi
JOURNAL_AX	Row and Column Access Control	Resource	IBMi
JOURNAL_C3	Advanced Analysis Command Configuration	Resource	IBMi
JOURNAL_CA	Authorization List or Object Authority Changes	Profile	IBMi
JOURNAL_CD	Commands Executed	Resource	IBMi
JOURNAL_CO	Create Operations	Resource	IBMi
JOURNAL_CP	User Profile Changes	Configuration	IBMi
JOURNAL_CQ	Change Request Descriptor Changes	Configuration	IBMi
JOURNAL_CU	Cluster Operation	Network	IBMi
JOURNAL_CV	Connection Verification	Profile	IBMi
JOURNAL_CY	Cryptographic Configuration Changes	Configuration	IBMi
JOURNAL_DI	LDAP Operations	Resource	IBMi
JOURNAL_DO	Delete Operations	Resource	IBMi

Collector ID	Collector Name	Collector Category	Platform
JOURNAL_DS	Changes to Service Tools Profiles	Profile	IBMi
JOURNAL_EV	Environment Variable Changes	Profile	IBMi
JOURNAL_FT	FTP Client Operations - Certificate data	Network	IBMi
JOURNAL_GR	Exit Point Maintenance Operations	Resource	IBMi
JOURNAL_GS	Socket Descriptor Details	Resource	IBMi
JOURNAL_IM	Intrusion Monitor Events	Network	IBMi
JOURNAL_IP	Inter-process Communication Events	Network	IBMi
JOURNAL_IR	Actions to IP Rules	Network	IBMi
JOURNAL_IS	Internet Security Management Events	Network	IBMi
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource	IBMi
JOURNAL_JS	Job Changes	Resource	IBMi
JOURNAL_KF	Key Ring File Changes	Configuration	IBMi
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource	IBMi
JOURNAL_M0	Db2 Mirror Setup Tools	Resource	IBMi
JOURNAL_M6	Db2 Mirror Communication Services	Resource	IBMi
JOURNAL_M7	Db2 Mirror Replication Services	Resource	IBMi
JOURNAL_M8	Db2 Mirror Product Services	Resource	IBMi
JOURNAL_M9	Db2 Mirror Replication State	Resource	IBMi
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration	IBMi
JOURNAL_NA	Network Attribute Changes	Profile	IBMi
JOURNAL_ND	Directory Search Violations	Resource	IBMi
JOURNAL_NE	APPN Endpoint Filter Violations	Network	IBMi
JOURNAL_O1	Single Optical Object Accesses	Resource	IBMi
JOURNAL_O2	Dual Optical Object Accesses	Resource	IBMi
JOURNAL_O3	Optical Volume Accesses	Resource	IBMi
JOURNAL_OM	Object Management Changes	Resource	IBMi
JOURNAL_OR	Objects Restored	Resource	IBMi
JOURNAL_OW	Object Ownership Changes	Resource	IBMi
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration	IBMi
JOURNAL_PF	PTF Operations	Resource	IBMi
JOURNAL_PG	Primary Group Changes	Resource	IBMi
JOURNAL_PO	Printer Output Changes	Resource	IBMi
JOURNAL_PS	Swap Profile Events	Configuration	IBMi
JOURNAL_PU	PTF Object Changes	Profile	IBMi
JOURNAL_PW	Invalid Sign-on Attempts	Profile	IBMi
JOURNAL_RA	Authority Changes to Restored Objects	Configuration	IBMi
JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration	IBMi
JOURNAL_RO	Ownership Changes for Restored Objects	Profile	IBMi
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration	IBMi
JOURNAL_RQ	Change Request Descriptors Restored	Resource	IBMi
JOURNAL_RU	Authority Restored for User Profiles	Profile	IBMi
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration	IBMi
JOURNAL_SD	System Directory Changes	Resource	IBMi
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration	IBMi

Collector ID	Collector Name	Collector Category	Platform
JOURNAL_SF	Spooled File Actions	Resource	IBMi
JOURNAL_SG	Asynchronous Signals Processed	Network	IBMi
JOURNAL_SK	Secure Socket Connections	Network	IBMi
JOURNAL_SM	Systems Management Changes	Configuration	IBMi
JOURNAL_SO	Server Security User Information Actions	Configuration	IBMi
JOURNAL_ST	Service Tools Actions	Configuration	IBMi
JOURNAL_SV	System Values Changes	Configuration	IBMi
JOURNAL_VA	Access Control List Changes	Configuration	IBMi
JOURNAL_VC	Connections Started, Ended, or Rejected	Network	IBMi
JOURNAL_VF	Close Operations on Server Files	Resource	IBMi
JOURNAL_VL	Exceeded Account Limit Events	Profile	IBMi
JOURNAL_VN	Network Log On and Off Events	Configuration	IBMi
JOURNAL_VO	Actions on Validation Lists	Resource	IBMi
JOURNAL_VP	Network Password Errors	Profile	IBMi
JOURNAL_VR	Network Resource Accesses	Resource	IBMi
JOURNAL_VS	Server Sessions Started or Ended	Network	IBMi
JOURNAL_VU	Network Profile Changes	Profile	IBMi
JOURNAL_VV	Service Status Change Events	Network	IBMi
JOURNAL_X0	Network Authentication Events	Network	IBMi
JOURNAL_X1	Identity Token Events	Profile	IBMi
JOURNAL_XD	Directory Server Extensions	Profile	IBMi
JOURNAL_YC	DLO Object Changes	Resource	IBMi
JOURNAL_YR	DLO Object Reads	Resource	IBMi
JOURNAL_ZC	Object Changes	Resource	IBMi
JOURNAL_ZR	Object Reads	Resource	IBMi
KEYSTORE_DATA	KeyStore	Configuration	IBMi
LIBRARY_STAT	Library Statistics	Resources	IBMi
LINE_DESCRIPTION_DATA	Line Description Information	Configuration	IBMi
MESSAGE_QUEUE	Message Queue Details	Configuration	IBMi
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration	IBMi
NETSERVER_CONFIG	NetServer Configuration	Network	IBMi
NETSERVER_SHARES	NetServer Shares	Network	IBMi
NETWORK_ATTRIBUTES	Network Attribute Information	Network	IBMi
NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network	IBMi
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network	IBMi
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network	IBMi
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network	IBMi
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network	IBMi
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network	IBMi
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network	IBMi
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network	IBMi
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes/Remote Exit Rule	Network	IBMi
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes/Remote Exit Rule	Network	IBMi
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network	IBMi

Collector ID	Collector Name	Collector Category	Platform
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network	IBMi
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_DDM	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_FILE	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_FTP_REXEC	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_PRINTER	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network	IBMi
NETWORK_TRANS_SIGNON	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_TELNET	Remote Exit Rules	Network	IBMi
OBJECT_AUTHORITY	Display Object Authority	Resource	IBMi
OBJECT_DETAILS	Display Object Details	Resource	IBMi
OBJECT_STAT	Object/File Statistics	Resource	IBMi
OUTPUT_QUEUE	Output Queue Information	Configuration	IBMi
PRODUCT_INFO	Basic Information about a software product	Configuration	IBMi
PROFILE_COMPLIANCE	Profile Compliance Data	Profile	IBMi
PROFILE_INACTIVITY_SETTINGS	Profile Inactivity Settings	Profile	IBMi
PROFILE_MANAGER_DEFAULTS	Profile Manager Defaults	Profile	IBMi
PROGRAM_ADOPT	Programs that Adopt Authority	Resource	IBMi
PROGRAM_REFERENCE_DATA	Program Reference Data	Resource	IBMi
PTF_DATA	Program Temporary Fix Data	Configuration	IBMi
QHST_MSG_INFO	QHST History Log Information	Configuration	IBMi
QSYS2.ACTIVE_JOB_INFO	Active job information	Configuration	IBMi
QSYS2.DATA_QUEUE_ENTRIES	Data Queue Entries	Resource	IBMi
QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User access	Configuration	IBMi
QSYS2.EXIT_POINT_INFO	Exit Point Information	Configuration	IBMi
QSYS2.EXIT_PROGRAM_INFO	Exit Program Information	Configuration	IBMi
QSYS2.FUNCTION_INFO	Function usage identifiers	Configuration	IBMi
QSYS2.FUNCTION_USAGE	Function usage configuration details.	Configuration	IBMi
QSYS2.GROUP_PTF_INFO	Group PTFs Information	Configuration	IBMi
QSYS2.JOURNAL_INFO	Journal and remote journal information	Configuration	IBMi
QSYS2.JOURNALED_OBJECTS	Journal object information	Resource	IBMi
QSYS2.LICENSE_INFO	Products license information.	Configuration	IBMi
QSYS2.MEDIA_LIBRARY_INFO	Media Library Status details	Configuration	IBMi
QSYS2.MEMORY_POOL	Memory pool details	Configuration	IBMi
QSYS2.MEMORY_POOL_INFO	Active memory pools	Configuration	IBMi
QSYS2.MESSAGE_QUEUE_INFO	Message Queue	Configuration	IBMi
QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 network connection details.	Configuration	IBMi
QSYS2.OBJECT_LOCK_INFO	Object lock information	Configuration	IBMi
QSYS2.OUTPUT_QUEUE_ENTRIES	Spooled file in output queue	Configuration	IBMi
QSYS2.RECORD_LOCK_INFO	Record lock information	Configuration	IBMi
QSYS2.REPLY_LIST_INFO	Current job's reply list entry information	Configuration	IBMi
QSYS2.SCHEDULED_JOB_INFO	Job Schedule Entry information	Configuration	IBMi
QSYS2.SECURITY_CONFIG	Security Configuration Information	Configuration	IBMi

Collector ID	Collector Name	Collector Category	Platform
QSYS2.SERVER_SBS_ROUTING	Alternate subsystem configurations	Configuration	IBMi
QSYS2.SERVER_SHARE_INFO	Server Share Information	Configuration	IBMi
QSYS2.SOFTWARE_PRODUCT	Server Software Product information	Configuration	IBMi
QSYS2.SYSCONTROLS	Permissions or column mask defined	Configuration	IBMi
QSYS2.SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration	IBMi
QSYS2.SYSDISKSTAT	Disk Information	Configuration	IBMi
QSYS2.SYSTEM_STATUS_INFO	Partition information	Configuration	IBMi
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration	IBMi
QSYS2.TELNET_ATTRIB	TELNET Server Attributes	Network	IBMi
QSYS2.USER_INFO	User Profile Information	Configuration	IBMi
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration	IBMi
REMOTE_TRAN_SUMMARY_BY_SERVER	Remote Summary Server	Network	IBMi
REMOTE_TRAN_SUMMARY_BY_USER	Remote Summary User	Network	IBMi
RSC_MGR_COMPLIANCE_DATA	Resource Manager Authority Out of compliance data	Network	IBMi
RSC_MGR_CONFIG	Resource Manager Configuration	Network	IBMi
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network	IBMi
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network	IBMi
SENSITIVE_DATABASE_CONTENT	Sensitive Database Content	Profile	IBMi
SERVICE_TOOL_SECURITY_ATTR	Service Tool Security Attributes	Profile	IBMi
SERVICE_TOOL_USERS	Service Tool User Data	Profile	IBMi
SOCKET_SUMMARY_BY_SERVER	Socket Summary by Server	Network	IBMi
SOCKET_SUMMARY_BY_USER	Socket Summary by User	Network	IBMi
SOCKET_TRAN_RULES	Socket Rules	Network	IBMi
SOCKET_TRANSACTIONS	Socket Transactions	Network	IBMi
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration	IBMi
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration	IBMi
SUBSYSTEM_COMMUNICATIONS	Subsystem Communication Entries	Configuration	IBMi
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration	IBMi
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration	IBMi
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration	IBMi
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration	IBMi
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration	IBMi
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration	IBMi
SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration	IBMi
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration	IBMi
SYS_VAL_CONFIG	System Value Configuration	Configuration	IBMi
SYS_VAL_DEFAULT	System Value Default	Configuration	IBMi
SYS_VAL_VALID	System Value Default	Configuration	IBMi
SYSCOLAUTH	Privileges Granted on a Column	Configuration	IBMi
SYSCONTROLS	Permission or Column Mask Defined	Configuration	IBMi
SYSCONTROLSDEP	Dependencies of Row Permissions and Column Masks	Configuration	IBMi
SYSCONTROLSDEP	Privileges Granted on a Row	Configuration	IBMi
SYSFIELDS	Columns with Field Procedures	Configuration	IBMi
SYSPACKAGEAUTH	Privileges Granted on a Package	Configuration	IBMi

Collector ID	Collector Name	Collector Category	Platform
SYSPROGRAMSTAT	Program, Service Program, and Module with SQL Statements	Configuration	IBMi
SYSROUTINEAUTH	Privileges Granted on a Routine	Configuration	IBMi
SYSSCHEMAAUTH	Privileges Granted on a Schema	Configuration	IBMi
SYSSEQUENCEAUTH	Privileges Granted on a Sequence	Configuration	IBMi
SYSTABAUTH	Privileges Granted on a Table or View	Configuration	IBMi
SYSTABLESTAT	Table Statistics Include all Partitions and Members	Configuration	IBMi
SYSTEM_VALUES	Display System Value Data	System	IBMi
SYSTOOLS.GROUP_PTF_CURRENCY	PTF Groups Installed per IBM Recommendations	Configuration	IBMi
SYSTOOLS.GROUP_PTF_DETAILS	PTFs within PTF Groups Installed per IBM Recommendations	Configuration	IBMi
SYSUDTAUTH	Privileges Granted on a Type	Configuration	IBMi
SYSVARIABLEAUTH	Privileges Granted on a Global Variable	Configuration	IBMi
SYSXSROBJECTAUTH	Privileges Granted on an XML Schema	Configuration	IBMi
TGMOBJINF	Object Information	Resource	IBMi
TG_NETWORK_GROUPS	TG Network Groups	Network	IBMi
TG_OBJECT_GROUPS	TG Object Groups	Network	IBMi
TG_OPERATION_GROUPS	TG Operation Groups	Network	IBMi
TG_USER_GROUPS	TG User Groups	Network	IBMi
USER_OBJECT_AUTHORITIES	User Profile Object Authorities	Profile	IBMi
USER_PRF_VIA_BLUEPRINT	User Profile via Blueprint	Profile	IBMi
USER_PROFILE_ACTIVITY	User Profile Activity	Profile	IBMi
USER_PROFILE_ARCHIVE	User Profile Archive	Profile	IBMi
USER_PROFILE_EXCLUSIONS	User Profile Exclusions	Profile	IBMi
USER_PROFILES	Display User Profile Data	Profile	IBMi

APPENDIX - TG Fix

The **TG Fix** tool allows you to install fixes via the TG menu quickly and easily. This feature also includes verification features that ensure the fix is installed properly.

See also

Working with TG Fix

APPENDIX - TG Management

The **TG Management** tool allows you to configure TG product administrative elements (e.g., licensing, user authorization, report output formats, etc.).

See also

Working with TG Management

APPENDIX - TG Save and Restore

The **TG Save and Restore** tool allows you to save the configuration of a specific instance of TGSecure or TGAudit. Once you save a configuration, you can then use that saved configuration file to do the following:

- Create a back-up (archive) of the current configuration to be used later to restore the configuration of an agent (server)
- Create multiple instances with identical configuration

A saved file stores the configuration for the following:

- Calendars
- Entitlement
- Groups
- Networks
- Reports
- Rules (i.e., Socket Rules, Exit Rules, etc.)

See also

Working with the TG Save and Restore

APPENDIX - TG Job Scheduler

The **TG Job Scheduler** tool allows you to select the desired scheduler:

- IBM
- IBMAJS
- ROBOT

See also

Working with the TG Job Scheduler

APPENDIX - TG Journal Cleanup

The **TG Journal Cleanup** (TGJRNCLEAN) tool is a command-line tool that allows you to manage journal receiver data.

Journaling is widely used on IBM i servers to keep track of database changes as well as system and security level audit information. Journal data cannot be altered or corrupted. Therefore, it is very useful for forensic analysis and makes IBM i the best platform for security. With all these journaling capabilities, cleaning up old journal data becomes a critical task for the system administrator or storage issues could result.

> **Important**: Before using this tool, review your data retention policy and make a backup of the receivers for later retrieval. In case of a security incident investigation, old receiver data is required for forensic analysis.

See also

Journal Cleanup Tool

Journaling Concepts

Journal Management

APPENDIX - TG Transaction Cleanup

The **TG Incoming Transaction Cleanup** (TGNTWCLEAN) tool is a command-line tool that allows you to manage incoming transaction data.

See also

Working with TGNTWCLEAN