NetIQ Security Solutions for IBM i
TG Central 2.1
User Guide
Revised August 2019

Legal Notice

Table of Contents

What's New in Version 2.1

Dashboard

You can now do the following:

- Display activity by server
- Display activity by user
- Display activity by type
- Display activity by operation server
- Display activity timeline
- Display platform. (A new column now appears in the server and report interfaces)

Network Security Defaults

You can now enable group inheritance.

See Manage Network Defaults for additional information.

Real Time Events

You can now do the following:

- Apply filter to alerts
- Reset alert filter
- Apply filter to network activities
- Reset network activity filter

Rules

You can now do the following:

- Work with Inactive Session Lockdowns
- Work with the Resource Manager

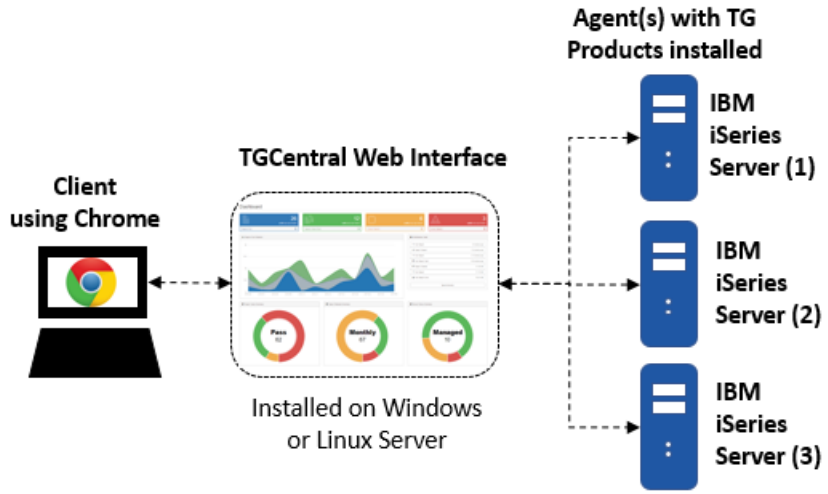
1. Introduction

1.1. TGCentral Overview

The Central Security Management console, which we will refer to as TGCentral in this guide, allows you to manage all your IBM i server security and compliance requirements from a single user interface.

In other words, TGCentral provides a centralized location (in the form of a web interface) from which a user can monitor security issues and update security features on agents. Agents, in this case, are IBM iSeries servers on which TG products (e.g., TGAudit and TGSecure) are installed.

Example usage: You are the administrator for some number IBM iSeries servers. Let say to make this example very specific. You purchase and install TGAudit and TGSecure for all three IBM iSeries servers. Without TGCentral, you would be required to log into each server and create the necessary components (i.e., rules, groups, etc.) necessary to secure properly each individual server. With TGCentral, you log into a single (web-based) dashboard from which you can update all three agents (i.e., IBM iSeries servers that have TG products installed.)



See also

Benefits

Features

Getting Started Using TGCentral

1.2. Benefits

TGCentral allows you to perform the same tasks you would perform via TGAudit or TGSecure but from a central location and with the benefit of accessing multiple agents. Agents, in this case, are IBM iSeries servers on which TG products (e.g., TGAudit and TGSecure) are installed.

TGCentral helps you do the following:

- Achieve regulation compliance across all your IBM i servers

- Minimize security breaches
- Easily maintain visibility of system security across your enterprise
- Save hundreds of resource hours that you would have used to build security reports based on industry security requirements (We've built those reports for you.)

1.3. Features

The following are the major system features:

- Dashboard - Provides a single user interface from which you can perform important security tasks
- Server Management - Allows you to view the status of all your IBM i servers
- Rules Management - Allows you to add, display, and modify IBM i server access rules
- Report Management - Allows you to access, manage, and analyze (identify the delta) all your IBM i server security reports
- Group Management - Allows you to work more efficiently by reducing repetitive tasks. Make a single change that impacts a group of networks, users, etc.
- Activity Management - Provides a role-base access control layer allowing you to provide granular permissions
- Administration - Allows you to define system settings

These features allow you to do the following:

- View security content covering the system journal, profiles, exit points, and access data
- View the pass/fail status of auditing report cards and then drill-down into those reports for additional details
- Access over 200 built-in reports that address industry compliance
- Create your own custom reports or report cards
- View detailed online help for reports

1.4. Roles

Each user must be assigned one of the following roles:

Role	Descriptions
ADMIN	Users in this role perform all TGCentral system actions: manage configuration, create/run/view reporting data. In addition, the admin manages users, grants permissions, and performs installation and maintenance tasks. **Note**: A larger organization might have many admins while a smaller organization might have a few, depending on resource availability. **Tip**: If a larger organization decides that they do not want to have one individual with the ability to perform all duties, then the organization can create new roles based on the admin role, and then limit the authorities for those roles. For example, they might create a role titled product admin that can only upgrade and maintain TGCentral and another role titled system admin that can perform all system tasks once the Product Admin installed TGCentral. **Note**: See User Permissions for a complete description of access levels.
SUPER USER	Users in this role perform all TGCentral system actions: manage configuration, create/run/view reporting data. A super user manages rules.

Role	Descriptions
HELP DESK	Users in this role manage agent groups/users, create/run/view reports, and create/run/view report cards. A help desk user provides troubleshooting assistance (e.g., logging in, using rules, running reports, etc.).
AUDITOR	Users in this role manage agent groups/users, create/run/view reports, and create/run/view report cards. An auditor view rules.
CREATOR	Users in this role create report and report card definitions.
READER	Users in this role view configuration and reporting data.

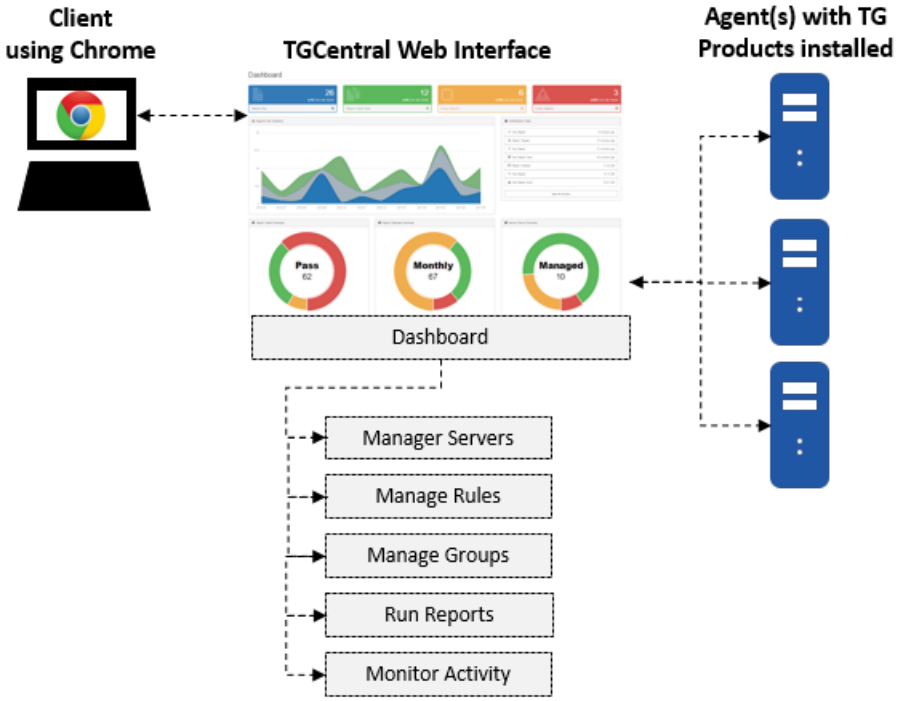
See also

User Permissions

2. Getting Started

TGCentral allows you to do the following for multiple agents:

- **View Dashboard** - See a high-level summary of activities from a central dashboard
- **Manage Servers** - Select which servers and server groups to monitor
- **Manage Rules** - Add and edit rules to control user access levels
- **Manage Groups** - Create groups to manage security more consistently and efficiently
- **Manage Calendars** - Create calendars to help limit enforcement of rules, entitlements, etc., to a specific time frame
- **Run Reports and Report Cards** - Run reports and report cards to monitor the security health
- **Monitor Activity** - View activities performed on a server



There is no single linear process for implementing or using TGCentral, but the following describes how a typical implementation might work. First, the admin tasks are described and then the user tasks are described.

2.1.1. Admin Tasks

Step 1	**Set Agent Status to *ACTIVE** For an agent to communicate with TGCentral, it must first be detected (seen). For TGCentral to detect an agent, its status must be set to *ACTIVE. To set the status of an agent to *ACTIVE, see the *TGCentral Installation Guide*. The activation of servers is part of the TGCentral installation and configuration process.

	Tip: If you have a TGCentral license, you can download the *TGCentral Installation Guide* from customer portal at TrinityGuard.com.
Step 2	**Create Roles** After installation of TGCentral, one of the first tasks the admin must complete is to create roles. You should create a role for each job category. Roles allow you to control access level. See Manage Roles for additional instructions on creating and modifying roles. **Tip:** A number of built-in roles are provided at the time of installation, See Permissions for a description of each built-in role and its associated access level.
Step 3	**Add Users** Once your project team establishes clear roles, then the administrator can begin adding users and assigning those users to a role. **Tip:** A user cannot access the system until an administrator adds the user and assign that user login credentials (i.e., username and password) See Manage Users for additional instructions.

2.1.2. User Tasks

Step 1	**Login** Contact your TGCentral admin and obtain the TGCentral URL specific to your organization and your unique login credentials (i.e., user name and password). See Login into TGCentral for additional instructions.
Step 2	**Add and remove servers** Determine which server(s) you want to manage. You can use TGCentral to manage as many or as few servers as necessary. See Manage Server for additional instructions.
Step 3	**Add and edit rules** Create and edit rules. Rules control access. **Tip**: You can distribute rules across multiple servers to promote consistency. See Manager Rules for additional instructions.
Step 4	**Add and edit groups** Create and edit groups. Groups allow you to work more efficiently. **Tip**: You can distribute groups across multiple servers to promote consistency. See the following topics for additional instructions: Manage User Groups Manage Object Groups Manage Operation Groups
Step 5	**Run reports and report cards** Run reports and report cards. Reports and report cards allow you to monitor the security health of your system. See the following topics for additional instructions: Manage Reports Manage Report Cards

Step 6	**Monitor activity** Monitor activities performed on each server. Activities are the tasks performed by TGCentral users (i.e., login attempts, report runs, rule modifications, etc.). See Manage Activities for additional instructions.
Step 7	**Modify user preferences** Each TGCentral user can modify their system settings to improve their user experience. See Manage Settings for additional instructions.

2.2. Log Into TGCentral

Use this task to log into TGCentral.

Important: Obtain the TGCentral URL specific to your organization and your user name and password from your TGCentral administrator.

To access TGCentral

1) Launch the web browser of your choice.
2) Enter the TGCentral URL in the address bar.
3) Press **Enter**.

Note: The **Sign In** dialog is displayed.

4) Enter your TGCentral username and password.
5) Click **Login**.

3. Dashboard

The dashboard provides quick access to TGCentral features from a central location.
Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

Use the dashboard to do the following:

- Customize dashboard
- Display report run activity
- Display report card run activity
- Display empty report activity
- Display error report activity
- Display run statistics
- Display activity history
- Display activity by server
- Display activity by user
- Display activity by type
- Display activity by operation server
- Display activity timeline
- Display report and report card summary
- Display scheduled report summary
- Display server status summary

3.1.1. Customize Dashboard

Use this task to customize the visual elements on the dashboard (e.g., reports, graphs, etc.).

To customize the dashboard

1) Select **Dashboard** in the left pane.
2) Click the **Dashboard** drop-down in the right pane.
3) Select the elements you want to show and deselect the elements you want to hide.

3.1.2. Display Report Run Activity

Use this task to display the activity status for reports run within the last month.

To display the report runs

1) Select **Dashboard** in the left pane.
2) Click **Reports Run** (blue icon at the top of the **Dashboard** pane).
3) Click the **Report Activity** tab.

Note: The **Report Activity** pane is displayed.

Tip: Click on a column heading to sort the list in ascending or descending order.

4) View the **Status** column to see the status of each report:

Status	Description
Completed	The report ran successfully and is ready for viewing
Processing	The report is still in progress and is not ready for viewing at this time
Error	The report did not run successfully because of an error

5) Click the **Action** button to manage (e.g., view, delete, run again, etc.) an activity.

Tip: To modify (edit) a report, see Manage Reports.

See also

Manage Reports

Manage Activities

3.1.3. Display Report Card Run Activity

Use this task to display the activity status of report cards.

To display the list of report card runs

1) Select **Dashboard** in the left pane.
2) Click **Report Cards Run** (green icon at the top of the **Dashboard** pane).
3) Click the **Report Activity** tab.

Note: The **Report Activity** pane is displayed.

Tip: Click on a column heading to sort the list in ascending or descending order.

4) View the **Status** column to see the status of each report card:

Status	Description
Completed	The report card ran successfully and is ready for viewing
Processing	The report card is still in progress and is not ready for viewing at this time
Error	The report card did not run successfully because of an error

5) Click the **Action** button to manage (e.g., view, delete, run again, etc.) an activity.

Tip: To modify (edit) a report card, see Manage Report Cards.

See also

Manage Activities

3.1.4. Display Empty Report Activity

Use this task to display the list of reports that returned zero rows (empty report). A report that returns zero rows (no data) might be appropriate in certain situations, but it might also indicate an issue. The **Empty Reports** option provides a quick way to identify and investigate empty reports.

To display the list of empty reports

1) Select **Dashboard** in the left pane.
2) Click **Empty Reports** (orange icon at the top of the **Dashboard** pane).
3) Click the **Report Activity** tab.

Note: The list of empty reports is displayed in the **Report Activity** pane.

Tip: Click on a column heading to sort the list in ascending or descending order.

4) Click the **Action** button to manage (e.g., view, delete, run again, etc.) a report.

Tip: To modify (edit) a report, see Manage Reports.

See also

Manage Reports

Manage Activities

3.1.5. Display Error Report Activity

Use this task to display the list of reports that returned errors (did not run successfully). The **Error Reports** option provides a quick way to identify and investigate reports that generated errors during a run.

To display the list of error reports

1) Select **Dashboard** in the left pane.
2) Click **Error Reports** (red icon at the top of the **Dashboard** pane).
3) Click the **Report Activity** tab.

Note: The list of error reports is displayed in the **Report Activity** pane.

Tip: Click on a column heading to sort the list in ascending or descending order.

4) Click the **Action** button to manage (e.g., view, delete, run again, etc.) a report.

Tip: To modify (edit) a report, see Manage Reports.

See also

Manage Reports

Manage Activities

3.1.6. Display Run Statistics

Use this task to display the monthly run statistics for both reports and report cards (in a comparison graph).
Note: The run statistics are displayed graphically. The X-axis represents time, and the Y-axis represents the number of runs.

To display the run statistics

1) Select **Dashboard** in the left pane.
2) View the **Report Run Statistics** graph to see a visual representation of the run statistics.
3) Hover your mouse over a point on the graph to see the name of the managed server represented in the graph.

See also

Manage Reports
Manage Report Cards

3.1.7. Display Activity History

Use this task to display the most recent activities.

To display the activity history

1) Select **Dashboard** in the left pane.
2) View the **Activity History** panel to see a list of the most recent activities (listed in chronological order).

Tip: Click the **View All Activity** button to access the **Activity** pane, which displays all activities in more detail.

3.1.8. Display Activity by Server

Use this task to display activities by server.

To display the activity by server

1) Select **Dashboard** in the left pane.
2) View the **Network Activity by Server** panel to see the list of the activities organized by server.

Tip: Use the timeframe option to filter the display by period (i.e., last week, last month, last three months, last six months, last year).

3.1.9. Display Activity by User

Use this task to display activities by user.

To display the activity by server

1) Select **Dashboard** in the left pane.
2) View the **Network Activity by User** panel to see the list of the activities organized by user.

Tip: Use the timeframe option to filter the display by period (i.e., last week, last month, last three months, last six months, last year).

3.1.10. Display Activity by Type

Use this task to display the activities by type (i.e., socket, exit level, pass, fail).

To display the activity by type

1) Select **Dashboard** in the left pane.
2) View the **Network Activity by Type** panel to see the list of the activities organized by type.

Tip: Use the timeframe option to filter the display by period (i.e., last week, last month, last three months, last six months, last year).

3.1.11. Display Activity by Operation Server

Use this task to display the activities by operation server (i.e., signon).

To display the activity by operation server

1) Select **Dashboard** in the left pane.
2) View the **Network Activity by Operation Server** panel to see the list of the activities organized by type.

Tip: Use the timeframe option to filter the display by period (i.e., last week, last month, last three months, last six months, last year).

3.1.12. Display Activity by Timeline

Use this task to display the activities by timeline (i.e., exit level, pass, fail).

To display the activity by timeline

1) Select **Dashboard** in the left pane.
2) View the **Network Activity by Timeline** panel to see the list of the activities organized along a timeline.

Tip: Use the timeframe option to filter the display by period (i.e., last week, last month, last three months, last six months, last year).

3.1.13. Display Report and Report Card Summary

Use this task to display totals for the following:

- Built-in (standard) reports
- Custom (client-specific) reports
- Built-in report cards
- Custom report cards

To display report and report card summary

1) Select **Dashboard** in the left pane.
2) View the **Report and Report Card Summary** donut chart.

Tip: Click on the different sections of the chart to see specific totals.

See also

Manage Reports
Manage Report Cards

3.1.14. Display Scheduled Report Summary

Use this task to display totals for the following:

- Ad-hoc scheduled report (scheduled to occur once)
- Daily scheduled reports (scheduled to occur daily)
- Weekly scheduled reports (scheduled to occur weekly)
- Monthly scheduled reports (scheduled to occur monthly)

To display scheduled report summary

1) Select **Dashboard** in the left pane.
2) View the **Report Scheduled Summary** donut chart.

Tip: Click on the different sections of the chart to see specific totals.

See also

Manage Reports
Manage Report Cards

3.1.15. Display Server Status Summary

Use this task to display totals for the following:

- Managed servers (collecting data for monitoring purposes)
- Unmanaged servers (not collecting data for monitoring purposes)

To display server status summary

1) Select **Dashboard** in the left pane.
2) View the **Server Status Summary** donut chart.

Tip: Click on the different sections of the chart to see specific totals.

See also

Manage Servers
Roles
User Permissions

4. Servers

4.1. Server Management

This section describes working with servers. Use the **Server Management** feature to do the following:

- Manage servers
- Manage server groups

The **Server** feature allows you to add, delete, modify, and import servers and server groups.

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

User Permissions

4.2. Manage Server

Use this task to do the following for servers you plan to manage:

Servers

- Display list of active servers
- Refresh list of active servers
- Display server details
- Display server activity history
- Add a server
- Delete a server
- Manage a Server
- Unmanage a Server
- Add server to group

Reports on Servers

- Run report on server
- Add scheduled report to server
- Delete scheduled report from server
- Disable scheduled report on server

Report cards on Servers

- Run report card on server
- Add scheduled report card to server
- Delete scheduled report card from server
- Disable scheduled report card on server

4.2.1. Display List of Active Servers

Use this task to view the list of active servers (agents).

In order for an agent to communicate with TGCentral, it must first be detected (seen and licensed). In order for TGCentral to detect an agent, its status must be set to *ACTIVE. To set the status of an agent to *ACTIVE, see the *TGCentral Installation Guide*. The activation of a server is part of the TGCentral installation and configuration process.

Tip: If you have TGCentral license, you can download the *TGCentral Installation Guide* from customer portal at TrinityGuard.com.

To display the list of servers

1) Expand the **Server Management** menu in the left pane.
2) Click on **Servers**.

Note: The **Servers** interface is displayed in the right pane.

Tip: Click on the column heading to sort the column items in ascending order. Click the column heading again to sort the items in descending order.

Field	Description
Server Name	Name assigned to the server
IP Address	IP address of the server
OS Version	Operating system version installed on the server
Platform	Identifies the platform: -- IBM i indicates an IBM i series server -- Linux indicates a Linux server
Status	**Managed**: TGCentral and the agent are communicating (sharing information) and are in sync **Unmanaged**: TGCentral and the agent are not communicating (not sharing information) and are not in sync **Unknown**: TGCentral and the agent are communicated, but the administrator has not yet determined if the server should be managed or unmanaged **Note**: If you see a gray dot beside the server name, it means the agent is either missing a TG product license or the license has expired. **Tip**: A color indicated should appear beside each server. -- A grey indicator icon (dot) appears when the server has been manually added, but TGCentral has not yet detected the TG products (e.g., TGSecure or TGAudit) necessary for integration (no agent detected). -- A **red** indicator icon (dot) appears when TGCentral detects the server, detects a valid license, but the server is offline (unable to communicated with TGCentral). -- A **green** indicator icon (dot) appears when TGCentral detects the server, detects a valid license, and the server is online (communicating with TGCentral).

	-- An **orange** indicator icon (dot) appears when TGCentral detects the server, the server is online, but a valid license is not detected (missing TGCentral license).
Action	Click on the **Action** button to see the list of tasks you can perform on the associated server

Note: Once you install TGCentral, you should use TGCentral exclusively to add, modify, or delete elements (i.e., rules, groups, reports, etc.). The system automatically pushes (syncs) actions that take place in TGCentral to the managed server. Keep in mind that this is a one-way sync. That is, elements modified in TGCentral are immediately pushed to the agent, but elements modified on the agent are not pushed to TGCentral. You can import elements from the agent to TGCentral.

4.2.2. Refresh List of Active Servers

Use this task at any time to refresh the **Servers** interface. This ensures that the information you are viewing in TGCentral is up-to-date.

To refresh the list of servers

1) Access the **Servers** interface.
2) Click the **Refresh** button.

Tip: A **Refresh** button is available for both the list of servers (top pane) and the server details (bottom pane)

4.2.3. Display Server Details

Use this task to view the details for a specific server (e.g., IP address, OS version, status, License, group)

To display the server details

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Details** tab.
4) View the server details in the bottom pane.

4.2.4. Display Server Activity History

Use this task to view the activity performed on a specific server. The server activity history includes the actions that have taken place on the server (e.g., addition of report, addition of report card).

To view the server activity history

Note: The **Servers** interface is displayed in the right pane.

1) Access the **Servers** interface.
2) Select a server by clicking on the server name.
3) Select the **Activity History** tab.
4) View the server activity history in the bottom pane.

4.2.5. Add Server

Normally, you don't need to add a server. Once you install TG software on a client (IBM) server and you set the client server status to *ACTIVE, TGCentral automatically detects the server. At which point, you only need to mark the server as managed or unmanaged. The only exception to this might be if you are performing a large

implementation. In such a case, you might want to pre-populate servers (create placeholders) in TGCentral. Creating or adding a server instance in TGCentral can be done fairly quickly; whereas, it might take much longer to prepare all the client servers for detection.

Tip: A grey indicator icon (dot) appears beside servers that were manually added, but that have not yet been detected by TGCentral.

To add a server

1) Access the **Servers** interface.
2) Click the **Add** button.
3) For each server you want to add, enter the following:

Field	Description
Server	Name you want to assign the server
IP Address	IP address of the server
OS Version	IBM operating version installed on the server

4) Click **Save**.

4.2.6. Delete Server

Use this task to delete a server from the list of active servers. If a server becomes decommissioned or no longer requires monitoring, it should be removed.

To delete a server

1) Access the **Servers** interface.
2) Click the **Action** button for the server you want to delete.
3) Select **Delete**.

4.2.7. Manage Server

Use this task to begin managing a server using TGCentral. A managed server is a server in which two-way communication is established. Once a server is marked as **Managed**, the system automatically begins pushing (syncing) modifications made in TGCentral to the managed server. Keep in mind that this is a one-way sync. That is, elements modified by a user in TGCentral are immediately pushed to the agent, but elements modified by a user on the agent are not pushed to TGCentral. You can import modified elements from the agent to TGCentral.

Note: A green indicator icon (dot) appears beside the name of managed servers.

To manage a server

1) Access the **Servers** interface.
2) Click the **Action** button for the server you want to begin managing.
3) Select **Manager Server**.

4.2.8. Unmanage a Server

Use this task to stop managing an active server using TGCentral. This is useful is a case where "noisy" activity might be occurring on the agent because of maintenance, testing, or decommissioning, etc., and it is not necessary for

those activities to be monitored and trigger notifications. Therefore, it might be useful to stop managing the agent for a period of time.

N**ote**: An orange indicator (dot) icon appears beside the name of unmanaged servers.

To unmanage a server

1) Access the **Servers** interface.
2) Click the **Action** button for the server you want to stop managing.
3) Select **Unmanage Server**.

4.2.9. Add Server to Group

Use this task to add a server to a server group to simplify management.
Note: See Manage Server Groups for additional information about server groups.

To add a server to a group

1) Access the **Servers** interface.
2) Click the **Action** button for the server you want to add to a group.
3) Select **Add to Server Group**.

Note: The **List of Server Groups** dialog is displayed.

4) Select the group to which you want to add the server.
5) Click **Save**.

4.2.10. Run Report on Server

Use this task to run a report on a specific server.

To run a report on a specific server

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Activity History** tab.
4) Click the **+ Run** button, and select **Report** from the list.

Note: The **Run Report** dialog appears.

5) Select the report you want to run from the list.
6) Click **Run Now**.

4.2.11. Add Scheduled Report to Server

Use this task to add a scheduled report. Schedules reports are run sometime in the future.

To add a scheduled report

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Schedule** tab.
4) Click the **+ New Schedule** button, and select **Report** from the list.

Note: The **Schedule Report** dialog is displayed.

5) Select the report you want to schedule from the list.

6) Complete the following fields:

Field	Description
Start Date	Start date on which the schedule is valid
End Date	End date on which the schedule becomes invalid
Frequency	How often the report should be run within the designated start and end date **One Day** - Once **Daily** - Once a day **Weekly** - Once a week **Monthly** - Once a month **Yearly** - Once a year
Time	Time at which the scheduled report should run

7) Click **Save**.

4.2.12. Delete Scheduled Report from a Server

Use this task to delete a scheduled report.

To delete a scheduled report

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Schedule** tab.

Note: The reports associated with the server are displayed in the bottom pane.

4) Click the **Actions** button for the scheduled report you want to delete.

5) Select **Delete**.

4.2.13. Disable Scheduled Report on Server

Use this task to disable a scheduled report temporally.

To disable a scheduled report

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Schedule** tab.

Note: The reports associated with the server are displayed in the bottom pane.

4) Click the **Actions** button for the scheduled report you want to disable.

5) Select **Disable Schedule**.

4.2.14. Run Report Card on Server

Use this task to run a report on a specific server.

To run a report card on a specific server

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Activity History** tab.
4) Click the **+ Run** button, and select **Report Card** from the list.

Note: The **Run Report Card** dialog appears.

5) Select the report card you want to run from the list.
6) Click **Run Now**.

4.2.15. Add Scheduled Report Card to Server

Use this task to add a scheduled report card.

To add a scheduled report card

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Schedule** tab.
4) Click the **+ New Schedule** button, and select **Report** from the list.

Note: The **Schedule Report Card** dialog is displayed.

5) Select the report card you want to schedule from the list.

6) Complete the following fields:

Field	Description
Start Date	Start date on which the schedule is valid
End Date	End date on which the schedule becomes invalid
Frequency	How often the report card should run within the designated start and end date **One Day** - Once **Daily** - Once a day **Weekly** - Once a week **Monthly** - Once a month **Yearly** - Once a year
Time	Time at which the scheduled report card should run

7) Click **Save**.

4.2.16. Delete Scheduled Report Card from a Server

Use this task to delete a scheduled report card.

To delete a scheduled report card

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Schedule** tab.

Note: The report cards associated with the server are displayed in the bottom pane.

4) Click the **Actions** button for the scheduled report card you want to delete.

5) Select **Delete**.

4.2.17. Disable Scheduled Report Card on Server

Use this task to disable a scheduled report card.

To disable a scheduled report card

1) Access the **Server** interface.
2) Select a server by clicking on the server name.
3) Select the **Schedule** tab.

Note: The reports associated with the server are displayed in the bottom pane.

4) Click the **Actions** button for the scheduled report card you want to disable.

5) Select **Disable Schedule**.

See also

- Manage Server Groups
- Manage Reports
- Manage Job Activity Rules

4.3. Manage Server Group

- Display list of server groups
- Refresh list of server groups
- Display list of servers in a server group
- Display server group activity history
- Add a server group
- Edit a server group
- Delete a server group
- Add a server to a server group
- Delete a server from a server group
- Add schedule report to server group
- Delete scheduled report from server group
- Disable scheduled server group report

4.3.1. Display List of Server groups

Use this task to view the list of server groups.

To display the list of server groups

1) Expand the **Server Management** menu in the left pane.
2) Click on **Server Groups**.

Note: The **Server Groups** interface is displayed.

Field	Description
Server Group Name	Name assigned to the server group
Action	Click on the **Action** button to see the list of tasks you can perform on the associated server group

Tip: Click on the column heading to sort the column items in ascending order. Click the heading again to sort the items in descending order.

4.3.2. Refresh List of Server Groups

Use this task at any time to refresh the **Server Groups** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the server groups.

To refresh the list of server groups

1) Access the **Server Groups** interface.
2) Click the **Refresh** button.

Tip: A **Refresh** button is available for both the list of server groups (top pane) and the server group details (bottom pane)

4.3.3. Display List of Servers in a Server Group

Use this task to view the list of servers in a server group. This provides an inventory of the group members.

To display the members of the server group

1) Access the **Server Group** interface.
2) Select a server group by clicking on the server group name.
3) Select the **Details** tab.

Note: The members of the group are displayed in the bottom pane.

Field	Description
Server Name	Name assigned to the server
IP Address	IP address of the server
OS Version	Operating system version installed on the server
Platform	Identifies the platform: -- IBM i indicates an IBM i series server -- Linux indicates a Linux server
Status	**Managed**: TGCentral and the agent are communicating (sharing information) and are in sync **Unmanaged**: TGCentral and the agent are not communicating (not sharing information) and are not in sync **Unknown**: TGCentral and the agent are communicated, but the administrator has not yet determined if the server should be managed or unmanaged

	Note: If you see a gray dot beside the server name, it means the agent is either missing a TG product license or the license has expired. **Tip**: A color indicated should appear beside each server. -- A grey indicator icon (dot) appears when the server has been manually added, but TGCentral has not yet detected the TG products (e.g., TGSecure or TGAudit) necessary for integration (no agent detected). -- A **red** indicator icon (dot) appears when TGCentral detects the server, detects a valid license, but the server is offline (unable to communicated with TGCentral). -- A **green** indicator icon (dot) appears when TGCentral detects the server, detects a valid license, and the server is online (communicating with TGCentral). -- An **orange** indicator icon (dot) appears when TGCentral detects the server, the server is online, but a valid license is not detected (missing TGCentral license).
Action	Click on the **Action** button to see the list of tasks you can perform on the associated server

4.3.4. Display Server Group Activity History

Use this task to view the server group activity history. The server group activity history includes the actions that have taken place on the member servers (e.g., addition of report, addition of report card).

To display the server group activity history

1) Access the **Server Group** interface.
2) Select a server group by clicking on the server group name.
3) Select the **Activity** tab.

Note: The activities associated with the server group are displayed in the bottom pane.

Field	Description
Server	IP address of the server
Report Name	Name of report
Date	Date on which report was run
Status	Status of the activity: **Completed** - Successful run **Processing** - In process (with percent complete) **Error** - An error stopped the report from completing
Action	Click on the **Action** button to see the list of tasks you can perform on the associated server

4.3.5. Add Server Group

Use this task to add a server group to the list of server groups.

To add a server group

1) Access the **Server Group** interface.
2) Click the **Add Server Group** button.

3) Enter the **Server Group Name**.
4) Click **Next**.
5) Select the server(s) you want included in the group and deselect the server(s) you want to exclude from the group.
6) Click **Save**.

4.3.6. Edit Server Group

Use this task to edit the server group. Editing might involve a group name change or adding and removing server(s) to or from the group.

To edit a server group

1) Access the **Server Groups** interface.
2) Click the **Actions** button.
3) Select **Edit**.
4) If you want to modify the **Server Group Name**, you can do that now.
5) Click **Next**.
6) Select the server(s) you want to include in the group and deselect the server(s) you want to exclude from the group.

Tip: Only servers detected (online or offline) by TGCentral may be added to a group. A red indicator icon (dot) appears beside servers that TGCentral detects, but that are offline (not communicated with TGCentral). A green indicator icon (dot) appears beside servers that TGCentral detects and that are online (communicating with TGCentral). A grey indicator icon (dot) appears beside servers that were manually added, but that have not yet been successfully detected by TGCentral

7) Click **Save**.

4.3.7. Delete Server Group

Use this task to delete a server group from the list of server groups.

To delete a server group

1) Access the **Server Groups** interface.
2) Click the **Action** button for the server group you want to delete.
3) Select **Delete**.

4.3.8. Add Server to Group

Use this task to add a server to a server group.

To add a server to a group

1) Access the **Server Groups** interface.
2) Click the **Actions** button for the server group you want to modify.
3) Select **Edit**.
4) If you want to modify the **Server Group Name**, you can do that now.
5) Click **Next**.
6) Select the server(s) you want to add to the group.
7) Click **Save**.

Tip: Alternatively, access the **Server** interface, and click the **Action** button and select **Add to ServerGroup** option.

4.3.9. Delete Server from Group

Use this task to delete a server from a server group.

To delete a server from a server group

1) Access the **Server Groups** interface.
2) Click on a server group to select it.

Note: The servers (members) associated with the server group are displayed in the bottom pane.

3) Click the **Details** tab.

4) Click the **Action** button beside the server you want to delete.
5) Select **Delete**.

4.3.10. Add Schedule Report to Server Group

Use this task to add a scheduled report.

To add a scheduled report to a server group

1) Access the **Server Group** interface.
2) Click on a server group to select it.
3) Select the **Schedule** tab.

Note: The reports associated with the server group are displayed in the bottom pane.

4) Click the **+ New Schedule** button.

Note: The **Schedule Report** dialog is displayed.

5) Select the report you want to schedule from the list.

6) Complete the following fields:

Field	Description
Start Date	Start date on which the schedule is valid
End Date	End date on which the schedule becomes invalid
Frequency	How often the report should run within the designated start and end date **One Day** - Once **Daily** - Once a day **Weekly** - Once a week **Monthly** - Once a month **Yearly** - Once a year
Time	Time at which the scheduled report should run

7) Click **Save**.

4.3.11. Delete Scheduled Report from Server Group

Use this task to delete a scheduled report.

To delete a scheduled report from a server group

1) Access the **Server Group** interface.
2) Click on a server group to select it.
3) Select the **Schedule** tab.

Note: The reports associated with the server group are displayed in the bottom pane.

4) Click the **Actions** button for the scheduled report you want to delete.

5) Select **Delete**.

4.3.12. Disable Scheduled Server Group Report

Use this task to disable a scheduled report.

To disable a scheduled report from a server group

1) Access the **Server Group** interface.
2) Click on a server group to select it.
3) Select the **Schedule** tab.

Note: The reports associated with the server group are displayed in the bottom pane.

4) Click the **Actions** button for the scheduled report you want to disable.

5) Select **Disable Schedule**.

See also

- Manage Servers
- Manage Reports

5. Rules

5.1. Rules Management

This section describes working with rules. Use the **Rules Management** feature to do the following:

Note: The rule types available are dependent on your license agreement.

Job Activity Monitor

Manage Job Activity Rules

Network Security

Manage Network Defaults

Manage Socket Rules

Manage Remote Exit Rules

Manage Exit Point Configuration

Access Escalation Management

Manage AEM Defaults

Manage Entitlements

Manage Access Control

Manage File Editors

Inactive Session Lockdown

Manage Inactive Session Lockdown Defaults

Manage Inactive Session Lockdown Rules

Manage Disconnect Options

Resource Manager

Manage Resource Manager Default

Manage Authority Collection Configuration

See also

User Permissions

5.2. Job Activity Monitor

5.2.1. Working with Job Activity Monitor

This section describes how to monitor job activities. The Job Activity Monitor gives you the ability to monitor the following:

- Activities performed by a specific user or user group on a designated server
- Activities performed on a specific subsystem on a designated server
- Command executed on a designated server

Note: For more information about Job Activity Monitor, see the TGAudit documentation on the customer portal at trinityguards.com.

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

Manage Job Activity Rules
Manage Subsystems
Manage Commands
Rules Management

5.2.2. Manage Job Activity Monitoring Rules

Job activity rules allow you to monitor the activities performed by a user or group of users. This is useful when auditing the activity of highly-privileged users who have access to sensitive information or who have the ability to run critical batch processes that impact important data. Job activity rules can also be used to filter (limit) the type of jobs data included in the job activity log. The job log is used to generate the following reports:

- Job Activity Details Report
- Job Activity Summary Report

Use this task to do the following:

- Display the list of job activity rules
- Refresh the list of job activity rules
- Edit a job activity rule
- Add a job activity rule
- Delete a job activity rule

5.2.2.1. Display List of Job Activity Rules

Use this task to view the list of job activity rules.

To display the list of job activity rules

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Job Activity Monitor** menu.
3) Select Job **Activity Monitor Rules**.

Note: The **Job Activity Monitor Rules** interface is displayed in the right pane.

Field	Description
Server	Name of server
User/Group	Name of user or user group impacted by the rule
Level	The log level (0-4): **0** - No messages are logged **1** - Log messages with log level greater than or equal to 1 **2** - Log messages with log level greater than or equal to 2 **3** - Log messages with log level greater than or equal to 3 **4** - Log messages with log level greater than or equal to 4
Severity	The severity level you want used in conjunction with the log level to determine which error messages are sent to job log (0-99).
Message	The text that will appear in the job log
Log CL	Status of CL (command-line) command logging ***YES** - Enable logging ***NO** - Disable logging
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.2.2.2. Refresh List of Job Activity Rules

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of job activity rules

1) Access the **Rules** interface.
2) Click the **Refresh** button.

5.2.2.3. Edit Job Activity Rule

Use this task to edit a job activity rule.

Note: You cannot edit the server.

To edit a job activity rule

1) Access the **Rules** interface.
2) Click the **Actions** button beside the rule you want to modify.
3) Select **Edit Rule**.
4) Modify the rule attributes as necessary:
5) Click **Save**.

5.2.2.4. Add Job Activity Rule

Use this task to add a job activity rule.

To add a job activity rule

1) Access the **Rules** interface.
2) Click the **Add** button.
3) Enter the necessary rule attributes.
4) Click **Save**.

5.2.2.5. Delete Job Activity Rule

Use this task to delete a job activity rule.

To delete a job activity rule

1) Access the **Rules** interface.
2) Click the **Actions** button beside the rule you want to delete.
3) Select **Delete**.

See also

Working with Job Activity Monitor
Rules Management

5.2.3. Manage Subsystems

You can use the Job Activity Monitor (JAM) to monitor a subsystem. When you add a subsystem, the system captures (logs) activities for users based on their job descriptions. You can limit or modify what is captured in the job monitor log by creating a job activity rule. Job activity rules take precedence over the user's job description. For example, if you add a subsystem, the system begins monitoring (logging) activities performed on that subsystems by each use. The activities logged will depend on the access rights defined for the user in their job description. If you have a number of users performing low-level tasks, the job activity log could become a huge file, so the administrator might want to limit what appears in the log by creating a jog activity rule. The rules allow you to define more precisely what you want to capture in the job activity log.

Example usage:

The administrator wants to begin monitoring activities on Subsystem 1, so the administrator adds Subsystem 1 to the list of subsystems to be monitored. The administrator finds that the job activity log is now huge because a user named Bob who works on Subsystem 1, performed a large number of low-level tasks. These low-level tasks have a very low probability of triggering a security issue; therefore, the administrator would like to exclude these tasks from the job activity log. To do this, the administrator creates a JAM rule that informs the system to only log higher level, high severity activities. This rule ensures that the low-level tasks are excluded from the log so that the administrator can focus on higher-level t asks.

Use this task to do the following:

- Display list of subsystems
- Refresh list of subsystems
- Edit a subsystem
- Add a subsystem
- Delete a subsystem

5.2.3.1. Display List of Subsystems

Use this task to view the list of subsystems.

To display the list of subsystems

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Job Activity Monitor** menu.
3) Select **Subsystems**.

Note: The **Subsystems** interface is displayed in the right pane.

Field	Description
Server	Name assigned to the server
Name	Name assigned to subsystem
Library	Name assigned to the library in which the subsystem resides
Description	Description of the subsystem
Log Status	Status of logging: ***ACTIVE** - Collect log data for job monitoring ***INACTIVE** - Do not collect log data for job monitoring
Action	Click on the **Action** button to see the list of tasks you can perform on the associated subsystem

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.2.3.2. Refresh List of Subsystems

Use this task at any time to refresh the **Subsystems** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of subsystems

1) Access the **Subsystems** interface.
2) Click the **Refresh** button.

5.2.3.3. Import Subsystems

Use this task to import subsystems from a managed server to TGCentral.

To import subsystems

1) Access the **Subsystems** interface.
2) Click the **Import** button.
3) Select the server from which you want to import the subsystem.
4) Click **Next**.

Note: The list of subsystems present on the server are displayed.

5) Select the subsystem you want to import.
6) Click **Import**.

Note: If the subsystem already exists in TGCentral for the specified server, the subsystem details in TGCentral will be overridden by the subsystem details present on the server at the time of import.

5.2.3.4. Export Subsystem

Use this task to export a subsystem to a server or group of severs.

To export a subsystem

1) Access the **Subsystems** interface.
2) Click the **Export** button.
3) Select the server(s) to which you want to export the subsystem.
4) Click **Next**.
5) Select the subsystem(s) you want to export.
6) Click **Save**.

Note: If the user subsystem already exists on the server, the system overrides the subsystem details defined on the server with the details defined in TGCentral at the time of export.

5.2.3.5. Edit Subsystem

Use this task to edit a subsystem. Editing might involve changing the log status.

To edit a subsystem

1) Access the **Subsystems** interface.
2) Click the **Actions** button beside the subsystem you want to modify.
3) Select **Edit**.
4) Modify the subsystem attributes as necessary:
5) Click **Save**.

5.2.3.6. Add Subsystem

Use this task to add a subsystem.

To add a subsystem

1) Access the **Subsystems** interface.
2) Click the **Add** button.
3) Enter the necessary subsystem attributes.
4) Click **Save**.

5.2.3.7. Delete Subsystem

Use this task to delete a subsystem.

To delete a subsystem

1) Access the **Subsystems** interface.
2) Click the **Actions** button beside the subsystem you want to delete.
3) Select **Delete**.

See also

Working with Job Activity Monitor

5.2.4. Manage Commands

You can use the job activity monitor to monitor specific commands. When you add a command, the system captures (logs) any instance when the specified command is executed on the designated server. This is helpful to identify who, when, and how often these commands are executed.

Use this task to do the following:

- Display list of commands
- Refresh list of commands
- Edit a command
- Add a command
- Delete a command

5.2.4.1. Display List of Commands

Use this task to view the list of commands.

To display the list of commands

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Job Activity Monitor** menu.
3) Select **Commands**.

Note: The **Commands** interface is displayed in the right pane.

Field	Description
Server	Name assigned to the server
Name	Name assigned to the command
Library	Library in which the command resides
Description	Description of the command
Action	Click on the **Action** button to see the list of tasks you can perform on the associated command

Tip: Click on the column heading to sort the column items in ascending order. Click the heading again to sort the items in descending order.

There are two things to keep in mind here:

First, during the initial installation, the following commands are automatically added. You should see these commands present in the list of commands after the installation is complete.

You have the option of deleting these commands if you do not want them to be tracked in the Job Activity log.

Tip: To ensure the most accurate monitoring of interactive user jobs, it's best to monitor all commands.

- ENDJOB
- SIGNOFF
- ENDJOBABN
- ENDPASTHR

Second, during a fresh install (iirc), these commands are not automatically added. You must add them manually. For additional information about these commands, refer to the TGAudit User Guide. All documentation is available via the customer portal.

5.2.4.2. Refresh List of Commands

Use this task at any time to refresh the **Commands** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of commands

1) Access the **Commands** interface.
2) Click the **Refresh** button.

5.2.4.3. Edit Command

Use this task to edit a command. Editing might involve changing the name and/or library.

To edit a command

1) Access the **Commands** interface.
2) Click the **Actions** button beside the command you want to modify.
3) Select **Edit**.
4) Modify the command attributes as necessary.
5) Click **Save**.

5.2.4.4. Add Command

Use this task to add a command.

To add a command

1) Access the **Command** interface.
2) Click the **Add New** button.
3) Enter the necessary command attributes.
4) Click **Save**.

5.2.4.5. Delete Command

Use this task to delete a command.

To delete a command

1) Access the **Commands** interface.
2) Click the **Actions** button beside the command you want to delete.
3) Select **Delete**.

See also

Working with Job Activity Monitor
Rules Management

5.3. Network Security

5.3.1. Working with Network Security

This section describes how to manage network security. Network security allows you to control who accesses your network.

See also

Manage Network Defaults

Manage Socket Rules

Manage Remote Exit Rules

Manage Exit Point Configuration

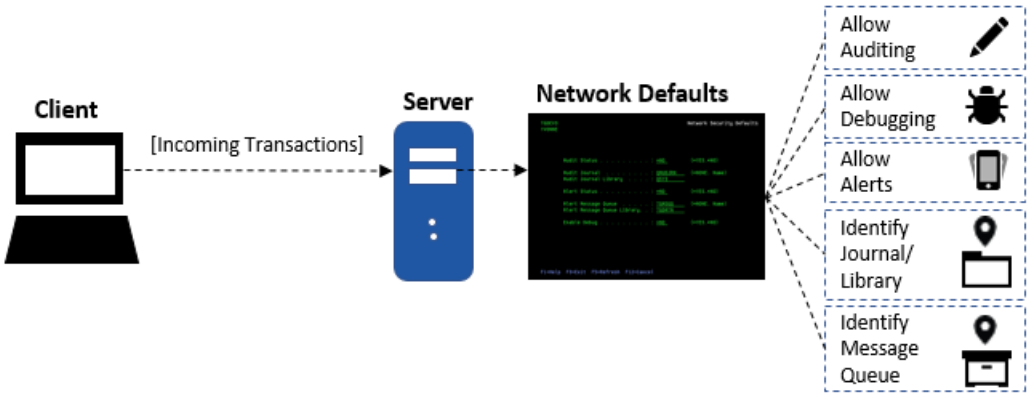
Rules Management

5.3.2. Manage Network Defaults

This section describes working with network security defaults.

Network security defaults define the following:

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



Use this task to do the following:

- Display network defaults
- Refresh list of network defaults
- Add network default
- Edit network default
- Delete network default

5.3.2.1. Display Network Defaults

Use this task to view the list of rule defaults.

To display the rule defaults

1) Expand the **Rules** menu in the left pane.
2) Expand the **Network Security** menu.
3) Select **Defaults**.

Note: The **Network Security Defaults** interface is displayed in the right pane.

Field	Description
Server	Server on which the network defaults are applicable
Audit Status	Whether to enable auditing: **Note**: Auditing is required if you plan to run network reports. ***YES** - Auditing enabled (record audit data) ***NO** - Auditing disabled (do not record audit data) **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.
Journal	Journal in which to store audit data
Library	Library in which the audit journal resides
Alert Status	Whether to enable alerting: ***YES** - Alerts enabled ***NO** - Alerts disabled
Message Queue	Queue in which to store alerts
Message Queue Library	Library in which to store alerts
Enable Debug	Whether to enable debugging: ***YES** - debug enabled ***NO** - debug disabled
Primary Group Inheritance	Whether to enable primary group inheritance: ***YES** - primary group inheritance enabled ***NO** - primary group inheritance disabled **Note**: The primary group is the user ID entered in the **Group profile** field when using command CHGUSRPRF. The primary group is the first ID from which a user inherits privileges.
Supplemental Group Inheritance	Whether to enable supplemental group inheritance: ***YES** - supplemental group inheritance enabled

	***NO** - supplemental group inheritance disabled **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.
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.3.2.2. Refresh List of Network Defaults

Use this task at any time to refresh the **Network Security Defaults** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of network defaults

1) Access the **Network Security Defaults** interface.
2) Click the **Refresh** button.

5.3.2.3. Edit Network Default

Use this task to edit a network default.

To edit a network default

1) Access the **Network Security Defaults** interface.
2) Click the **Actions** button beside the access control you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary.
5) Click **Save**.

5.3.2.4. Add Network Default

Use this task to add a network default.

To add a network default

1) Access the **Network Security Defaults** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.3.2.5. Delete Network Default

Use this task to delete a network default.

To delete a network default

1) Access the **Network Security Defaults** interface.
2) Click the **Actions** button beside the access control you want to delete.
3) Select **Delete**.

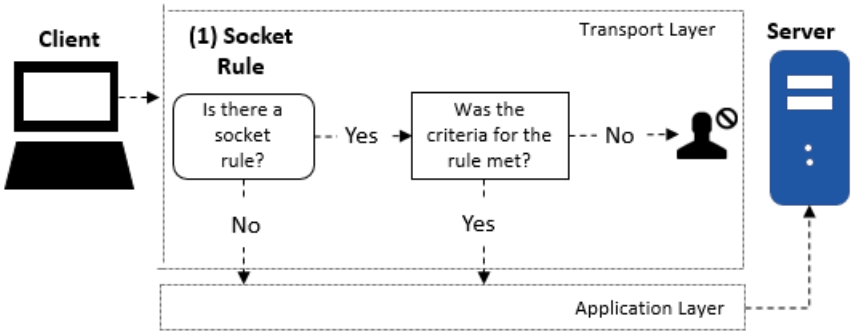
See also

Working the Network Security

Rules Management

5.3.3. Manage Socket Rules

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



Use this task to do the following:

- Display list of socket rules
- Refresh list of socket rules
- Edit socket rule
- Add socket rule
- Delete socket rule

5.3.3.1. Display List of Socket Rules

Use this task to view the list of socket rules.

To display the list of socket rules

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Network Security** menu.
3) Select Job **Socket Rules**.

Note: The **Socket Rules** interface is displayed in the right pane.

Field	Description
Server	Server on which the socket rule is applicable
User/Group	User or user group that initiated the transaction
Operation/Port	Port from which the transaction was initiated
Client IP	IP address from which the transaction was initiated

Calendar	Applicable calendar
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Socket Action	The level at which action is taken: ***EXITLVL** - Exit point level **Note**: If the action failed, you will see ***FAIL** in this column.
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.3.3.2. Refresh List of Socket Rules

Use this task at any time to refresh the **Socket Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of socket rules

1) Access the **Socket Rules** interface.
2) Click the **Refresh** button.

5.3.3.3. Edit Socket Rule

Use this task to edit a socket rule.

Note: You cannot edit the server.

To edit a socket rule

1) Access the **Socket Rules** interface.
2) Click the **Actions** button beside the rule you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.3.3.4. Add Socket Rule

Use this task to add a socket rule.

To add a socket rule

1) Access the **Socket Rules** interface.
2) Click the **Add** button.
3) Enter the necessary rule attributes.
4) Click **Save**.

5.3.3.5. Delete Socket Rule

Use this task to delete a socket rule.

To delete a socket rule

1) Access the **Socket Rules** interface.
2) Click the **Actions** button beside the rule you want to delete.
3) Select **Delete**.

See also

Working the Network Security

Rules Management

5.3.4. Manage Remote Exit Rules

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

Example Usage:

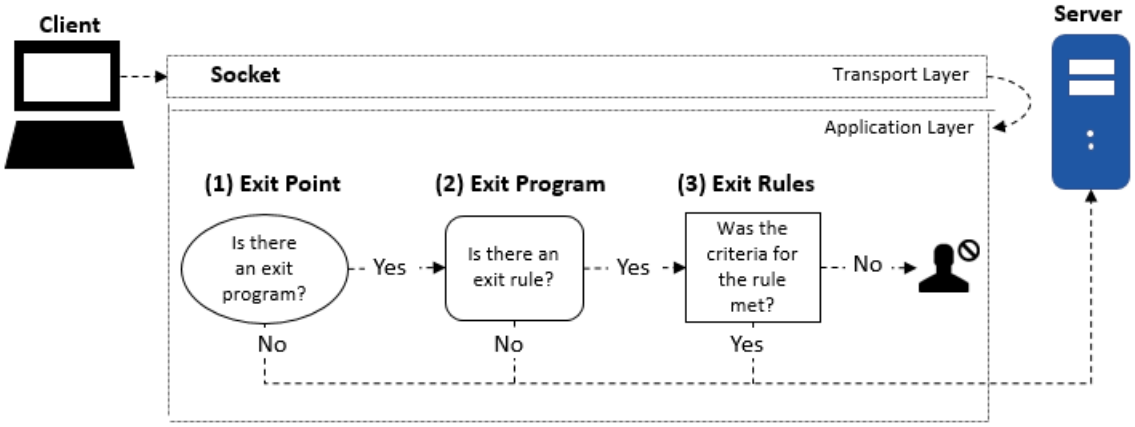
You might need a rule to reject all incoming transaction (connection) initiated by a specific user or member of a user group.

Client-Server Communication Process via transport layer:

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

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

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



Use this task to do the following:

- Display list of remote exit rules
- Refresh list of remote exit rules
- Edit remote exit rules
- Add remote exit rules
- Delete remote exit rules

5.3.4.1. Display List of Remote Exit Rules

Use this task to view the list of remote exit rules.

To display the list of remote exit rules

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Network Security** menu.
3) Select **Remote Exit Rules**.

Note: The **Remote Exit Rules** interface is displayed in the right pane.

Field	Description
Server	Server on which the exit rule is applicable
User/Group	User or user group that initiated the transaction
Operation Server	Server from which the transaction was initiated
Function	Function that was initiated
Client IP	IP address from which the transaction was initiated
Calendar	Applicable calendar
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Exit Rule 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
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.3.4.2. Refresh List of Remote Exit Rules

Use this task at any time to refresh the **Remote Exit Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of remote exit rules

1) Access the **Remote Exit Rules** interface.
2) Click the **Refresh** button.

5.3.4.3. Edit Remote Exit Rules

Use this task to edit a remote exit rule.

Note: You cannot edit the server.

To edit a remote exit rule

1) Access the **Remote Exit Rules** interface.
2) Click the **Actions** button beside the rule you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.3.4.4. Add Remote Exit Rules

Use this task to add a remote exit rule.

To add a remote exit rule

1) Access the **Remote Exit Rules** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.3.4.5. Delete Remote Exit Rules

Use this task to delete a remote exit rule.

To delete a remote exit rule

1) Access the **Remote Exit Rules** interface.
2) Click the **Actions** button beside the rule you want to delete.
3) Select **Delete**.

See also

Working the Network Security

Rules Management

5.3.5. Manage Exit Points

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

Analogy

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

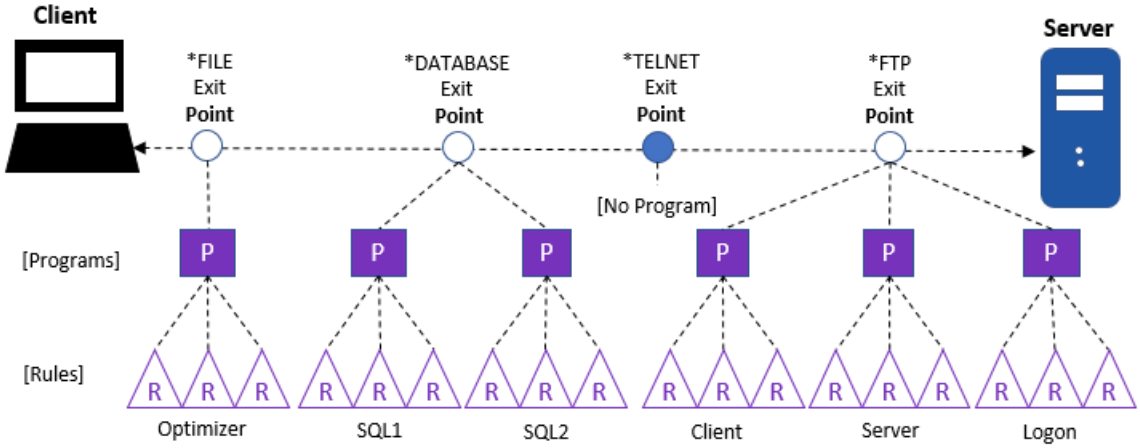
program) carries in its passengers (exit rules). Once an exit program is parked in an exit point, the rules (passengers) associated with that exit program become linked to the exit point.

Client-Server Communication Process via transport layer:

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

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

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



Use this task to do the following:

- Display list of exit point configurations
- Refresh list of exit point configurations
- Edit exit point configuration
- Add exit point configuration
- Delete exit point configuration
- Cycle server

5.3.5.1. Display List of Exit Point Configurations

Use this task to view the list of exit points.

To display the list of exit points

1) Expand the **Rules** menu in the left pane.
2) Expand the **Network Security** menu.
3) Select **Exit Point Config**.

Note: The **Exit Point Configuration** interface is displayed in the right pane.

Field	Description
Server	Server on which the exit point is applicable

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.
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.
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.
Collection 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
Network Description	A short description of the network
Functional Usage	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
Exit Inst?	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**.
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.3.5.2. Refresh List of Exit Point Configurations

Use this task at any time to refresh the **Exit Point Configuration** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of exit points

1) Access the **Exit Point Configuration** interface.
2) Click the **Refresh** button.

5.3.5.3. Edit Exit Point Configuration

Use this task to edit an exit point.

To edit an exit point

1) Access the **Exit Point Configuration** interface.
2) Click the **Actions** button beside the exit point you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.3.5.4. Add Exit Point Configuration

Use this task to add an exit point.

To add an exit point

1) Access the **Exit Point Configuration** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.3.5.5. Delete Exit Point Configuration

Use this task to delete an exit point.

To delete an exit point

1) Access the **Exit Point Configuration** interface.
2) Click the **Actions** button beside the exit point configuration you want to delete.
3) Select **Delete**.

5.3.5.6. 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 server

1) Access the **Exit Point Configuration** interface.
2) Click the **Actions** button beside the server you want to cycle.
3) Select **Cycle Server**.

See also

Working the Network Security

Rules Management

5.4. Access Escalation Management

5.4.1. Working with Access Escalation Management

This section describes how to escalate user access. Use the **Access Escalation Management** feature to allow user to swap profiles.

See also

Manage AEM Defaults

Manage Entitlements

Manage Access Control

Manage File Editors

Rules Management

5.4.2. Manage Access Escalation Management Defaults

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

Access escalation defaults allow you 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

Use this task to do the following:

- Display AEM defaults
- Refresh list of AEM defaults
- Edit AEM defaults
- Add AEM default
- Delete AEM default

5.4.2.1. Display AEM Defaults

Use this task to view the list of AEM defaults.

To display the list of AEM defaults

1) Expand the **Rules** menu in the left pane.
2) Expand the **Access Escalation Mgmt** menu.
3) Select **Defaults**.

Note: The **Access Escalation Defaults** interface is displayed in the right pane.

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

Field	Description
Server	Server on which the AEM defaults are applicable
Default Swap User	The default swap user (if one is not identified)
Authentication Timeout (Minutes)	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 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.
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Action	Click on the **Action** button to see the list of tasks you can perform on the associated AEM default

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.4.2.2. Refresh List of AEM Defaults

Use this task at any time to refresh the **Access Escalation Defaults** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of AEM defaults

1) Access the **Access Escalation Defaults** interface.
2) Click the **Refresh** button.

5.4.2.3. Edit AEM Defaults

Use this task to edit an AEM default.

To edit an AEM default

1) Access the **Access Escalation Defaults** interface.
2) Click the **Actions** button beside the AEM default you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.4.2.4. Add AEM Default

Use this task to add an AEM default.

To add an AEM default

1) Access the **Access Escalation Defaults** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.4.2.5. Delete AEM Default

Use this task delete an AEM default.

To delete an AEM Default

1) Access the **Access Escalation Defaults** interface.
2) Click the **Actions** button beside the AEM default you want to delete.
3) Select **Delete**.

See also

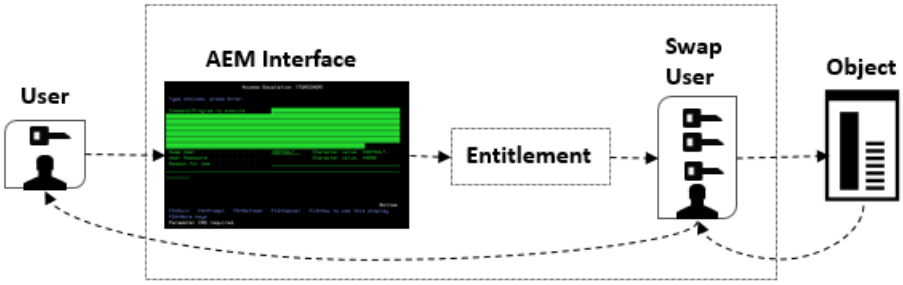
Working the Access Escalation Management

Rules Management

5.4.3. Manage User Entitlements

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

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



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

Use this task to do the following:

- Display list of entitlements
- Refresh list of entitlements
- Edit entitlements
- Add entitlements
- Delete entitlements

5.4.3.1. Display List of Entitlements

Use this task to view the list of entitlements.

To display the list of entitlements

1) Expand the **Rules** menu in the left pane.
2) Expand the **Access Escalation Mgmt** menu.
3) Select **Entitlements**.

Note: The **Entitlements** interface is displayed in the right pane.

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

Field	Description
Server	Server on which the socket rule is applicable
Enable Status	Whether the entitlement is enabled: **Y** - Enabled **N** - Disabled
User	User or user groups to which the entitlement applies
Object	Object or object groups 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
Calendar	Applicable calendar
Aut Req?	Whether 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
Description	Short description identifying the purpose of the entitlement
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.4.3.2. Refresh List of Entitlements

Use this task at any time to refresh the **Entitlements** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of entitlements

1) Access the **Entitlements** interface.
2) Click the **Refresh** button.

5.4.3.3. Edit Entitlements

Use this task to edit an entitlement.

Note: You cannot edit the server.

To edit an entitlement

1) Access the **Entitlements** interface.
2) Click the **Actions** button beside the entitlement you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.4.3.4. Add Entitlements

Use this task to add an entitlement.

To add an entitlement

1) Access the **Entitlements** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.4.3.5. Delete Entitlements

Use this task to delete an entitlement.

To delete an entitlement

1) Access the **Entitlements** interface.
2) Click the **Actions** button beside the entitlement you want to delete.
3) Select **Delete**.

See also

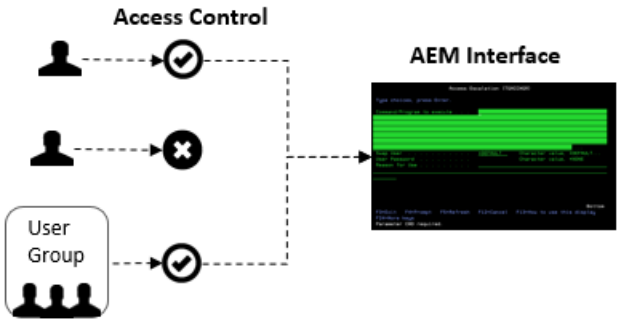
Working with Access Escalation Management
Rules Management

5.4.4. Manage Access Control

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

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

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



Use this task to do the following:

- Display access controls
- Refresh list of access controls
- Edit access controls
- Add access controls
- Delete access controls

5.4.4.1. Display Access Controls

Use this task to view the list of access control rules.

To display the list of access control

1) Expand the **Rules** menu in the left pane.
2) Expand the **Access Escalation Mgmt** menu.
3) Select **Access Control**.

Note: The **Access Control** interface is displayed in the right pane.

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

Field	Description
Server	Server on which the access control is applicable
User	User or user group to which the entitlement applies
Client IP	IP address from which the transaction was initiated
Action	Click on the **Action** button to see the list of tasks you can perform on the associated access control

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.4.4.2. Refresh List of Access Controls

Use this task at any time to refresh the **Access Control** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of access controls

1) Access the **Access Control** interface.
2) Click the **Refresh** button.

5.4.4.3. Edit Access Controls

Use this task to edit an access control.

To edit an access control

1) Access the **Access Control** interface.
2) Click the **Actions** button beside the access control you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.4.4.4. Add Access Controls

Use this task to add an access control rule.

To add an access control

1) Access the **Access Control** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.4.4.5. Delete Access Controls

Use this task to delete an access control.

To delete an access control

1) Access the **Access Control** interface.
2) Click the **Actions** button beside the access control you want to delete.
3) Select **Delete**.

See also

Working the Access Escalation Management

Rules Management

5.4.5. Manage File Editors

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

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

Use this task to do the following:

- Display file editors
- Refresh list of file editors
- Edit file editor
- Add file editor
- Delete file editor

5.4.5.1. Display File Editors

Use this task to view the list of file editors.

To display the list of file editors

1) Expand the **Rules** menu in the left pane.
2) Expand the **Access Escalation Mgmt** menu.
3) Select **File Editors**.

Note: The **File Editor** interface is displayed in the right pane.

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

Field	Description
Server	Server on which the file editor is applicable
Editor Command	Command to be executed
Editor Library	Library in which to execute the command
Editor Parameter	Parameter to be executed
Action	Click on the **Action** button to see the list of tasks you can perform on the associated file editor

5.4.5.2. Refresh List of File Editors

Use this task at any time to refresh the **File Editor** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of file editors

1) Access the **File Editor** interface.
2) Click the **Refresh** button.

5.4.5.3. Edit File Editor

Use this task to edit a file editor.

To edit a file editor

1) Access the **File Editor** interface.
2) Click the **Actions** button beside the file editor you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

5.4.5.4. Add File Editor

Use this task to add a file editor.

To add a file editor

1) Access the **File Editor** interface.
2) Click the **Add** button.
3) Enter the necessary attributes.
4) Click **Save**.

5.4.5.5. Delete File Editor

Use this task to delete a file editor.

To delete a file editor

1) Access the **File Editor** interface.
2) Click the **Actions** button beside the file editor you want to delete.
3) Select **Delete**.

See also

Working the Access Escalation Management

Rules Management
Rules Management

5.5. Inactive Session Lockdown

5.5.1. Working with Inactive Session Lockdown

This section describes how to work inactive session lockdown.

See also

Manage ISL Defaults

Manage ISL Rules

Manage Disconnect Options

Rules Management

5.5.2. Manage Inactive Session Lockdown Defaults

This section describes working with Inactive Session Lockdown (ISL) defaults.

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

5.5.2.1. Display ISL Defaults

Use this task to view the list of defaults.

To display the Resource Manager Defaults

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Inactive Sess. Lockdown** menu.
3) Select **Defaults**.

Note: The **Inactive Session Lockdown Defaults** interface is displayed in the right pane.

Field	Description
Server	Name of server
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 report
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.
Library	Library in which the journal resides
Alert Status	Whether alerts are enabled (stored in alert queue): ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Message Queue	Queue in which to store alerts
Message Queue Library	Library in which to store the queue
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.
Action	Click on the **Action** button to see the list of tasks you can perform on the associated enforcement

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.5.2.2. Refresh List of ISL Defaults

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of defaults

1) Access the **Rules** interface.
2) Click the **Refresh** button.

5.5.2.3. Edit ISL Default

Use this task to edit a default.

Note: You cannot edit the server.

To edit a default

1) Access the **Rules** interface.
2) Click the **Actions** button beside the default you want to modify.
3) Select **Edit**.
4) Modify the default attributes as necessary:
5) Click **Save**.

5.5.2.4. Add ISL Default

Use this task to add a default.

To add a default

1) Access the **Rules** interface.
2) Click the **Add** button.
3) Enter the necessary default attributes.
4) Click **Save**.

5.5.2.5. Delete ISL Default

Use this task to delete a default.

To delete a default

1) Access the **Rules** interface.
2) Click the **Actions** button beside the default you want to delete.
3) Select **Delete**.

See also

Working with Inactive Session Lockdown

Rules Management

5.5.3. Manage Inactive Session Lockdown Rules

The Inactive Session Lockdown (ISL) feature allows you 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 resource, 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.

Use this task to do the following:

- Display the list of ISL rules
- Refresh the list of ISL rules

- Add an ISL rule
- Edit an ISL rule
- Delete an ISL rule

5.5.3.1. Display List of Inactive Session Lockdown Rules

Use this task to view the list of Inactive Session Lockdown (ISL) rules.

To display the list of ISL rules

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Inactive Sess. Lockdown** menu.
3) Select **Inactive Session Rules**.

Note: The **Inactive Session Rules** interface is displayed in the right pane.

Field	Description
Server	Server on which the ISL rule is applicable
Rule Type	Type of rule: **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
Object	Object or object groups to which the ISL rule applies
Library	Library in which the object resides
Calendar	Applicable calendar
Disconnect Option	Name assigned to the disconnect option Note: ***Default** represent the default disconnect option defined for all object.
Rule Action	Action performed
Action	Click on the **Action** button to see the list of tasks you can perform on the associated rule

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.5.3.2. Refresh List of ISL Rules

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of ISL rules

1) Access the **Rules** interface.
2) Click the **Refresh** button.

5.5.3.3. Add ISL Rule

Use this task to add an ISL rule.

To add an ISL rule

1) Access the **Rules** interface.
2) Click the **Add** button.
3) Complete the following fields:

Field	Description
Server	Enter the server on which the ISL rule is applicable
Rule Type	Select the rule type: **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
User Name/Group	Enter the name of the user or group to which the rule applies **Tip**: To select from the list of existing groups, click the icon beside the field. This is a toggle field, so the first time you click the icon, the field switches (toggles) from a text-entry field to a drop-down selection field. Click on the drop-down arrow to select the desired group from the list. To toggle back to a text-entry field, click the icon again.
Object Library	Enter the library in which the object resides
Calendar	Enter the applicable calendar
Disconnect Option	Enter desired disconnect option Note: ***Default** represent the default disconnect option defined for all object.
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
Description	Enter a short description

4) Click **Save**.

5.5.3.4. Edit ISL Rule

Use this task to edit an ISL rule.

Note: You cannot edit the server.

To edit an ISL rule

1) Access the **Rules** interface.
2) Click the **Actions** button for the rule you want to modify.
3) Select **Edit Rule**.
4) Modify the rule attributes as necessary:
5) Click **Save**.

5.5.3.5. Delete ISL Rule

Use this task to delete an ISL rule.

To delete an ISL rule

1) Access the **Rules** interface.
2) Click the **Actions** button for the rule you want to delete.
3) Select **Delete**.

See also

Working with Inactive Session Lockdown

Rules Management

5.5.4. Manage Disconnect Options

Use this task to do the following:

- Display the list of disconnect options
- Refresh the list of disconnect options
- Edit a disconnect option
- Add a disconnect option
- Delete a disconnect option

5.5.4.1. Display List of Disconnect Options

Use this task to view the list of disconnect options.

To display the list of disconnect options

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Interactive Sess. Lockdown** menu.
3) Select **Disconnect Options**.

Note: The **Disconnect Options** interface is displayed in the right pane.

Field	Description
Server	Name of server
Disconnect Option	Name assigned to the disconnect option
Time Limit (minutes)	Time limit defined for the disconnect option
Disconnect type	Type of disconnect option: **ENDJOB** - End the job (user must start the job over) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - Signoff from the server

	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.
Action	Click on the **Action** button to see the list of tasks you can perform on the associated enforcement

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.5.4.2. Refresh List of Disconnect Options

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of disconnect options

1) Access the **Rules** interface.
2) Click the **Refresh** button.

5.5.4.3. Edit Disconnect Option

Use this task to edit a disconnect option.

Note: You cannot edit the server.

To edit a disconnect option

1) Access the **Rules** interface.
2) Click the **Actions** button beside the disconnect option you want to modify.
3) Select **Edit**.
4) Modify the disconnect option attributes as necessary:
5) Click **Save**.

5.5.4.4. Add Disconnect Option

Use this task to add a disconnect option.

To add a disconnect option

1) Access the **Rules** interface.
2) Click the **Add** button.
3) Enter the necessary disconnect option attributes.
4) Click **Save**.

5.5.4.5. Delete Disconnect Option

Use this task to delete a disconnect option.

To delete a disconnect option

1) Access the **Rules** interface.
2) Click the **Actions** button beside the disconnect option you want to delete.
3) Select **Delete**.

See also

Working with Inactive Session Lockdown

Rules Management

5.6. Resource Manager

5.6.1. Working with Resource Manager

This section describes how to work with the resource manager.

See also

Manage Resource Manager Default

Manage Authority Schemas

Manage Authority Schema Rules

Rules Management

5.6.2. Manage Resource Manager Defaults

This section describes working with Resource Manager defaults.

Resource Manager defaults allow you to identify 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

In order to work with the resource manager, you must access the **Resource Manager Defaults** interface.

5.6.2.1. Display Resource Manager Defaults

Use this task to view the list of defaults.

To display the Resource Manager Defaults

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Resource Manager** menu.
3) Select **Defaults**.

Note: The **Resource Manager Defaults** interface is displayed in the right pane.

Field	Description
Server	Name of server
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 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
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Action	Click on the **Action** button to see the list of tasks you can perform on the associated enforcement

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.6.2.2. Refresh List of Resource Manager Defaults

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of defaults

1) Access the **Rules** interface.
2) Click the **Refresh** button.

5.6.2.3. Edit Resource Manager Default

Use this task to edit a default.

Note: You cannot edit the server.

To edit a default

1) Access the **Rules** interface.
2) Click the **Actions** button for the default you want to modify.
3) Select **Edit**.
4) Modify the default attributes as necessary:
5) Click **Save**.

5.6.2.4. Add Resource Manager Default

Use this task to add a default.

To add a default

1) Access the **Rules** interface.
2) Click the **Add** button.
3) Enter the necessary default attributes.
4) Click **Save**.

5.6.2.5. Delete Resource Manager Default

Use this task to delete a default.

To delete a default

1) Access the **Rules** interface.
2) Click the **Actions** button for the default you want to delete.
3) Select **Delete**.

See also

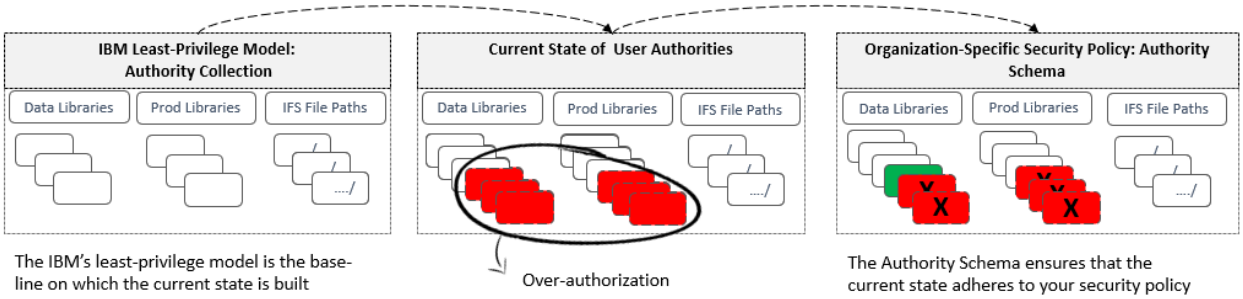
Working with Resource Manager

Rules Management

5.6.3. Manage Authority Schemas

This section describes working with authority schemas. Authority schemas allow you to define an architecture (template) for granting user authorities. Each authority scheme is the ideal model of how your organization should implemented 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:



Use this task to do the following:

- Display the list of schemas
- Refresh the list of schemas
- Edit a schema
- Add a schema
- Delete a schema
- Run a schema compliance report
- Run a schema enforcement

5.6.3.1. Display List of Schemas

Use this task to view the list of schemas.

To display the list of schemas

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Resource Manager** menu.
3) Select **Authority Schema Config**.

Note: The **Authority Schema Configuration** interface is displayed in the right pane.

Field	Description
Server	Name of server
Schema ID	ID assigned to the schema
Compliance Date	Date and time at which the last check for authority schema compliance was performed
Enforcement Date	Date and time at which user authorities where 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.
Action	Click on the **Action** button to see the list of tasks you can perform on the associated enforcement

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.6.3.2. Refresh List of Schemas

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of schemas

1) Access the **Authority Schema Configuration** interface.
2) Click the **Refresh** button.

5.6.3.3. Edit Schema

Use this task to edit a schema.

Note: You cannot edit the server.

To edit a schema

1) Access the **Authority Schema Configuration** interface.
2) Click the **Actions** button for the schema you want to modify.
3) Select **Edit**.
4) Modify the schema attributes as necessary:
5) Click **Save**.

5.6.3.4. Add Schema

Use this task to add a schema.

To add a schema

1) Access the **Authority Schema Configuration** interface.
2) Click the **Add** button.
3) Enter the necessary schema attributes.
4) Click **Save**.

5.6.3.5. Delete Schema

Use this task to delete a schema.

To delete a schema

1) Access the **Authority Schema Configuration** interface.
2) Click the **Actions** button for the schemas you want to delete.
3) Select **Delete**.

5.6.3.6. Run Schema Compliance Report

Use this task to run a report to identify non-compliance with a schema.

IMPORTANT: You should run this report before enforcing a schema.

To run the schema compliance report

1) Access the **Authority Schema Configuration** interface.
2) Click the **Actions** button for the schema you want to use to evaluate compliance.
3) Select **Run Compliance Report**.

5.6.3.7. Run Schema Enforcement

Use this task to apply the user-authority best practices defined in a schema.

IMPORTANT: Run the schema compliance report prior to enforcing a schema to identify non-compliance issues.

To enforce a schema

1) Access the **Authority Schema Configuration** interface.
2) Click the **Actions** button for the schema you want to enforce.
3) Select **Run Enforcement**.

See also

Working with Resource Manager

Manage Authority Schema Rules (Details)

Rules Management

5.6.4. Manage Authority Schema Rules

This section describes working with the authority schema rules (details).

Use this task to do the following:

- Display list of authority schema rules
- Refresh list of schema rules
- Add schema rule
- Edit schema rule
- Delete schema rule

5.6.4.1. Display List of Authority Schema Rules

Use this task to view the list of authority scheme rules (details), including exceptions.

To display the list of authority schema rules

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Resource Manager** menu.
3) Select **Authority Schema Config**.

Note: The **Authority Schema Configuration** interface is displayed in the right pane.

4) Click the **Details** tab.

Field	Description
Path or ASP	Either the file path for the IFS or the ASP (Auxiliary Storage Pool) for the system libraries **Note**: If you enter ***SYSBAS**, the system ASP and all basic user ASPs are included.
Library	Name of the library you want to monitor, or enter one of the following: ***ALL** - Include all libraries ***NONE** - Exclude all libraries

Object Name	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 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
Object Owner	Enter the name of the object owner
Auth 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 authority to access a specific object.
User Object	Name of the user (or group) that has access to the object
Exception	Whether the rule (detail) is an exception
Action	Click on the **Action** button to see the list of tasks you can perform on the associated enforcement

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

5.6.4.2. Refresh List of Schema Rules

Use this task at any time to refresh the **Rules** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of schemas rules

1) Access the **Authority Schema Configuration** interface.
2) Click the **Refresh** button.

5.6.4.3. Add Schema Rule

Use this task to add a schema rule (detail), including exceptions.

To add a schema rule

1) Access the **Authority Schema Configuration** interface.
2) Click the **Details** tab.
3) Click the **Add** button.
4) Complete the following field:

Field	Description
File System	Select ***SYS**.
Object Name	Enter the 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 begin with the letters identified are to be included. ***ALL** - Include all objects

Object Library	Enter the name of the library you want to monitor or enter one of the following: ***ALL** - Include all libraries ***NONE** - Exclude all libraries
Object Type	Enter the name of the object type or one of the following: ***ALL** - Include all object types
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 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
Exception	Identify whether the rule (detail) is an exception

5) Click **Save**.

5.6.4.4. Edit Schema Rule

Use this task to edit a schema rule (detail), including exceptions.

Note: You cannot edit the server.

To edit a schema

1) Access the **Authority Schema Configuration** interface.
2) Click the **Details** tab.
3) Click the **Actions** button for the schema rule (detail) you want to modify.
4) Select **Edit**.
5) Modify the schema rule attributes as necessary:
6) Click **Save**.

5.6.4.5. Delete Schema Rule

Use this task to delete a schema rule (detail), including exceptions.

To delete a schema rule

1) Access the **Authority Schema Configuration** interface.
2) Click the **Details** tab.
3) Click the **Actions** button for the schema rule you want to delete.
4) Select **Delete**.

See also

Working with Resource Manager

Rules Management

6. Groups

6.1. Group Management

This section describes working with groups. Use the **Group Management** feature to do the following:

- Manage user groups
- Manage Network/Server Groups
- Manage Operation Groups
- Manage Object Groups

The **Groups** feature allows you to add, delete, modify, and import groups for the purpose of organizing system elements. Once you create a group, you can use that group for different purposes. For example, you could use a group as a parameter when defining a rule. Therefore, the rule would apply to all user in the group.

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

User Permissions

6.2. Manage User Groups

This section describes working with user groups. User groups allow you to create a community of users. Once created, a rule can be applied to all members of a group, not just one individual. Therefore, user groups allow you to work more efficiently.

Use this task to do the following:

- Display the list of user groups
- Refresh the list of user groups
- Import user groups
- Export user group
- Edit as user group
- Add a user group
- Delete a user group

6.2.1. Display List of User Groups

Use this task to view the list of user groups.

To display the list of user groups

1) Expand the **Groups** menu in the left pane.
2) Click on **User Groups**.

Note: The **User Groups** interface is displayed in the right pane.

Field	Description

Server	Name of server in which the user group exists.
Name	Name assigned to the user group **Note**: User group names always begin with a colon.
Description	Description assigned to the user group
Action	Click on the **Action** button to see the list of tasks you can perform on the associated user group

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

6.2.2. Refresh List of User Groups

Use this task at any time to refresh the **Groups** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the servers.

To refresh the list of User Groups

1) Access the **User Groups** interface.
2) Click the **Refresh** button.

6.2.3. Import User Group

Use this task to import a user group.

To import a user group

1) Access the **User Groups** interface.
2) Click the **Import** button.
3) Select the server from which you want to import the user group.
4) Click **Next**.

Note: The list of user groups present on the server are displayed.

5) Select the user groups you want to import.
6) Do one of the following:
7) Click **Import**.

Note: If the user group already exists in TGCentral for the specified server, the user group details in TGCentral will be overridden by the user group details present on the server at the time of import.

6.2.4. Export User Group

Use this task to export a user group to a server or group of severs.

To export a user group

1) Access the **User Groups** interface.
2) Click the **Export** button.
3) Select the server(s) to which you want to export the user group.
4) Click **Next**.
5) Select the user group(s) you want to export.
6) Click **Save**.

Note: If the user group already exists on the server, the system overrides the user group details defined on the server with the details defined in TGCentral at the time of export.

6.2.5. Edit User Group

Use this task to edit a user group. Editing might involve changing the group description.

To edit a user group

1) Access the **User Groups** interface.
2) Click the **Actions** button beside the group you want to modify.
3) Select **Edit Group**.
4) Modify the group attributes as necessary:

Field	Description
Description	Description assigned to the user group

5) Click **Save**.

6.2.6. Add User Group

Use this task to add a user group.

To add a user group

1) Access the **User Groups** interface.
2) Click the **Add** button.
3) Enter the necessary group attributes:
4) Click **Save**.

6.2.7. Delete User Group

Use this task to delete a user group.

To delete a user group

1) Access the **User Groups** interface.
2) Click the **Actions** button for group you want to delete.
3) Select **Delete**.

6.3. Manage Network/Server Groups

This section describes working with network groups. Network groups allow you to create a community of networks or servers. Once created, a rule can be applied to all members of a group. Therefore, user groups allow you to work more efficiently.

Use this task to do the following:

- Display list of network groups
- Refresh list of network groups
- Edit network groups
- Add network groups

- Delete network groups

6.3.1. Display List of Network Groups

Use this task to view the list of network groups.

To display the list of network groups

1) Expand the **Groups** menu in the left pane.
2) Click on **Network/Server Groups**.

Note: The **Network Groups** interface is displayed in the right pane.

Field	Description
Server	Name of server in which the network group exists.
Name	Name assigned to the network group **Note**: Network group names always begin with a colon.
Description	Description assigned to the network group
Action	Click on the **Action** button to see the list of tasks you can perform on the associated network group

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

6.3.2. Refresh List of Network Groups

Use this task at any time to refresh the **Network Groups** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the servers.

To refresh the list of Network Groups

1) Access the **Network Groups** interface.
2) Click the **Refresh** button.

6.3.3. Edit Network Groups

Use this task to edit a network group. Editing might involve changing the group description.

To edit a network group

1) Access the **Network Groups** interface.
2) Click the **Actions** button beside the group you want to modify.
3) Select **Edit Group**.
4) Modify the group attributes as necessary:
5) Click **Save**.

6.3.4. Add Network Groups

Use this task to add a network group.

To add a network group

1) Access the **Network Groups** interface.
2) Click the **Add** button.
3) Enter the necessary group attributes:
4) Click **Save**.

6.3.5. Delete Network Groups

Use this task to delete a network group.

To delete a network group

1) Access the **Network Groups** interface.
2) Click the **Actions** button for group you want to delete.
3) Select **Delete**.

6.4. Manage Operation Groups

This section describes working with operation groups. Operation groups allow you to create a community of operations. Once created, a rule can be applied to all members of a group. Therefore, user groups allow you to work more efficiently.

Use this task to do the following:

- Display list of operation groups
- Refresh list of operation groups
- Edit operation groups
- Add operation groups
- Delete operation groups

6.4.1. Display List of Operation Groups

Use this task to view the list of operation groups.

To display the list of operation groups

1) Expand the **Groups** menu in the left pane.
2) Click on **Operation Groups**.

Note: The **Operation Groups** interface is displayed in the right pane.

Field	Description
Server	Name of server in which the operation group exists.
Name	Name assigned to the operation group **Note**: Operation group names always begin with a colon.
Description	Description assigned to the operation group
Action	Click on the **Action** button to see the list of tasks you can perform on the associated operation group

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

6.4.2. Refresh List of Operation Groups

Use this task at any time to refresh the **Operation Groups** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the servers.

To refresh the list of Operation Groups

1) Access the **Operation Groups** interface.
2) Click the **Refresh** button.

6.4.3. Edit Operation Groups

Use this task to edit an operation group. Editing might involve changing the group description.

To edit an operation group

1) Access the **Operation Groups** interface.
2) Click the **Actions** button beside the group you want to modify.
3) Select **Edit Group**.
4) Modify the group attributes as necessary:
5) Click **Save**.

6.4.4. Add Operation Groups

Use this task to add an operation group.

To add an operation group

1) Access the **Operation Groups** interface.
2) Click the **Add** button.
3) Enter the necessary group attributes:
4) Click **Save**.

6.4.5. Delete Operation Groups

Use this task to delete an operation group.

To delete an operation group

1) Access the **Operation Groups** interface.
2) Click the **Actions** button for group you want to delete.
3) Select **Delete**.

6.5. Manage Object Groups

This section describes working with object groups. Object groups allow you to create a community of objects. Once created, a rule can be applied to all members of a group. Therefore, user groups allow you to work more efficiently.

Use this task to do the following:

- Display list of object groups
- Refresh list of object groups
- Edit object groups
- Add object groups
- Delete object groups

6.5.1. Display List of Object Groups

Use this task to view the list of object groups.

To display the list of object groups

1) Expand the **Groups** menu in the left pane.
2) Click on **Object Groups**.

Note: The **Object Groups** interface is displayed in the right pane.

Field	Description
Server	Name of server in which the object group exists.
Name	Name assigned to the object group **Note**: Object group names always begin with a colon.
Description	Description assigned to the object group
Action	Click on the **Action** button to see the list of tasks you can perform on the associated object group

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

6.5.2. Refresh List of Object Groups

Use this task at any time to refresh the **Object Groups** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the servers.

To refresh the list of Object Groups

1) Access the **Object Groups** interface.
2) Click the **Refresh** button.

6.5.3. Edit Object Groups

Use this task to edit an object group. Editing might involve changing the group description.

To edit an object group

1) Access the **Object Groups** interface.
2) Click the **Actions** button beside the group you want to modify.
3) Select **Edit Group**.

4) Modify the group attributes as necessary:
5) Click **Save**.

6.5.4. Add Object Groups

Use this task to add an object group.

To add an object group

1) Access the **Object Groups** interface.
2) Click the **Add** button.
3) Enter the necessary group attributes:
4) Click **Save**.

6.5.5. Delete Object Groups

Use this task to delete an object group.

To delete an object group

1) Access the **Object Groups** interface.
2) Click the **Actions** button for group you want to delete.
3) Select **Delete**.

7. Calendars

7.1. Calendar Management

This section describes working with calendars. Use the **Calendar** feature to do the following:

- Manage calendars

7.2. Manage Calendars

This section describes working with calendars.

Use this task to do the following:

- Display list of calendars
- Refresh list of calendars
- Edit calendar
- Add calendar
- Delete calendar

7.2.1. Display List of Calendars

Use this task to view the list of calendars.

To display the list of object groups

1) Expand the **Calendar** menu in the left pane.
2) Click on **Calendar**.

Note: The **Calendar** interface is displayed in the right pane.

Field	Description
Server	Name of server in which the object group exists.
Calendar	ID used to identify the calendar
Start Date	Start date on which the calendar is valid
Start Time	Start time on which the calendar is valid
End Date	End date on which the calendar becomes invalid
End Time	End time on which the calendar becomes invalid
Description	Short description identifying the purpose of the calendar
Action	Click on the **Action** button to see the list of tasks you can perform on the associated calendar

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

7.2.2. Refresh List of Calendars

Use this task at any time to refresh the **Calendar** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the servers.

To refresh the list of Calendar

1) Access the **Calendar** interface.
2) Click the **Refresh** button.

7.2.3. Edit Calendar

Use this task to edit a calendar. Editing might involve changing the description.

To edit a calendar

1) Access the **Calendar** interface.
2) Click the **Actions** button beside the group you want to modify.
3) Select **Edit**.
4) Modify the attributes as necessary:
5) Click **Save**.

7.2.4. Add Calendar

Use this task to add a calendar.

To add a calendar

1) Access the **Calendar** interface.
2) Click the **Add** button.
3) Enter the necessary attributes:
4) Click **Save**.

7.2.5. Delete Calendar

Use this task to delete a calendar.

To delete a calendar

1) Access the **Calendar** interface.
2) Click the **Actions** button for group you want to delete.
3) Select **Delete**.

8. Reporting

8.1. Reporting Management

This section describes working with reports. Use the **Reporting** feature to do the following:

- Manage reports
- Manage report cards

The **Reports** feature allows you to add, delete, and modify reports for the purpose of monitoring the security health of your system.

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

User Permissions

8.2. Manage Reports

You can work with both built-in and custom reports.

Use this task to do the following:

- Display the list of reports
- Refresh the list of reports
- Add report
- Copy report
- Edit report
- Delete report
- Run report
- Schedule report
- Schedule report email notification

8.2.1. Display List of Reports

Use this task to view the list of reports available on the managed servers.

To display the list of reports

1) Expand the **Reporting** menu in the left pane.
2) Click on **Reports**.

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

Field	Description
Category	Report category (i.e., **Resource**, **Profile**, **Configuration**, etc.)

Report Name	Name assigned to the report
Collector ID	ID assigned to the collector
Collector	Journal collector from which report data is pulled
Built-in	**Y** (Yes): Pre-built report (delivered as part of the product) **N** (No): Custom report (specific to the client)
Platform	Identifies the platform: -- IBM i indicates an IBM i series server -- Linux indicates a Linux server
Action	Click on the **Action** button to see the list of tasks you can perform for the associated report (e.g., copy, run, schedule, etc.)

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

8.2.2. Refresh List of Reports

Use this task at any time to refresh the **Reports** interface. This ensures that the information you are viewing is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of reports

1) Access the **Reports** interface.
2) Click the **Refresh** button.

8.2.3. Add Report

Use this task to add a custom report.

To add a report

1) Access the **Reports** interface.
2) Click the **Add** button.
3) Enter the required report parameters.

Field	Description
Collector	Journal collector from which report data is pulled
Report ID	ID assigned to the report **Tip:** 30-characters max, must start with a letter, no spaces or special characters allowed
Report Name	Descriptive name for the report (100 characters max)
Category	Report category (i.e., Resource, Profile, Configuration, Network, etc.)

4) Click **Next**.
5) Select the fields (columns) you want to include in your report.
6) Click **Next**.
7) Enter exception parameters (boolean options) if desired.

Note: The boolean options allow you filter the data presented in the report output.

Tip: Click the + (plus sign) icon to add additional filters.

8) Click **Next**.
9) Complete the following fields:

Field	Description
From Date	Start date on which to begin reporting
To Date	End date on which to begin reporting
From Time	Start time at which to begin reporting
To Time	End time at which to begin reporting
User Name	Profile (user ID) of the user on which the report will be based or enter *ALL to collect data for all users
Email Report	Select this option if you want to schedule an email to generate each time the report is run. See Schedule Report Email Notification for additional information.

10) Click **Save**.

8.2.4. Copy Report

Use this task to copy a report.

To copy a report

1) Access the **Reports** interface.
2) Click the **Action** button for the report you want to copy.
3) Select **Copy**.
4) Enter the required report parameters.
5) Click **Next**.
6) Select the fields you want to include in your report.
7) Click **Next**.
8) Enter filter parameters if desired.

Tip: Click the + (plus sign) icon to add additional filters.

9) Click **Next**.
10) Enter the required date criteria.
11) Click **Save**.

8.2.5. Edit Report

Use this task to edit a custom report.

Note: Built-in reports cannot be edited. You can, however, create a custom report by copying an exiting built-in report, which makes it available for editing.

To view the report details

1) Access the **Reports** interface.
2) Click the **Action** button beside the report you want to edit.
3) Select **Edit**.

4) Make the necessary modifications.

Note: The edit option is only available (enabled) for custom reports.

8.2.6. Delete Report

Use this task to delete a custom report.

Note: This option is only available for customer reports (a report created by someone in your company), not built-in reports (a standard report delivered as part of the product).

Tip: The way to tell if a report is custom or built-in is by looking at the flag in the **Built-in** column.

To delete a report

1) Access the **Reports** interface.
2) Click the **Action** button for the report you want to delete.
3) Select **Delete**.

8.2.7. Run Report

Use this task to run a report.

To run a report

1) Access the **Reports** interface.
2) Click the **Action** button for the report you want to run.
3) Select **Run Report**.
4) Complete the following fields:

Field	Description
Server	Server on which you want to run the report
From Date	Start date on which to begin reporting
To Date	End date on which to begin reporting
From Time	Start time at which to begin reporting
To Time	End time at which to begin reporting
User Name	Profile (user ID) of the user on which the report will be based or enter *ALL to collect data for all users

5) Click **Run Now**.

Tip: To view the status of a report or to cancel a report, access the **Activity** interface and click the **Report Activity** tab.

Use this task to run a report.

8.2.8. Schedule Report

Use this task to schedule a report to run in the future. For example, as part of your security process, you might run reports at the close of business.

To schedule a report

1) Access the **Reports** interface.
2) Click the **Action** button for the report you want to schedule.
3) Select **Add to Schedule**.
4) Complete the following fields.

Field	Description
Server	Server on which you want to run the report **Tip**: The Server field will not appear if a report is available only on a single server.
From Date	Start date on which to begin reporting
To Date	End date on which to begin reporting
Frequency	How often the report should run within the designated start and end date **Ad-hoc** - Once on a specific day and time **Daily** - Once a day **Weekly** - Once a week **Monthly** - Once a month **Yearly** - Once a year
Time	Time at which the report should run

5) Click **Save**.

Tip: Access the **Servers** interface and select the **Schedule** tab to see all scheduled reports for a selected server.

See also

Manage Server Activities

8.2.9. Schedule Report Email Notification

Use this task to setup up an automatic email to a designated recipient when a report is run.

Tip: In addition, you can email a generate reports at any time. See Email Report Notification for additional information.

To schedule an email

1) Access the **Reports** interface.
2) Click the **Action** button for the desired report.
3) Select **Email Report**.

Note: The **Email Report** dialog is displayed.

4) Complete the following fields:

Field	Description
Report Format	Select the desired report format from the options available (e.g., PDF, CVS)
Always Recipients	Select the desire "always" recipient. The user(s) you select in this field will always receive an email when the report is run. You have the following options: **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users **User Group (Role)**: Click the **Select** option beside a user group (role) to send an email to all members of a user group

Alert Criteria	This field consists of two parts: **Expression**: Select a comparison operator (e.g., =, <=, >=) **Number**: Enter the number of report rows **Note**: When the number of rows in a generated report matches the alert criteria defined, the system sends the report via email to the designated recipients.
Security Recipients	Select the desire "security" recipient. The user(s) you select in this field will only receive an email when the alert criteria is met. You have the following options: **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users **User Group (Role)**: Click the **Select** option beside a user group (role) to send an email to all members of a user group

5) Click **Save**.

Tip: If the generated report exceeds the email server size limit, the designated recipient will receive an email notification and not the complete report. See Edit Mail Server Details for additional information about the email server size limit.

See also

Report Management

Manage Report Activities

Manage Settings

8.3. Manage Report Cards

Use this task to do the following:

- Display list of report cards
- Refresh list of report cards
- View detail for a specific report card
- Add report card
- Copy report card
- Edit report card
- Delete report card
- Schedule report card
- Schedule report card email notification
- Run report card
- Add exceptions to report card

8.3.1. Display List of Report Cards

Use this task to view the list of reports available on any of the managed servers.

To display the list of reports

1) Expand the **Reporting** menu in the left pane.
2) Click on **Report Cards**.

Note: The **Report Cards** interface is displayed.

Field	Description
Category	Report category (i.e., **Resource**, **Profile**, **Configuration**, etc.)
Report Card Name	Name assigned to the report
Built-in	**Y** (Yes): Pre-built report card delivered as part of the product **N** (No): Custom report card **Note**: An **N** (No) appears in this column for all report cards you create
Platform	Identifies the platform: -- IBM i indicates an IBM i series server -- Linux indicates a Linux server
Action	Click on the **Action** button to see the list of tasks you can perform for the associated report (e.g., copy, run, schedule, etc.)

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

8.3.2. Refresh List of Report Cards

Use this task at any time to refresh the **Report Cards** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed servers.

To refresh the list of report cards

1) Access the **Report Cards** interface.
2) Click the **Refresh** button.

8.3.3. View Report Card Details

Use this task to view the report card details.

To view the report card details

1) Access the **Report Cards** interface.
2) Click the **Action** button.
3) Select **View Details**.

8.3.4. Add a Report Card

Use this task to create a report card.

Tip: Report cards must consist of at least two or more reports.

To add a report card

1) Access the **Report Cards** interface.
2) Click the **Add** button.
3) Complete the following fields:

Field	Description
Card Name	Name you want to assign the report card
Category	Category to which the report card will be classified (e.g., Analysis, IFS, Regulator, etc) **Note**: For custom report cards, you can create custom category to help with organization

4) Click **Next**.
5) For each report you want to include in the report card, complete the following fields:

Field	Description
Report Name	Select the report you want to include from the list
Regulation Clause	Regulation associated with the report. This will help you later to identify which regulation requirement the report is monitoring.
Pass Criteria	Criteria (e.g., less than, greater than, equal to, etc.) used with the **Number of Rows** column to determine if the report card qualifies as a pass or fail
Number of Rows	Number of issues (rows) that will trigger a status of fail
Email Report Card	Select this option if you want to schedule an email to generate each time the report card is run. See for additional information.

Tip: Use the + (plus sign) icon to add additional reports to the report card. Use the trash can icon to delete a report from a report card.

Note: You are unable to save the report card until you add at least two reports.

6) Click the **Defaults** button to modify the default values used to run the report.

Note: The values you enter here are used in place of the default values defined for the report.

7) Click the **Exceptions** button to add failure exceptions.

Note: Exceptions might be necessary to temporarily or permanently disregard information (data) when determining the pass/fail status of the report.

8) Click **Save**.

See also

Add Exceptions to Report Card

Edit Report Defaults

8.3.5. Copy Report Card

Use this task to copy (clone) a report card.

To copy a report

1) Access the **Report Cards** interface.
2) Click the **Action** button for the report card you want to copy.
3) Select **Copy Report Card**.

8.3.6. Edit Report Card

Use this task to edit a custom report card.

Note: Built-in report cards cannot be edited. You can, however, create a custom report card by cloning an exiting built-in report card, which makes it available for editing.

To edit a report card

1) Access the **Report Cards** interface.
2) Click the **Action** button for the report card you want to edit.
3) Select **Edit**.
4) Make the necessary modifications.

Note: The edit option is only available (enabled) for custom report cards.

8.3.7. Delete Report Card

Use this task to delete a report card.

Note: This option is only available for customer report cards (a report card created by someone in your company), not built-in report cards (a standard report card delivered as part of the product).

Tip: The way to tell if a report card is custom or built-in is by looking at the flag in the **Built-in** column.

To delete a report card

1) Access the **Report Cards** interface.
2) Click the **Action** button for the report card you want to delete.
3) Select **Delete**.

8.3.8. Schedule Report Card

Use this task to schedule a report card to run.

To schedule a report card

1) Access the **Report Cards** interface.
2) Click the **Action** button for the report card you want to schedule.
3) Select **Add to Schedule**.

Note: The **Schedule Report** dialog is displayed.

4) Complete the following fields:

Field	Description
Server	Server on which you want to run the report **Tip**: The Server field will not appear if a report is available only on a single server.
Start Date	Start date on which to begin reporting
End Date	End date on which to begin reporting
Frequency	How often the report card should run within the designated start and end date **Ad-hoc** - Once on a specific day and time

	Daily - Once a day **Weekly** - Once a week **Monthly** - Once a month **Yearly** - Once a year
Time	Time at which to run the report card

5) Click **Save**.

8.3.9. Schedule Report Card Email Notification

Use this task to setup up an automatic email to a designated recipient when specific report card criteria are met.

Tip: In addition, you can email a generate report cards at any time. See Email Report Card Notification for additional information.

To email a report card when specific criteria is met

1) Access the **Reports** interface.
2) Click the **Action** button for the desired report.
3) Select **Email Report**.

Note: The **Email Report** dialog is displayed.

4) Complete the following fields:

Field	Description
Report Format	Select the desired report format from the options available (e.g., PDF, CVS)
Always Recipients	Select the desire "always" recipient. The user(s) you select in this field will always receive an email when the report card is run. You have the following options: **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users **User Group (Role)**: Click the **Select** option beside a user group (role) to send an email to all members of a user group
Alert Criteria	This field consists of two parts: **Expression**: Select a comparison operator (e.g., =, <=, >=) **Number**: Enter the number of report rows **Note**: When the number of rows in a generated report matches the alert criteria defined, the system sends the report via email to the designated recipients.
Security Recipients	Select the desire "security" recipient. The user(s) you select in this field will only receive an email when the alert criteria is met. You have the following options: **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users **User Group (Role)**: Click the **Select** option beside a user group (role) to send an email to all members of a user group

5) Click **Save**.

Tip: If the generated report card exceeds the email server size limit, the designated recipient will receive an email notification and not the complete report. See Edit Mail Server Details for additional information about the email server size limit.

8.3.10. Run Report Card

Use this task to run the report card.

Note: Report cards show the pass/fail status of multiple reports.

To run a report card

1) Access the **Report Cards** interface.
2) Click the **Action** button for the report card you want to run.
3) Select **Run Report Card**.
4) Complete the following fields:

Field	Description
Server	Server on which you want to run the report card

5) Click **Run Now**.

Tip: To view the status of a report or to cancel a report, access the **Activity** interface and click the **Report Activity** tab.

Note: To view the status of a report card or to cancel a report card, access the **Activity** interface.

See also

Activity Management

8.3.11. Add Exceptions to Report Card

Use this task to create a failure exception for a report card. Exceptions might be necessary to temporarily or permanently disregard a regulation. You can create an exception so that when the report card is run, criteria that normally would cause the report card to fail is disregarded.

Example usage:

For example, your company might install third-party software that requires high-level access to your data, but adding an additional high-level user account would trigger the failure of a regulatory compliance report that recommends that the number of high-level user accounts remain under a specific total. In this case, you would want to create an exception so that the report card would not continuously fail because of the additional of this single high-level user account.

Note: When you add an expect ion, the status of the report card displays as **Passed with Exception** instead of **Passed** to help qualify the pass status.

To add an exception to a report card

1) Access the **Report Cards** interface.
2) Click the **Action** button for the report card you want to edit.
3) Select **Edit**.
4) (Optional) Make any necessary modifications to the card name any/or category.
5) Click **Next**.
6) (Optional) Make any necessary modifications to the reports included in the report card.
7) Click the **Exceptions** button to add failure exceptions.
8) Click **Save**.

See also

Report Management

Manage Report Activities

Manage Settings

9. Activity

9.1. Activity Management

This section describes working with activities. Use the **Activity** feature to do the following:

- Manage report activities
- Manager server activities

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

User Permissions

9.2. Manage Report Activities

Use this task to do the following:

- Display list of report activities
- Refresh list of report activities
- View report as HTML
- View report as PDF
- View report messages
- View report card details
- Email report notification
- Email report card notification
- Export report as CSV
- Delete report from List of activities
- Rerun report
- Run delta report

9.2.1. Display List of Report Activities

Use this task to view the list of report activities.

To display list of report activities

1) Expand the **Activity** menu in the left pane.
2) Click the **Report Activity** tab.

Note: The **Report Activity** interface is displayed.

Field	Description
User	Name of user whom ran the report or report card last or the word "SCHEDULED" will appear in this field to indicate that this was a scheduled report
Server	Server from which the report data was obtained

Description	Description of the report or report card
Date	Date on which the report or report card was run
Type	This column identifies whether the activity involved a report or report card
Status	Status of the activity: **Completed** - Successful run **Processing** - In process (with percent complete) **Error** - An error stopped the report from completing
Action	Click on the **Action** button to see the list of tasks you can perform for the associated report/report card

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

9.2.2. Refresh List of Report Activities

Use this task at any time to refresh the **Report Activity** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on managed agent.

To refresh list of report activities

1) Access the **Report Activity** interface.
2) Click the **Refresh** button.

9.2.3. View Report as HTML

Use this task to view the HTML version of a report.

To view as HTML

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Depending on the type of activity you select, click **View Report** or **View Report Card**.

9.2.4. View Report as PDF

Use this task to view the PDF version of the report.

To view as PDF

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **View PDF**.

9.2.5. View Report Messages

Use this task to view the system messages associated with the report activity.

To view report messages

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **View Messages**.

9.2.6. View Report Card Details

Use this task to view the run details for the reports associated with a report card.

To view report card details

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report card.
3) Select **View Details**.

Note: The list of reports associated with the report card are displayed.

4) Click on a report to view the details.

9.2.7. Email Report Notification

Use this task to email a generated report to a designated recipient immediately.

Tip: Alternatively, you can schedule emails to generate automatically each time a report is run. See Schedule Report Email Notification for additional information.

To email a report

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Email Report**.

Note: The **Email Report** dialog box is displayed.

4) Complete the following fields:

Field	Description
Report Type	Select the desired report format from the options available (e.g., PDF, CVS)
Recipients	Select the desire recipient. You have the following options: **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users **User Group (Role)**: Click the **Select** option beside a user group (role) to send an email to all members of a user group

5) Click **Send**.

Tip: If the generated report exceeds the email server size limit, the designated recipient will receive an email notification and not the complete report. See Edit Mail Server Details for additional information about the email server size limit.

9.2.8. Email Report Card Notification

Use this task to email a report to a designated recipient.

Tip: Alternatively, you can schedule emails to generate automatically each time a report card is run. See Schedule Report Card Email Notification for additional information.

To email a report card

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Email Report**.

Note: The **Email Report** dialog box is displayed.

4) Complete the following fields:

Field	Description
Report Card Format	Select the desired report format from the options available (e.g., PDF, CVS)
Recipients	Select the desire recipient. You have the following options: **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users **User Group (Role)**: Click the **Select** option beside a user group (role) to send an email to all members of a user group

5) Click **Send**.

Tip: If the generated report exceeds the email server size limit, the designated recipient will receive an email notification and not the complete report. See Edit Mail Server Details for additional information about the email server size limit.

9.2.9. Export Report as CSV

Use this task to export a CSV (spreadsheet) version of the report.

To export as CSV file

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Export CSV**.

9.2.10. Delete Report from List of Activities

Use this task to delete the report activity. When you delete the report activity, you are deleting the record of the run, not the actual report. You can also use this option if you want to cancel a report run.

Tip: To delete a report or report card, you must access the Reports or Reports Card interface.

To delete a report activity

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Delete**.

9.2.11. Rerun Report

Use this task to rerun the report. This is useful if you want to rerun the report using the exact same run parameters (start time, end time, etc.).

Tip: To run the report using different run parameters, you must access the Reports or Reports Card interface.

To delete a report activity

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Run Again**.

9.2.12. Run Delta Report

Use this task to run the report again (using the same parameters from a previous run), but only show the changes.

Tip: To run the report using different run parameters, you must access the Reports or Reports Card interface.

To run a delta report

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Run Delta**.

Note: The **Select Report** dialog is displayed.

4) Select the report to which you want to compare the current report to identify the delta (change).

Tip: If the dialog shows no reports to select, then there is no report history on which to base a delta (change) report.

See also

Manage Reports

Manage Report Cards

Manage Settings

9.3. Manage Server Activities

Use this task to do the following:

- Display list of server activities
- Refresh list of server activities
- Search list of server activities

9.3.1. Display List of Sever Activities

Use this task to view the list of activities on a specific server.

To display the list of activities

1) Expand the **Activity** menu in the left pane.
2) Click the **Activity** tab.

Note: The **Server Activity** interface is displayed.

Field	Description
User	Name of the user who performed the activity
Server	Server on which the activity was performed

Description	Description of the activity
Date	Date on which the activity was performed
Type	Type of activity: **JAM** - Activity involving a job activity rule **Report** - Activity involving a report **Report Card** - Activity involving a report card **User** - Activity involving a user group
Status	Status of the activity: **Completed** - Successful run **Processing** - In process (with percent complete) **Error** - An error stopped the report from completing

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

9.3.2. Refresh List of Server Activities

Use this task at any time to refresh the **Activity** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed agent.

To refresh the list of activities

1) Access the **Activity** interface.
2) Click the **Activity** tab.
3) Click the **Refresh** button.

9.3.3. Search List of Server Activities

Use this search for a specific activity.

To search the list of activities

1) Access the **Activity** interface.
2) Click the **Activity** tab.
3) Enter the desired search term in the **Search** field.

See also

Manage Report Activities

Manage Reports

10. Real Time Events

10.1. Real Time Event Management

This section describes working with real time events (incoming transactions). Use the **Real Time Event** feature to do the following:

- Manage Network Activity
- Manage Alerts

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

User Permissions

10.2. Manage Network Activity

This section describes working with network activities.

Use this task to do the following:

- Customize Network Activity interface
- Display list of network activities
- Refresh list of network activities
- Search network activities
- Apply filter to network activities
- Reset network activity filter

10.2.1. Customize Network Activity Interface

Use this task to customize the columns displayed in the Network Activity interface.

To customize the Network Activity Interface

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.

Note: The **Network Activity** interface is displayed in the right pane.

3) Click the **Show** button (in the right pane).
4) Select the columns you want to show and deselect the columns you want to hide.

10.2.2. Display List of Network Activities

Use this task to view the list of activities (incoming transactions) on all servers.

To display the list of network activities

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.

Note: The **Network Activity** interface is displayed in the right pane.

Field	Description
Server	Server on which the activity was performed
Type	Type of activity: **JAM** - Activity involving a job activity rule **Report** - Activity involving a report **Report Card** - Activity involving a report card **User** - Activity involving a user group
User	Name of user performed the activity
OP Server	Operation server
Function	Function
SSL	Secure socket layer certificate
Client IP	IP address from which the transaction was initiated
Count	Number of transactions
Status	Status of activity
Object Details	Description of object involved in transaction
Timestamp	Time at which transaction occurred
Action	Click on the **Action** button to see the list of tasks you can perform on the associated activity

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

10.2.3. Refresh List of Network Activities

Use this task at any time to refresh the **Network Activity** interface. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed agent.

To refresh the list of activities

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.
3) Click the **Refresh** button.

10.2.4. Search List of Network Activities

Use this task to search for a specific activity.

To search the list of activities

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.

3) Enter the desired search term in the **Search** field.

10.2.5. Apply Filter to Network Activities

Use this task to limit the list of network activities displayed based on selection criteria.

To apply a filter

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.
3) Click the **Filter** button.
4) Enter the desired selection criteria in the fields provided.
5) Click the **Filter** button.

10.2.6. Reset Network Activity Filter

Use this task to remove an applied filter.

To reset the filter

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.
3) Click the **Reset Filter** button.

See also

Real Time Event Management

10.3. Manage Alerts

This section describes working with alerts.

Use this task to do the following:

- Customize Alerts Interface
- Display list of alerts
- Refresh list of alerts
- Search list of alerts
- Apply filter to alerts
- Reset alter filter

10.3.1. Customize Alerts Interface

Use this task to customize the columns displayed in the **Alerts** interface.

To customize the Alerts Interface

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Alerts**.

Note: The **Alerts** interface is displayed (in the right pane).

3) Click the **Show** button (in the right pane).
4) Select the columns you want to show and deselect the columns you want to hide.

10.3.2. Display List of Alerts

Use this task to view the list of alerts.

To display the list of alerts

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Alerts**.

Note: The **Alerts** interface is displayed (in the right pane).

Field	Description
Message	Message text
Message ID	ID assigned to the message
Severity	Severity of the message
Timestamp	Time at which transaction occurred
Type	Type of alert: ***CMD** - Command executed ***EMAIL**- Email sent ***MSG** - System (login) message queued ***SYSLOG** - Syslog communication initiated

10.3.3. Refresh List of Alerts

Use this task at any time to refresh the list of alerts. This ensures that the information you are viewing in TGCentral is up-to-date (synchronized) with the information on the managed agent.

To refresh the list of alerts

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Alerts**.
3) Click the **Refresh** button.

10.3.4. Search List of Alerts

Use this search for a specific alert.

To search the list of alerts

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Alerts**.
3) Enter the desired search term in the **Search** field.

10.3.5. Apply Filter to Alerts

Use this task to limit the list of alerts displayed based on selection criteria.

To apply a filter

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.
3) Click the **Filter** button.
4) Enter the desired selection criteria in the fields provided.
5) Click the **Filter** button.

10.3.6. Reset Alert Filter

Use this task to remove an applied filter.

To reset the filter

1) Expand the **Real Time Events** menu (in the left pane).
2) Select **Network Activity**.
3) Click the **Reset Filter** button.

See also

Real Time Event Management

11. Admin

11.1. Administration Management

This section describes how to manage TGCentral users, which is separate and distinct from the management of IBM i users.
Note: Any action performed in the **Admin** section of TGCentral are specific to the TGCentral GUI, not the IBM iSeries server.
Use this feature to do the following:

- Manage TGCentral Users
- Manage TGCentral Roles
- Manage TGCentral Settings
- Manage TGCentral Agent Configuration

Tip: The features available to each user are dependent on the user's permission level, which is based on their assigned role.

See also

User Permissions

11.2. Manage Users

Important: Any action performed in the **Admin** section of TGCentral are specific to the TGCentral GUI, not the IBM iSeries server.

Use this task to do the following:

- Display list of users
- Add a user
- Edit a user
- Disable user
- Enable user
- Delete a user

11.2.1. Display List of Users

Use this task to view the list of users who have access to TGCentral.

To display the list of users

1) Expand the **Admin** menu in the left pane.
2) Click on **Users**.

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

Field	Description
Login	Login ID assigned to the TGCentral user

Full Name	Full name of user
Email	User's email address **Note**: This will be used for notifications.
Group	TGCentral group to which the user is assigned
Role	TGCentral role to which the user is assigned **Tip**: A user's permission level is dependent on the role assigned to the user.
Language	Language in which interface text should be presented
Date	Date on which the user was granted access (added) to TGCentral
Action	Click on the **Action** button to see the list of tasks you can perform for the associated user

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

See also

User Permissions

11.2.2. Add User

Use this task to add a new TGCentral user.

To add a user

1) Access the **Users** interface.
2) Click the **Add** button.
3) Complete the following fields:

Field	Description
Username	ID you want to assign the new user
Full Name	Full name of user
Email	User's email address **Note**: This will be used for notifications.
Password	Initial password assigned to the user Note: The user should change the password immediately.
Server Group	TGCentral group to which the user is assigned
Role	TGCentral role to which the user is assigned **Tip**: A user's permission level is dependent on the role assigned to the user.
Language	Language in which interface text should be presented
Theme	Theme (color scheme) applied to the user interface
Allow Multiple Access	Select the appropriate option: **Yes** - Allow the user to log in from different machines concurrently **No** - Do not allow the user to log in from different machines concurrently

4) Click **Save**.

See also

User Permissions

11.2.3. Edit User

Use this task to edit an existing TGCentral user.

To modify a user

1) Access the **Users** interface.
2) Click the **Action** button.
3) Select **Edit User**.
4) Modify the user parameters.
5) Click **Save**.

11.2.4. Disable User

Use this task to disable a user temporarily (versus delete the user).

To disable a user

1) Access the **Users** interface.
2) Click the **Action** button.
3) Select **Disable User**.

11.2.5. Enable User

Use this task to re-enable a temporally disabled user.

To enable a user

1) Access the **Users** interface.
2) Click the **Action** button.
3) Select **Enable User**.

11.2.6. Delete User

Use this task to delete a TGCentral user.

To delete a user

1) Access the **Users** interface.
2) Click the **Action** button.
3) Select **Delete User**.

See also

User Permissions

Administration Management

11.3. Manage Roles

Important: Any action performed in the **Admin** section of TGCentral are specific to the TGCentral GUI, not the IBM iSeries server.

Use this task to do the following:

- Display list of roles
- Add role
- Copy role
- Edit role name (only available for custom roles)
- Edit role permissions (only available for custom roles)
- Delete role (only available for custom roles)

Tip: A number of built-in roles are provided at the time of installation, See Permissions for a description of each built-in role.

11.3.1. Display List of Roles

Use this task to view the list of roles in TGCentral.

To display the list of roles

1) Expand the **Admin** menu in the left pane.
2) Click on **Roles**.

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

Field	Description
Name	Name assigned to role
Description	Description of role
Built-in	**Y** (Yes): Pre-built role delivered as part of the product **N** (No): Custom role **Note**: You can only edit customer roles.
Action	Click on the **Action** button to see the list of tasks you can perform for the associated role

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

11.3.2. Add Role

Use this task to add a new TGCentral role.

To add a role

1) Access the **Roles** interface.
2) Click the **Add** button.
3) Complete the following fields:

Field	Description

Name	Name you want to assign the role (30-character max)
Description	Description of role (100-character max)

4) Click **Save**.

11.3.3. Copy Role

Use this task to clone a TGCentral role.

To clone a role

1) Access the **Roles** interface.
2) Click the **Action** button.
3) Select **Copy Role**.
4) Modify the parameters as necessary.
5) Click **Save**.

11.3.4. Edit Role Name

Use this task modify the name assigned to a TGCentral role.

Note: This option is only available for customer/cloned roles (a role created by someone in your company), not built-in roles (a standard role delivered as part of the product).

Tip: The way to tell if a role is customer/cloned or built-in is by looking at the flag in the **Built-in** column.

To edit the role name

1) Access the **Roles** interface.
2) Click the **Action** button.
3) Select **Edit Role Name**.
4) Modify the parameters as necessary.
5) Click **Save**.

11.3.5. Edit Role Permissions

Use this task modify the permissions assigned to a TGCentral role.

Note: This option is only available for custom/copied roles (a role created by someone in your company), not built-in roles (a standard role delivered as part of the product).

Tip: The way to tell if a role is custom or built-in is by looking at the flag in the **Built-in** column.

To edit the role permissions

1) Access the **Roles** interface.
2) Click the **Action** button.
3) Select **View/Edit Permissions**.
4) Enable (allow) permissions as necessary.
5) Click **Save**.

See also

Permissions

11.3.6. Delete Role

Use this task to delete a TGCentral role.

Note: This option is only available for customer/cloned roles (a role created by someone in your company), not built-in roles (a standard role delivered as part of the product).

Tip: The way to tell if a role is customer/cloned or built-in is by looking at the flag in the **Built-in** column.

To delete a role

1) Access the **Roles** interface.
2) Click the **Action** button.
3) Select **Delete Role**.

See also

User Permissions

Administration Management

11.4. Manage Settings

Important: Any action performed in the **Admin** section of TGCentral are specific to the TGCentral GUI, not the IBM iSeries server.
In addition, not all user roles have access to this interface. If you are unable to access the **Admin** feature, contact your system administrator.

Use this task to do the following:

- Create color theme
- Edit color theme
- Copy color theme
- Chose color theme
- Edit color scheme
- Display custom SSL certificate
- Edit database password
- Edit PDF settings
- Edit mail server details
- Cleanup of reports and report cards

11.4.1. Create Color Theme

Use this task to create a new color theme.

To add a user interface color theme

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Theme** tab.
4) Click the **Add** button.

Note: The **New Theme** dialog box is displayed.

5) Complete the following fields:

Field	Description
Name	Enter the name you want to assign the theme
Description	Add a short description describing the purpose of the t heme

6) Select the desired tab.

Note: There is tab for each of the major user interface components (i.e., General, Delta Reports, Dashboard).

7) Click in the field to select the desired color.

8) Click **Save**.

11.4.2. Edit Color Theme

Use this task to edit an existing color theme.

To modify the user interface color theme

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Theme** tab.
4) Click the **Action** button, and select **Edit**.
5) Make the desired modifications.

Tip: Tabs (General, Delta, and Dashboard) are present for the different user interface elements.

6) Click **Save**.

11.4.3. Copy Color Theme

Use this task to copy an existing color theme. This is useful if you want to make a minor tweak to an existing theme.

To duplicate the user interface color theme

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Theme** tab.
4) Click the **Action** button, and select **Copy**.

Note: The **Copy Theme** dialog box is displayed.

5) Make the desired modifications.

Tip: Tabs (General, Delta, and Dashboard) are present for the different user interface elements.

6) Click **Save**.

11.4.4. Chose Color Theme

Use this task to chose a user interface color theme. Each user has the option to choose a preferred theme.

To chose a user interface color theme

1) Expand the **Admin** menu in the left pane.
2) Click on **Users**.

3) Click the **Action** button, and select **Edit User**.

Note: The **Edit User** dialog box appears.

4) Select the desired theme from the list available.
5) Click Save.

Tip: See Create Color Theme for instructions on adding new themes.

11.4.5. Display Custom SSL Certificate

Use this task to view any custom SSL certificates associated with the current installation.

To display a custom SSL Certificate

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **SSL Certificate** tab.
4) Review the following fields.

Field	Description
Certificate File	The path to the client-specific SSL (Secure Sockets Layer) certificate. This is a text file used to generate a Certificate Signing Request (CSR). It is also used to secure and verify the connection.
Private Key	The path to the client-specific private key. This is a text file that generates the digital signature.

11.4.6. Edit Database Password

Use this task to change the password used by the administrator to access the TGCentral database.

To modify the database password

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Database** tab.

Field	Description
Database Password	Enter the new database password
Repeat Database Password	Enter the new database password again for verification purposes

4) Click **Change Database Password**.

11.4.7. Edit PDF Settings

Use this task to change the default PDF settings for reports.

To modify the PDF Settings

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **PDF Settings** tab.
4) Select the desired setting from list available.

5) Click **Save**.

11.4.8. Edit Mail Server Details

Use this task to add/change the email server details. These settings define the email settings for the sender of emails generated from TGCentral.

Note: This information is necessary if you plan to email report notifications or email report card notifications.

To modify the mail server details

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Mail Server** tab.
4) Complete the following fields.

Field	Description
Mail Server Address	Enter the IP address of the mail server you want to use to support email notifications from TGCentral
Port	Enter the mail server port (default 465)
Username	Enter the user ID necessary to log into the mail server
Password	Enter the password necessary to log into the mail server
Size Limit (MB)	Enter the size limit in megabytes of messages (including file attachments) sent through the mail server
Skip verify certificate	Select this option to skip certificate verification

5) Click **Save**.

11.4.9. Cleanup of Reports and Report Cards

Use this task to cleanup (remove) old reports and report cards.

To cleanup reports and report cards

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Cleanup Report** tab.
4) Enter the cleanup date.
5) Click **Delete** to delete reports and report cards older than the clean up date you specified.

See also

User Permissions

Administration Management

11.5. Manage Agent Configuration

This section describes working the agent configuration (i.e., rules, groups, entitlements, defaults, etc.)

Use this task to import or export the following:

Job Activity Monitor

- Activity monitor rules
- Subsystems
- Commands

Groups

- User groups
- Network/server groups
- Object groups

Network Security

- Socket rules
- Remote exit rules
- Exit point configuration
- Network defaults

Access Escalation Management (AEM)

- Entitlements
- Access controls
- File editors
- AEM defaults

Calendar

- Calendar

11.5.1. Import Agent Configuration

To import the agent configuration

1) Expand the **Admin** menu (in the left pane).
2) Select **Import/Export Agent Config**.

Note: The **Import/Export Agent Configuration** interface is displayed in the right pane.

3) Select the desired configuration details (i.e., rules, groups, defaults, etc.) you want to import.
4) Click **Import**.

11.5.2. Export Agent Configuration

Use this task to export the following:

To import the agent configuration

1) Expand the **Admin** menu (in the left pane).
2) Select **Import/Export Agent Config**.

Note: The **Import/Export Agent Configuration** interface is displayed in the right pane.

3) Select the desired configuration details (i.e., rules, groups, defaults, etc.) you want to export.
4) Click **Export**.

See also

User Permissions

Administration Management

12. Troubleshooting

12.1. TGCentral FAQs

12.1.1. Where are the log files stored?

Trinity Guard Log Files

The log files are stored in the following directory: /Trinityguard/Logs/
This directory stores the log file that track the events that occur between the middle tier and the IBM i server.
In this directory, you should find the following 4 log files:

- tgagent.log — Identifies requests made by the agent to TGCentral and includes information about the routing of those requests
- tgrequest.log — Information about the execution (running) of reports and report cards on the agent
- tgtasks.log — Information about the creation of reports and report cards created on the agent
- tgjam_sync.log — Information about the Job Activity Monitor (JAM), including the import/export of job activity rules

TGCentral Log Files

The log files are stored in the following directory: /TGCentral-1.XX/log/

This directory stores the log file that track the events that occur between the GUI and the middle tier.

In this directory, you should find the following log file:

- tgcentral.log

12.1.2. How do I adjust the log levels?

12.1.2.1. Adjust Trinity Guard Log Files located on IBM i Server

Use this task to adjust the log levels. By default, only **CRITICAL** issues are logged. If you would like lower the log lever (include more issues), you must adjust the log level.
Note: The log files have a max size in bytes of 1,024,000 with a backup count of 5. The rotation process is automatic.

To adjust the log levels

1) Sign into IBM i server.
2) At the **Selection or command** prompt, enter **TGMENU** to access the **TG Main** menu.
3) At the **Selection or command** prompt, enter **10** (TGCentral Configuration).
3) Press **Enter**.

Note: The **TGCentral Configuration** interface is displayed.

4) Enter the desired log level in the **Log Status** field.
Note: By default, the log status is set to **CRITICAL**.

12.1.2.2. Adjust TGCentral Log Files Located on Windows Machine

To adjust the TGCentral log file:

1) Navigate directory in which you have TGCentral installed (main directory).
2) Locate the tgcentral.conf file.
3) Modify the parameters as necessary.

12.1.2.3. Adjust TGCentral Log Files Located on Linux Machine

To adjust the TGCentral log file

1) From the command line, enter the following:

```
cd tgcentral-1.x.x
```

2) From the command line, enter the following:

```
sudo nano tgcentral.conf
```

3) Edit the parameters as necessary.
4) Press **Ctrl + x**.
5) Press **y** to save the changes

12.1.2.4. Adjust TGCentral Log Files Located on Windows Machine

To adjust the TGCentral log file

1) From the command line, enter the following:

```
cd tgcentral-1.x.x
```

2) From the command line, enter the following:

```
sudo nano tgcentral.conf
```

3) Edit the parameters as necessary.

12.1.3. How do I change the SSL certificate?

Use this task when you want to change the default TGCentral SSL certificate to a customer SSL certificate.

To change the SSL certificate

1) Sign into TGCentral.
2) Select **Admin** in the **Navigation** (left) pane.
3) Select **Settings**.
4) Select the **SSL Certificate** tab.
5) Document the location (directory path) of the SSL certificate.
6) Navigate to the location of the SSL certificate and replace the existing certificated file with your custom certificate.

12.1.4. What if the TGCentral logon page doesn't appear after installation?

12.1.4.1. Linux Installation

Use this task to ensure that both the “tgcentral” process and the “postgresql” service is running . Both the process and service must be running for the TGCentral login page to appear.

To troubleshoot the missing TGCentral logon page on a Linux machine

1) Ensure that the "tgcentral" process is running by executing the following command:

Command	Expected Result

`ps -A | grep tgcentral`	Your results will not be identical, but should look similar to the following:
	`tguser@tgubuntu1:~/tgcentral-1.1.11$ ps -A | grep tgcentral`
	` 1365 pts/0 00:08:29 tgcentral`

2) If the process is not running, access the directory in which TGCentral is installed (main directory) and use the following command to start the process:

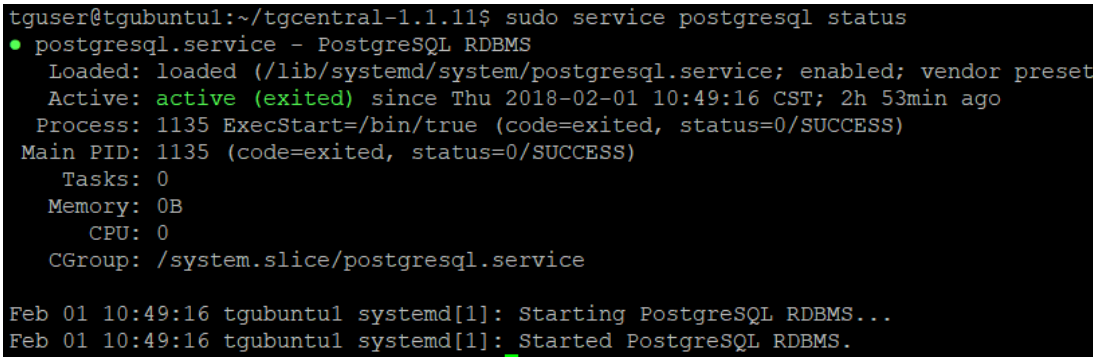
```
sudo sh start.sh
```

3) Ensure the “postgresql” service is running by execute the following command:

Command	Expected Result

```
sudo
service
postgres
ql
status
```

Your results will not be identical, but should look similar to the following:



4) If the service is not running, access the terminal and use the following command:

```
sudo service postgresql start
```

12.1.4.2. Windows Installation

Use this task to ensure that both the "TGCentral" and "PostgreSQL" services are running. Both services must be running for the TGCentral login page to appear.

To troubleshoot the missing TGCentral logon page on a Windows machine

1) On your keyboard press, the **Windows** key + **R**.

Note: The **Run** dialog appears.

2) In the **Open** field, enter **services.msc**.

Note: The **Services** dialog appears.

3) Locate the following services and validate that the services are running:

Name	Status must be
PostgreSQL	Running
TGCentral	Running

3) If they are not running, right click the service and select **Start**.

12.1.5. What do I do if the TGCentral install fails?

Use this task when your install fails.

To troubleshoot the TGCentral installation

1) Ensure all system requirement have been met.

Note: See the TGCentral Installation guide for prerequisites, which is available from the Customer Portal at TrinityGuard.com.

2) Verify that you have administrator privileges before attempting to run the TGCentral installation.
3) Verify that your firewall is not excluding the TGCentral executable file (TGCentral-x.x.exe) from running.
4) Ensure you TGCentral license is valid and has not expired.
5) If you are still having issues after completing step 1-5, contact support via the Customer Portal at TrinityGuard.com.

12.1.6. What if TGCentral won't load on a user's machine?

Use this task if you are unable to connect to the TGCentral server.
Note: Complete these steps on the server on which TGCentral is installed.

1) Access the **Control Panel**.
2) Select **System and Security**.
3) Select **Windows Firewall**.
4) Select **Allow an app or feature through Windows Firewall**.
5) Click **Change settings**.
6) Click **Allow another app**.
7) Click **Browse**.
8) Navigate to the directory in which TGCentral is installed (main directory), and choose **tg.exe** to add it to the list of allowed apps.
9) Once you add **tg.exe** to the list, check (select) all three options: Domain, Private, Public.
10) Click **OK**.

Note: If you are using Linux, complete similar steps according to your firewall configuration. Ensure that your firewall is not excluding the **tgcentral** service on Linux.

12.1.7. What if I forget my admin password?

Unfortunately, the admin password is encrypted and cannot be retrieved if lost. Companies often have security policies that address the preservation and tracking of administrative passwords; therefore, contact your local security officer for assistance.

12.1.8. What if a report won't stop running?

Use this task to stop a report from running and to diagnose what might be causing the delay.

To stop a report from running:

1) Log into TGCentral.
2) In the left pane, select **Activity**.

Note: The **Report Activity** interface is displayed.

3) Click the **Action** button beside the report that shows the status of **Processing**.
4) Select **Delete**.

Option 1: Message Wait (MSGW)

To diagnose if the message wait (MSGW) time is causing the issue:

1) Sign into your IBM i server.
2) At the **Selection or command** prompt, enter WRKACTJOB SBS(TGCMN) to access a list of working jobs.

Note: The **Work with Activity Jobs** interface is displayed.

3) Locate any jobs with the status MSGW (message wait).
4) In the **Opt** column beside the job, enter **7** (Display message).
5) Enter ***NOMAX**
6) Press **Enter**.

Note: This changes the message wait time to *NOMAX.

Option 2: Print file (PRTF)

To diagnose if the print file (PRTF) is causing the issue:

1) Sign into your IBM i server.
2) At the **Selection or command** prompt, enter CHGPRTF FILE(QPRINT) MAXRCDS(*NOMAX).

Note: This changes the printer file size to *NOMAX.

Option 3: Log File (LOGCLPGM)

To diagnose if the log file (LOGCLPGM) is causing the issue:

1) Sign into your IBM i server.
2) At the **Selection or command** prompt, enter JOBD(TGPROD/TGAGENT) LOG(0 99 *NOLIST) LOGCLPGM(*NO) and JOBD(TGPROD/TGREQUEST) LOG(0 99 *NOLIST) LOGCLPGM(*NO).

Note: This change the log level of the job descriptions (TGREQUEST and TGAGENT in library TGPROD) to the minimum.

12.1.9. What if I do if my PostgreSQL is corrupted?

Restore tgcentraldb database. For more information, refer to the PostgreSQL documentation.

12.1.10. Which TGCentral files should I backup on a daily basis?

Follow the recommends provided by your security office. However, for your convenience, we recommend that you include the following in your regular backup procedures:

- Config files
- Database files
- Logs files

13. APPENDIX - Collectors

Collector ID	Collector Name	Collector Category
ACCESS_ESCAL_ACC_CONTROLS	Access Escalation Access Controls	Network
ACCESS_ESCAL_DEFAULTS	Access Escalation Defaults	Network
ACCESS_ESCAL_ENTITLEMENTS	Access Escalation Entitlements	Network
ACCESS_ESCAL_FILE_EDITORS	Access Escalation File Editors	Network
ACCESS_ESCALATION_USAGE	Access Escalation Usage	Network
AUTH_USERS_VIA_AUTH_LISTS	Authorized Users through Authorization Lists	Resource
AUTHORITY_COLLECTION	Authority Collection Data	Journal
AUTHORITY_COMPLIANCE	Authority Compliance	Resource
AUTHORITY_LIST	Authority List Data	System
BLUEPRINT_3RD_PARTY_FILE	Blueprint 3rd Party Integration File	Profile
BLUEPRINT_AUTH_SETTINGS_FILE	Blueprint Authority List Settings File	Profile
BLUEPRINT_MASTER	Blueprint Master	Profile
BLUEPRINT_NON_COMPLIANCE_USER	Blueprint Non-Compliance User Profiles	Profile
BLUEPRINT_OBJECT_AUTH_FILE	Blueprint Object Authority File	Profile
BLUEPRINT_PARAMETER_FILE	Blueprint Parameter File	Profile
CONTROLLER_ATTACHED_DEVICES	Controller Attached Device Information	Network
CONTROLLER_DESCRIPTION_DATA	Controller Description Information	Network
DATA_AREA_AUDITING	Audit data area changes	Network
DATABASE_AUDITING	Monitor Database changes	Network
DATABASE_CONTENT	Database Content	Configuration
DET_ACT_HISTORY	Detect Activity History	Network
DET_CMD_RULES	Command Monitor Rules	Configuration
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration
DET_JRNMON_RULES	Journal Monitor Rules	Configuration
DET_MON_MASTER	Monitor Master	Configuration
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration

DET_MSQ_RULES	Message Queue Rules	Configuration
DET_SEIM_PROVIDERS	SEIM Providers	Configuration
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network
DEVICE_DESCRIPTION_DATA	Device Description Information	Network
EXIT_POINTS	Display Exit Point Data	Network
FIELD_AUTHORITY	Display Field Level Authorities	Object
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource
IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource
IFS_CONTENT	IFS Content	Configuration
IFS_JOURNALING	Display extended journaling information for the IFS object	Resource
IFS_STATUS	Display status information about an IFS file	Resource
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network
ISL_RULES	ISL Inclusion Exclusion Rules	Network
JOB_ACTIVITY_DETAILS	Job Activity Details	Log
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log
JOB_DESCRIPTIONS	Job Description Data	Configuration
JOURNAL_AD	Object Auditing Attribute Changes	Configuration
JOURNAL_AF	Authority Failures	Profile
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration
JOURNAL_AU	EIM Attribute Changes	Configuration
JOURNAL_AX	Row and Column Access Control	Resource
JOURNAL_CA	Authorization List or Object Authority Changes	Profile
JOURNAL_CD	Commands Executed	Resource
JOURNAL_CO	Create Operations	Resource
JOURNAL_CP	User Profile Changes	Configuration
JOURNAL_CQ	Change Request Descriptor Changes	Configuration
JOURNAL_CU	Cluster Operation	Network
JOURNAL_CV	Connection Verification	Profile
JOURNAL_CY	Cryptographic Configuration Changes	Configuration

JOURNAL_DI	LDAP Operations	Resource
JOURNAL_DO	Delete Operations	Resource
JOURNAL_DS	Changes to Service Tools Profiles	Profile
JOURNAL_EV	Environment Variable Changes	Profile
JOURNAL_GR	Exit Point Maintenance Operations	Resource
JOURNAL_GS	Socket Descriptor Details	Resource
JOURNAL_IM	Intrusion Monitor Events	Network
JOURNAL_IP	Inter-process Communication Events	Network
JOURNAL_IR	Actions to IP Rules	Network
JOURNAL_IS	Internet Security Management Events	Network
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource
JOURNAL_JS	Job Changes	Resource
JOURNAL_KF	Key Ring File Changes	Configuration
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource
JOURNAL_M0	Db2 Mirror Setup Tools	Resource
JOURNAL_M6	Db2 Mirror Communication Services	Resource
JOURNAL_M7	Db2 Mirror Replication Services	Resource
JOURNAL_M8	Db2 Mirror Product Services	Resource
JOURNAL_M9	Db2 Mirror Replication State	Resource
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration
JOURNAL_NA	Network Attribute Changes	Profile
JOURNAL_ND	Directory Search Violations	Resource
JOURNAL_NE	APPN Endpoint Filter Violations	Network
JOURNAL_O1	Single Optical Object Accesses	Resource
JOURNAL_O2	Dual Optical Object Accesses	Resource
JOURNAL_O3	Optical Volume Accesses	Resource
JOURNAL_OM	Object Management Changes	Resource
JOURNAL_OR	Objects Restored	Resource
JOURNAL_OW	Object Ownership Changes	Resource
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration
JOURNAL_PF	PTF Operations	Resource
JOURNAL_PG	Primary Group Changes	Resource

JOURNAL_PO	Printer Output Changes	Resource
JOURNAL_PS	Swap Profile Events	Configuration
JOURNAL_PU	PTF Object Changes	Profile
JOURNAL_PW	Invalid Sign-on Attempts	Profile
JOURNAL_RA	Authority Changes to Restored Objects	Configuration
JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration
JOURNAL_RO	Ownership Changes for Restored Objects	Profile
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration
JOURNAL_RQ	Change Request Descriptors Restored	Resource
JOURNAL_RU	Authority Restored for User Profiles	Profile
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration
JOURNAL_SD	System Directory Changes	Resource
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration
JOURNAL_SF	Spooled File Actions	Resource
JOURNAL_SG	Asynchronous Signals Processed	Network
JOURNAL_SK	Secure Socket Connections	Network
JOURNAL_SM	Systems Management Changes	Configuration
JOURNAL_SO	Server Security User Information Actions	Configuration
JOURNAL_ST	Service Tools Actions	Configuration
JOURNAL_SV	System Values Changes	Configuration
JOURNAL_VA	Access Control List Changes	Configuration
JOURNAL_VC	Connections Started, Ended, or Rejected	Network
JOURNAL_VF	Close Operations on Server Files	Resource
JOURNAL_VL	Exceeded Account Limit Events	Profile
JOURNAL_VN	Network Log On and Off Events	Configuration
JOURNAL_VO	Actions on Validation Lists	Resource
JOURNAL_VP	Network Password Errors	Profile
JOURNAL_VR	Network Resource Accesses	Resource
JOURNAL_VS	Server Sessions Started or Ended	Network
JOURNAL_VU	Network Profile Changes	Profile
JOURNAL_VV	Service Status Change Events	Network

JOURNAL_X0	Network Authentication Events	Network
JOURNAL_X1	Identity Token Events	Profile
JOURNAL_XD	Directory Server Extensions	Profile
JOURNAL_YC	DLO Object Changes	Resource
JOURNAL_YR	DLO Object Reads	Resource
JOURNAL_ZC	Object Changes	Resource
JOURNAL_ZR	Object Reads	Resource
KEYSTORE_DATA	KeyStore	Configuration
LINE_DESCRIPTION_DATA	Line Description Information	Configuration
MESSAGE_QUEUE	Message Queue Details	Configuration
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration
NETWORK_ATTRIBUTES	Network Attribute Information	Network
NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes	Network
NETWORK_TCPIP_IPV4	Remote Exit Rules	Network
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes	Network
NETWORK_TCPIP_IPV6	Remote Exit Rules	Network
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network
NETWORK_TRANS_DDM	Remote Exit Rules	Network
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network
NETWORK_TRANSACTIONS_FILE	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_FTP_REXEC	Remote Exit Rules	Network

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

QSYS2.SYSDISKSTAT	Disk Information	Configuration
QSYS2.SYSTEM_STATUS_INFO	Partition information	Configuration
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration
QSYS2.USER_INFO	User Profile Information	Configuration
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration
REMOTE_TRAN_SUMMARY_BY_SERVER	Remote Summary Server	Network
REMOTE_TRAN_SUMMARY_BY_USER	Remote Summary User	Network
RSC_MGR_COMPLIANCE_DATA	Resource Manager Authority Out of compliance data	Network
RSC_MGR_CONFIG	Resource Manager Configuration	Network
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network
SERVICE_TOOL_SECURITY_ATTR	Service Tool Security Attributes	Profile
SERVICE_TOOL_USERS	Service Tool User Data	Profile
SOCKET_SUMMARY_BY_SERVER	Socket Summary by Server	Network
SOCKET_SUMMARY_BY_USER	Socket Summart by User	Network
SOCKET_TRAN_RULES	Socket Rules	Network
SOCKET_TRANSACTIONS	Socket Transactions	Network
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration
SUBSYSTEM_COMMUNICATIONS	Subsystem Communication Entries	Configuration
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration
SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration
SYSCOLAUTH	Privileges granted on a column	Configuration
SYSCONTROLS	Permission or column mask defined	Configuration
SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration

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

14. APPENDIX - Permissions

14.1. Built-in Roles

MENUS

Use the following table to identify access levels for built-in roles.

Permission	Admin	Super User	Help Desk	Auditor	Creator	Reader
MENUS						
Server Management - D(eny)/**A**(llow)						
Servers Menu	A	A	D	D	D	D
Servers Group Menu	A	A	D	D	D	D
Rules - D(eny)/**A**(llow)						
Job Activity Monitor						
Job Activity Monitor Rules	A	A	A	A	D	D
Subsystems	A	A	A	A	D	D
Commands	A	A	A	A	D	D
Network Security						
Socket Rules	A	A	A	A	D	D
Remote Exit Rules	A	A	A	A	D	D

Exit Point Config	A	A	A	A	D	D
Defaults						
Access Escalation Mgmt						
Entitlement	A	A	A	A	D	D
Access Control	A	A	A	A	D	D
File Editors	A	A	A	A	D	D
Defaults	A	A	A	A	D	D
Groups - D(eny)/**A**(llow)						
User Groups	A	A	A	A	D	D
Network Groups	A	A	A	A	D	D
Operation Groups	A	A	A	A	D	D
Object Groups	A	A	A	A	D	D
Reporting - D(eny)/**A**(llow)						
Report Menu	A	A	A	A	A	A
Report Cards Menu	A	A	A	A	A	A
Real Time Events - D(eny)/**A**(llow)						
Network Activity	A	A	A	A	D	D
Alerts	A	A	A	A	D	D

Admin - D(eny)/**A**(llow)						
User Menu	A	A	D	D	D	D
Roles Menu	A	D	D	D	D	D
Settings Menu	A	D	D	D	D	D
Import/Export Agent Conf.	A	A	A	D	D	D

PAGES

Permission	**Admin**	**Super User**	**Help Desk**	**Auditor**	**Creator**	**Reader**
PAGES						
Server Management - D(eny)/**A**(llow)						
Servers						
Add Server	A	A	D	D	D	D
Edit IP Address	A	A	D	D	D	D
Add to Server Group	A	A	D	D	D	D
Run Report	A	A	D	D	D	D
Run Report Card	A	A	D	D	D	D
Delete Server	A	A	D	D	D	D
Manage/Unmanaged Server	A	A	D	D	D	D
View Report of Report Card	A	A	D	D	D	D
View PDF Format	A	A	D	D	D	D
Export CSV	A	A	D	D	D	D
Delete Run Report or Report Card	A	A	D	D	D	D
Run Again	A	A	D	D	D	D
Delta Report	A	A	D	D	D	D

View Servers Details	A	A	D	D	D	D
Add Schedule	A	A	D	D	D	D
Enable/Disable Schedule	A	A	D	D	D	D
Delete Schedule	A	A	D	D	D	D
View Servers Details	A	A	D	D	D	D
Servers Group						
Add Server Group	A	A	D	D	D	D
Edit Server Group	A	A	D	D	D	D
Run Report in Server Group	A	A	D	D	D	D
Run Report in Card in Server Group	A	A	D	D	D	D
Delete Server Group	A	A	D	D	D	D
Rules - D(eny)/**A**(llow)						
Job Activity Monitor						
JAM Rules						
Add New	A	A	D	D	D	D
Edit	A	A	D	D	D	D
Delete	A	A	D	D	D	D
Subsystems						
Add New	A	A	D	D	D	D
Edit	A	A	D	D	D	D
Delete	A	A	D	D	D	D
Commands						
Add New	A	A	D	D	D	D
Edit	A	A	D	D	D	D

Delete	A	A	D	D	D	D
Network Security						
Socket Rules						
Add New	A	A	A	D	D	D
Edit	A	A	A	D	D	D
Delete	A	A	A	D	D	D
Remote Exit Rules						
Add New	A	A	A	D	D	D
Edit	A	A	A	D	D	D
Delete	A	A	A	D	D	D
Exit Point Configuration						
Add Exit Program	A	A	A	D	D	D
Remove Exit Program	A	A	A	D	D	D
Edit	A	A	A	D	D	D
Cycle Server	A	A	A	D	D	D
Network Security Defaults						
Edit	A	A	D	D	D	D
Access Escalation Management						
Entitlement						
Add New	A	A	A	D	D	D
Edit	A	A	A	D	D	D
Delete	A	A	A	D	D	D

Access Control						
Add New	A	A	A	D	D	D
Edit	A	A	A	D	D	D
Delete	A	A	A	D	D	D
File Editors						
Add New	A	A	A	D	D	D
Edit	A	A	A	D	D	D
Delete	A	A	A	D	D	D
Access Esc. Defaults						
Edit	A	A	D	D	D	D
Groups - D(eny)/**A**(llow)						
User Groups						
Add Group	A	A	D	D	D	D
Edit Group	A	A	D	D	D	D
Delete Group	A	A	D	D	D	D
Add User	A	A	A	D	D	D
Edit User	A	A	A	D	D	D
Delete User	A	A	D	D	D	D
Network Groups						
Add Group	A	A	A	D	D	D
Edit Group	A	A	A	D	D	D
Delete Group	A	A	A	D	D	D
Add Detail	A	A	A	D	D	D
Edit Detail	A	A	A	D	D	D
Delete Detail	A	A	A	D	D	D
Operation Groups						

Add Group	A	A	A	D	D	D
Edit Group	A	A	A	D	D	D
Delete Group	A	A	A	D	D	D
Add Detail	A	A	A	D	D	D
Edit Detail	A	A	A	D	D	D
Delete Detail	A	A	A	D	D	D
Object Groups						
Add Group	A	A	A	D	D	D
Edit Group	A	A	A	D	D	D
Delete Group	A	A	A	D	D	D
Add Detail	A	A	A	D	D	D
Edit Detail	A	A	A	D	D	D
Delete Detail	A	A	A	D	D	D
Reporting - D(eny)/**A**(llow)						
Report						
Add Report Definition	A	A	A	A	A	D
Edit Report Definition	A	A	A	A	A	A
Add Report to Schedule	A	A	A	A	A	D
Copy Report Definition	A	A	A	A	A	D
Delete Report Definition	A	A	A	A	A	D
Run Report	A	A	A	A	A	D
Import	A	A	A	A	A	D
Export	A	A	A	A	A	D
Email Report	A	A	A	A	A	A
Report Card						

Add Report Card Definition	A	A	A	A	A	D
View/Edit Report Card Definition	A	A	A	A	A	A
Add Report Card to Schedule	A	A	A	A	A	D
Copy Report Card Definition	A	A	A	A	A	D
Delete Report Card Definition	A	A	A	A	A	D
Run Report Card	A	A	A	A	D	D
Import	A	A	A	A	A	D
Export	A	A	A	A	A	D
Email Report Card	A	A	A	A	A	A
Activity - D(eny)/**A**(llow)						
View Report Activity	A	A	A	A	A	D
View Activity Log	A	A	A	A	A	D
View Messages	A	A	A	A	A	A
View Report	A	A	A	A	A	A
View Report Card	A	A	A	A	A	A
View PDF	A	A	A	A	A	A
Export CSV	A	A	A	A	A	A
Delete Run	A	A	A	A	D	D
Run Again	A	A	A	A	D	D
Delta Reports	A	A	A	A	D	A
Email Report	A	A	A	A	A	A
Real Time Events - D(eny)/**A**(llow)						
Network Activity						

Add Remote Exit Rule	A	A	A	D	D	D
Admin - D(eny)/**A**(llow)						
Users						
Add User	A	A	A	D	D	D
Edit User	A	A	A	D	D	D
Delete User	A	A	D	D	D	D
Enable/Disable User	A	A	A	D	D	D
Roles						
Add Role	A	D	D	D	D	D
Edit Role	A	D	D	D	D	D
Delete Role	A	D	D	D	D	D
Copy Role	A	D	D	D	D	D
Import/Export Agent Conf.						
Import Job Activity Rules	A	A	D	D	D	D
Export Job Activity Rules	A	A	D	D	D	D
Import Job Activity Subsystems	A	A	D	D	D	D
Export Job Activity Subsystems	A	A	D	D	D	D
Import Job Activity Commands	A	A	D	D	D	D
Export Job Activity Commands	A	A	D	D	D	D
Import Network Security Socket Rules	A	A	A	D	D	D
Export Network Security Socket Rules	A	A	A	D	D	D

Import Network Security Remote Exit Rules	A	A	A	D	D	D
Export Network Security Remote Exit Rules	A	A	A	D	D	D
Import Access Escalation Entitlements	A	A	A	D	D	D
Export Access Escalation Entitlements	A	A	A	D	D	D
Import Access Escalation Access Control	A	A	A	D	D	D
Export Access Escalation Access Control	A	A	A	D	D	D
Import User Groups	A	A	D	D	D	D
Export User Groups	A	A	D	D	D	D
Import Network Groups	A	A	A	D	D	D
Export Network Groups	A	A	A	D	D	D
Import Operation Groups	A	A	A	D	D	D
Export Operation Groups	A	A	A	D	D	D
Import Object Groups	A	A	A	D	D	D
Export Object Groups	A	A	A	D	D	D
Import Calendar	A	A	A	D	D	D
Export Calendar	A	A	A	D	D	D

REPORTS AND REPORT CARDS

Permission	Admin	Super User	Help Desk	Auditor	Creator	Reader

Reports - **E**(xclude)/**V**(iew)/**R**(un)						
Category: Configuration	V/R	V/R	V/R	V/R	V/R	V
Category: Log	V/R	V/R	V/R	V/R	E	E
Category: Network	V/R	V/R	V/R	V/R	V/R	V
Category: Profile	V/R	V/R	V/R	V/R	V/R	V
Category: Resource	V/R	V/R	V/R	V/R	V/R	V
Custom Categories	V/R	V/R	V/R	V/R	V/R	V
Report Cards - **E**(xclude)/**V**(iew)/**R**(un)						
Category: Analysis	V/R	V/R	V/R	V/R	V/R	V
Category: IFS Reports	V/R	V/R	V/R	V/R	V/R	V
Category: Regulations	V/R	V/R	V/R	V/R	V/R	V
Custom Categories	V/R	V/R	V/R	V/R	V/R	V

14.2. Custom Roles

Use the following table as a template to build custom roles.

Permission	Admin	Super User	Help Desk	Auditor	Creator	Reader

15. APPENDIX - Delta Reports

Collector_ID	Report_ID	Correlation Fields
Access_Escal_Acc_Controls	Access_Controls_Config	User Name
Access_Escal_Defaults	Defaults_Config	Journal Name
Access_Escal_Entitlements	Entitlements_Config	User Name , Object Name, Object Library, Object Type
Access_Escal_File_Editors	File_Editors_Config	Edit Command , Edit Library
Auth_Users_via_Auth_Lists	Auth_Users_via_Auth_Lists	Object , Library ,Type , Auth List User
Blueprint_Auth_Settings_File	Blueprint_Auth_Settings	BluePrint ID, Authority List
Blueprint_Master	Blueprint_Master	BluePrint ID, User Group
Blueprint_Non_Compliance_User	Blueprint_Non_Cmpl	BluePrint ID, User Name, Violation Category, Violation Keyword
Blueprint_Object_Auth_File	Blueprint_Object_Auth_File	BluePrint ID, Profile Object owner
Blueprint_Parameter_File	Blueprint_Parameter_File	BluePrint ID, User Parameter
Blueprint_Permissions_File	Blueprint_Permissions_File	BluePrint ID, Authorized User/Group
Blueprint_3rd_Party_File	Blueprint_3rd_Party_File	BluePrint ID, Script Type, Script Statement
Controller_Attached_Devices	Controller_Attached_Devices	Device Name, Device Category , Device Type
Controller_Description_Data	Controller_Description_Data	Controller Name, Controller Category
Det_Cmd_Rules	Det_Cmd_Rules	Rule ID, Command Name, Command Library, Command User
Det_Defaults	Det_Defaults	Journal Name
Det_Jrn_SIEM_Rules	Det_Jrn_SIEM_Rules	Journa Name, Journal Library , Journal Code and Journal Type , Alert Sequence
Det_JrnMon_Alerts	Det_JrnMon_Alerts	Journa Name, Journal Library , Journal Code and Journal Type , Filter Sequence
Det_JrnMon_Rules	Det_JrnMon_Rules	Journa Name, Journal Library , Journal Code and Journal Type
Det_Mon_Master	Det_Mon_Master	Monitor Name, Monitor Library, Monitor Type
Det_Msq_Cmd_Alr	Det_Msq_Cmd_Alr	Monitor Name, Monitor Library, Monitor Type, Rule Name, Alert Sequence

Collector_ID	Report_ID	Correlation Fields
Det_Msq_Rules	Det_Msq_Rules	Rule ID , Message Queue, Message Queue Library, Message ID
Det_SIEM_Providers	Det_SIEM_Providers	syslog provider Name
Device_Description_APPC	Device_Description_APPC	Device Name, Device Category
Device_Description_Data	Device_Description_Data	Device Name, Device Category
ISL_Configuration_Settings	ISL_Configuration	
ISL_Disconnect_Options	ISL_Disconnect	Disconnect Option
ISL_Rules	ISL_Monitor_Rules	Rule Type, Object Name,Object Library
Network_Exit_Config	Exit_Point_Config_Report	Server Name, Exit Point, Exit Format
Network_Svr_Encrypt_Status	Network_Svr_Encrypt_Not_Verif	TCPIP App ID
Network_Svr_Encrypt_Status	Network_Svr_Encrypt_Status	TCPIP App ID
Network_Svr_Encrypt_Status	Network_Svr_Encrypt_Verified	TCPIP App ID
Profile_Compliance	Profile_Compliance_Report	BluePrint ID, User Name, Violation Category, Violation Keyword
Profile_Inactivity_Settings	Profile_Inactivity_Settings	Only one record
Profile_Manager_Defaults	Profile_Manager_Defaults	Only one record
QSYS2.ACTIVE_JOB_INFO	QSYS2_ACTIVE_JOB_INFO	Job Name
QSYS2.DRDA_AUTHENTICATION	QSYS2_DRDA_AUTHENTICATION	User Name , Server Name
QSYS2.FUNCTION_INFO	QSYS2_FUNCTION_INFO	Function ID
QSYS2.FUNCTION_USAGE	QSYS2_FUNCTION_USAGE	Function ID , User Name
QSYS2.GROUP_PTF_INFO	QSYS2_GROUP_PTF_INFO	PTF_G00001
QSYS2.JOURNAL_INFO	QSYS2_JOURNAL_INFO	Journal Name , Journal Library
QSYS2.LICENSE_INFO	QSYS2_LICENSE_INFO	LICPGM,FEATURE
QSYS2.MEDIA_LIBRARY_INFO	QSYS2_MEDIA_LIBRARY_INFO	DEVICE,DEVICE TYPE
QSYS2.MEMORY_POOL	QSYS2_MEMORY_POOL	POOL_NAME
QSYS2.REPLY_LIST_INFO	QSYS2_REPLY_LIST_INFO	MSGID
QSYS2.SCHEDULED_JOB_INFO	QSYS2_SCHEDULED_JOB_INFO	SCDJOBNAME
QSYS2.SERVER_SBS_ROUTING	QSYS2_SERVER_SBS_ROUTING	User Name,DRDADDMSBS
QSYS2.SYSCONTROLS	QSYS2_SYSCONTROLS	SCHEMA
QSYS2.SYSCONTROLSDEP	QSYS2_SYSCONTROLSDEP	SCHEMA
QSYS2.SYSDISKSTAT	QSYS2_SYSDISKSTAT	UNITNBR

Collector_ID	Report_ID	Correlation Fields
QSYS2.SYSTEM_STATUS_INFO	QSYS2_SYSTEM_STATUS_INFO	Only one record
QSYS2.SYSTMPSTG	QSYS2_SYSTMPSTG	BKTNBR,GLBBKTNAME
QSYS2.USER_INFO	QSYS2_USER_INFO	USER NAME
QSYS2.USER_STORAGE	QSYS2_USER_STORAGE	USER NAME
Rsc_Mgr_Compliance_Data	Rsc_Mgr_Compliance_Data	SCMID FILESYS PATH ASPNAME LIBNAME OBJNAME OBJTYPE
Rsc_Mgr_Config	Rsc_Mgr_Config	Only one record
Rsc_Mgr_Schema_Details	Rsc_Mgr_Schema_Details	Schema ID ,File Systems, IFS Path, Auxilary Storage Pool,Object.Library,Type
Rsc_Mgr_Schema_Header	Rsc_Mgr_Schema_Header	Schema ID
Socket_Tran_Rules	Socket_Rules_Report	User, Port, Operation, IP Address
SYSTABLESTAT	SYSTABLESTAT_Delete_Operations	Library Name, Long File Name
SYSTABLESTAT	SYSTABLESTAT_Deleted_Records	Library Name, Long File Name
SYSTABLESTAT	SYSTABLESTAT_Insert_Operations	Library Name, Long File Name
SYSTABLESTAT	SYSTABLESTAT_Large_Files	Library Name, Long File Name
SYSTABLESTAT	SYSTABLESTAT_Read_Operations	Library Name, Long File Name
TG_Network_Groups	TG_Network_Groups_Report	Network Group Name, Network Name
TG_Object_Groups	TG_Object_Groups_Report	Object Group Name,OBJSYS,OBJNM,OBJLB,OBJTYP,OBJIFS
TG_Operation_Groups	TG_Operation_Groups_Report	Operation Group Name, Server , Function, Command
TG_User_Groups	TG_User_Groups_Report	User Group Name, User Name
User_Profile_Archive	User_Profile_Archive	User Name
User_Profile_Exclusions	User_Profile_Exclusions	User Name