

# NetIQ Security Solutions for IBM i
# TGCentral 2.4
## User Guide
**Revised September 2021**

## Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

**Copyright© 2021 Trinity Guard LLC. All rights reserved.**

1. What's New . . . 6
2. TGCentral Introduction . . . 7
2.1 Features . . . 8
2.2 Roles . . . 9
3. Getting Started . . . 10
3.1 Log Into TGCentral . . . 13
3.2 Working with TGCentral . . . 14
4. Dashboard . . . 15
5. Servers . . . 21
5.1 Server Management . . . 22
5.2 Working with Server Management . . . 23
5.3 Display Server Details . . . 24
5.4 Display Server Group Details . . . 27
5.5 Manage Servers . . . 30
5.6 Manage Server Groups . . . 36
6. Rules . . . 40
6.1 Rules Management . . . 41
6.2 Access Escalation Management . . . 42
6.2.1 Working with Access Escalation Management . . . 43
6.2.2 AEM Defaults . . . 44
6.2.2.1 Display AEM Defaults . . . 45
6.2.2.2 Manage AEM Defaults . . . 47
6.2.3 Access Control . . . 49
6.2.3.1 Display Access Control Details . . . 50
6.2.3.2 Manage Access Control . . . 51
6.2.4 Entitlements . . . 53
6.2.4.1 Display Entitlement Details . . . 54
6.2.4.2 Manage Entitlements . . . 56
6.2.5 File Editor . . . 58
6.2.5.1 Display File Editor Details . . . 59
6.2.5.2 Manage File Editors . . . 60
6.3 Inactive Session Lockdown . . . 62
6.3.1 Working with Inactive Session Lockdown . . . 63
6.3.2 ISL Defaults . . . 64
6.3.2.1 Display ISL Defaults . . . 65
6.3.2.2 Manage ISL Defaults . . . 67
6.3.3 ISL Rules . . . 69
6.3.3.1 Display ISL Rules . . . 70
6.3.3.2 Manage ISL Rules . . . 72
6.3.4 Disconnect Options . . . 75
6.3.4.1 Display Disconnect Options . . . 76
6.3.4.2 Manage Disconnect Options . . . 78
6.4 Job Activity Monitor . . . 80
6.4.1 Working with Job Activity Monitor . . . 81
6.4.2 Job Activity Details . . . 82
6.4.2.1 Display Job Activity Rule Details . . . 83
6.4.2.2 Manage Job Activity Monitor Rules . . . 85
6.4.3 Commands . . . 87
6.4.3.1 Display Command Details . . . 88
6.4.3.2 Manage Commands . . . 90
6.4.4 Subsystems . . . 92
6.4.4.1 Display Subsystem Details . . . 93
6.4.4.2 Manage Subsystems . . . 94
6.5 Network Security . . . 97
6.5.1 Working with Network Security . . . 98
6.5.2 Network Defaults . . . 99
6.5.2.1 Display Network Defaults . . . 100
6.5.2.2 Manage Network Defaults . . . 102
6.5.3 Socket Rules . . . 104
6.5.3.1 Display Socket Rules . . . 105

6.5.3.2 Manage Socket Rules . . . 107
6.5.4 Remote Exit Rules . . . 109
6.5.4.1 Display Remote Exit Rule Details . . . 110
6.5.4.2 Manage Remote Exit Rules . . . 112
6.5.5 Exit Points . . . 114
6.5.5.1 Display Exit Point Configuration Details . . . 115
6.5.5.2 Manage Exit Point . . . 118
6.6 Resource Manager . . . 121
6.6.1 Working with Resource Manager . . . 122
6.6.2 Resource Manager Defaults . . . 123
6.6.2.1 Display Resource Manager Defaults . . . 124
6.6.2.2 Manage Resource Manager Defaults . . . 127
6.6.3 Authority Schemas . . . 129
6.6.3.1 Display Authority Schemas . . . 130
6.6.3.2 Manage Authority Schemas . . . 132
6.6.4 Authority Schema Rules . . . 136
6.6.4.1 Display Authority Schema Rules . . . 137
6.6.4.2 Manage Authority Schema Rules . . . 139
6.7 User Profile Manager . . . 141
6.7.1 Working with User Profile Manager . . . 142
6.7.2 User Profile Manger Defaults . . . 143
6.7.2.1 Display UPM Defaults . . . 144
6.7.2.2 Manage UPM Defaults . . . 147
6.7.3 Archived Profiles . . . 151
6.7.3.1 Display Archived Profile Details . . . 152
6.7.3.2 Manage Archived Profile . . . 154
6.7.4 Blueprints . . . 156
6.7.4.1 Display Blueprint Details . . . 157
6.7.4.2 Manage Blueprints . . . 160
6.7.5 Password Rules . . . 168
6.7.5.1 Display Password Rule Details . . . 169
6.7.5.2 Manage Password Rule Settings . . . 171
6.7.6 Profile Inactivity . . . 173
6.7.6.1 Display Profile Inactivity Settings . . . 174
6.7.6.2 Manage Profile Inactivity Settings . . . 176
6.7.7 User Exclusions . . . 180
6.7.7.1 Display User Exclusion Details . . . 181
6.7.7.2 Manage User Exclusions . . . 183
6.7.8 User Profiles . . . 185
6.7.8.1 Manage User Profiles . . . 186
6.8 Detect Monitor . . . 188
6.8.1 Working with Detect Monitors . . . 189
6.8.1.1 Display Detect Monitors . . . 190
6.8.1.2 Manage Detect Monitors . . . 192
6.8.2 Command Monitor . . . 194
6.8.2.1 Display Command Monitor Rules . . . 195
6.8.2.2 Manage Command Monitor Rules . . . 199
6.8.3 History Log Monitor . . . 204
6.8.3.1 Display History Log Rules . . . 205
6.8.3.2 Manage History Log Rules . . . 209
6.8.4 Journal Monitor . . . 214
6.8.4.1 Display Journal Monitor Rules . . . 215
6.8.4.2 Manage Journal Monitor Rules . . . 219
6.8.5 Message Queue Monitor . . . 223
6.8.5.1 Display Message Queue Rules . . . 224
6.8.5.2 Manage Message Queue Rules . . . 228
6.8.6 SIEM Monitor . . . 233
6.8.6.1 Display SIEM Monitor Rules . . . 234
6.8.6.2 Manage SIEM Monitor Rules . . . 237
6.8.7 Syslog Monitor . . . 239

6.8.7.1 Display Syslog Monitor Rules . . . 240
6.8.7.2 Manage Syslog Monitor Rules . . . 242
7. Groups . . . 244
7.1 Group Management . . . 245
7.2 Working with Groups . . . 246
7.3 Manage User Groups . . . 247
7.4 Manage Network Server Groups . . . 250
7.5 Manage Operation Groups . . . 252
7.6 Manage Object Groups . . . 254
8. Calendars . . . 256
8.1 Calendar Management . . . 257
8.2 Working with Calendars . . . 258
8.3 Manage Calendars . . . 259
9. Reports . . . 261
9.1 Report Management . . . 262
9.2 Working with Reports and Report Cards . . . 263
9.3 Display TGCentral Reports . . . 264
9.4 Display List of TGCentral Report Cards . . . 266
9.5 Manage Reports . . . 268
9.6 Manage Report Cards . . . 273
9.7 Run Report . . . 278
9.8 Run Report Card . . . 279
10. Activity . . . 280
10.1 Activity Management . . . 281
10.2 Working with Activities . . . 282
10.3 Manage Report Activities . . . 283
10.4 Manage Server Activities . . . 288
11. Real Time Events . . . 290
11.1 Real Time Event Management . . . 291
11.2 Working with Real Time Event Management . . . 292
11.3 Manage Network Activity . . . 293
11.4 Manage Alerts . . . 296
12. Admin . . . 299
12.1 Administration Management . . . 300
12.2 Working with Administration Management . . . 301
12.3 Manage Users . . . 302
12.4 Manage Roles . . . 305
12.5 Manage Settings . . . 308
12.6 Manage Agent Configuration . . . 315
13. Appendices . . . 316
13.1 APPENDIX - TGCentral Revisions . . . 317
13.1.1 Version 2.4 - TGCentral User Guide Revisions . . . 318
13.1.2 Version 2.3 - TGCentral User Guide Revisions . . . 319
13.1.3 Version 2.2 - TGCentral User Guide Revisions . . . 320
13.1.4 Version 2.1 - TGCentral User Guide Revisions . . . 321
13.2 APPENDIX - TGCentral Collectors . . . 322
13.3 APPENDIX - TGCentral Delta Reports . . . 332
13.4 APPENDIX - TGCentral Permissions . . . 336
13.5 APPENDIX - TGCentral FAQs . . . 344

# What's New

| Version 2.4 - TGCentral User Guide Revisions |
| --- |
| TGCentral 2.4 contains the following:<br>**New Features**<br>• TGEncrypt Support<br>**Enhancements**<br>• TGAudit for Linux - Content Updates<br>• TGAudit for Linux - Licensing<br>• Database - Performance improvement<br>• User Profile Management - Archive Options *SAVSEC,*SAVPRF |

**See also**

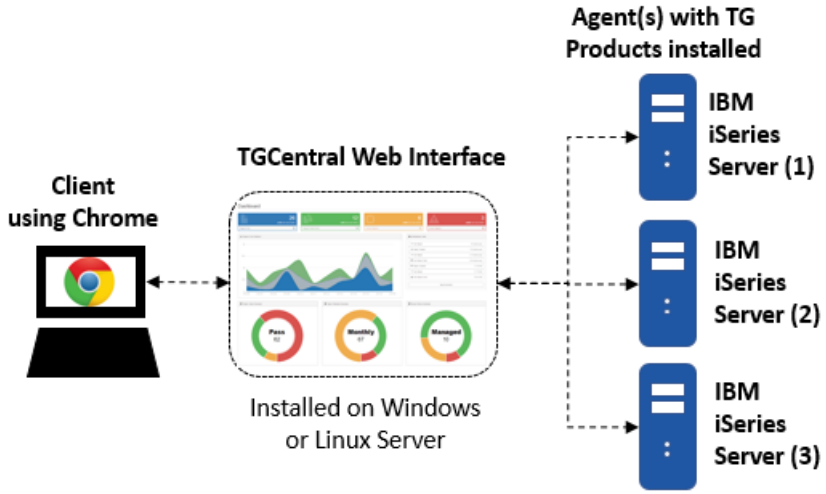
APPENDIX - TGCentral Revisions

# TGCentral Introduction

**TGCentral** (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**

What's New

Getting Started

# 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-based access control layer allowing you to provide granular permissions
- Administration Management - 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

**See also**

TGCentral Introduction

# Roles

Each user must be assigned one of the following roles:

| Role | Description |
|---|---|
| **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.<br>**Note**: A larger organization might have many admins while a smaller organization might have a few, depending on resource availability.<br><br>**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.<br><br>**Note**: See 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.<br>A superuser manages rules. |
| **HELP DESK** | Users in this role manage agent groups/users, create/run/view reports, and create/run/view report cards.<br>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.<br>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**

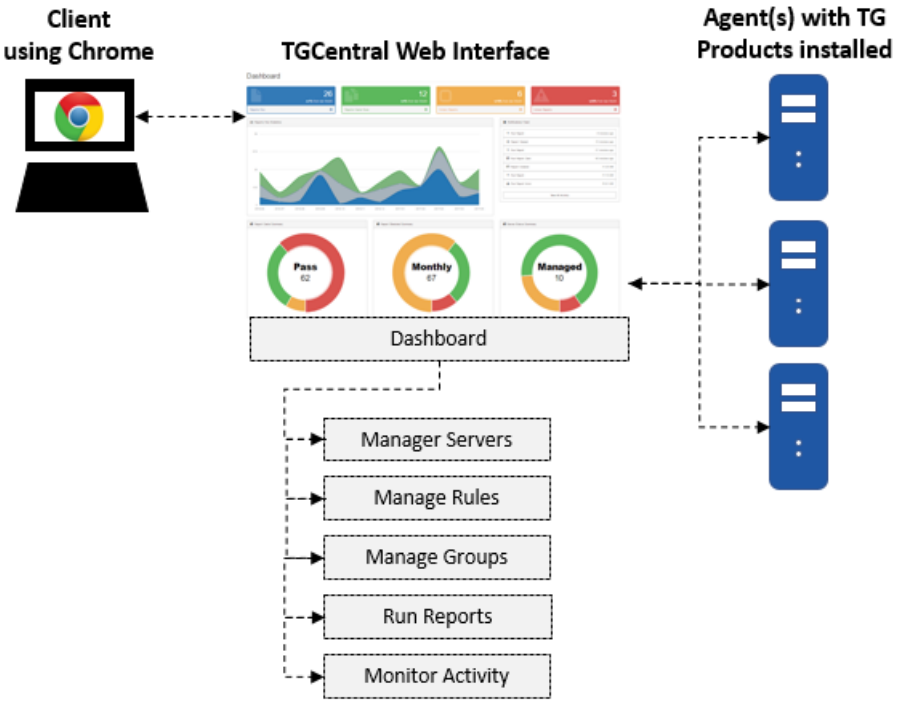
TGCentral Introduction

Permissions

# 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.

## Admin Tasks

| Step | Description |
|---|---|

| | |
|---|---|
| 1 | **Set Agent Status to *ACTIVE**<br><br>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.<br><br>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.<br><br>**Tip**: If you have a TGCentral license, you can download the *TGCentral Installation Guide* from customer portal at TrinityGuard.com. |
| 2 | **Create Roles**<br>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 the access level.<br><br>**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.<br><br>See Manage Roles for additional instructions on creating and modifying roles. |
| 3 | **Add Users**<br>Once your project team establishes clear roles, then the administrator can begin adding users and assigning those users to a role.<br><br>**Tip:** A user cannot access the system until an administrator adds the user and assign that user login credentials (i.e., username and password)<br><br>See Manage Users for additional instructions. |

## User Tasks

| Step | Description |
|---|---|
| 1 | **Login**<br>Contact your TGCentral admin and obtain the TGCentral URL specific to your organization and your unique login credentials (i.e., user name and password).<br><br>See Login into TGCentral for additional instructions. |
| 2 | **Add and remove servers**<br>Determine which server(s) you want to manage. You can use TGCentral to manage as many or as few servers as necessary.<br><br>See Manage Server for additional instructions. |
| 3 | **Add and edit rules**<br>Create and edit rules. Rules control access.<br><br>**Tip**: You can distribute rules across multiple servers to promote consistency.<br><br>See Manage Rules for additional instructions. |

| | |
|---|---|
| **4** | **Add and edit groups**<br>Create and edit groups. Groups allow you to work more efficiently.<br><br>**Tip**: You can distribute groups across multiple servers to promote consistency.<br><br>See the following topics for additional instructions:<br>• Manage User Groups<br>• Manage Object Groups<br>• Manage Operation Groups |
| **5** | **Run reports and report cards**<br>Run reports and report cards. Reports and report cards allow you to monitor the security health of your system.<br><br>See the following topics for additional instructions:<br>• Manage Reports<br>• Manage Report Cards |
| **6** | **Monitor activity**<br>Monitor activities performed on each server. Activities are the tasks performed by TGCentral users (i.e., login attempts, report runs, rule modifications, etc.).<br><br>See Manage Activities for additional instructions. |
| **7** | **Modify user preferences**<br>Each TGCentral user can modify their system settings to improve their user experience.<br><br>See Manage Settings for additional instructions. |

# 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**. The **Sign In** dialog is displayed.
4) Enter your TGCentral username and password.
5) Click **Login**.

### See also

Getting Started

# Working with TGCentral

# Dashboard

This section describes how to work with the **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 by Timeline
- Display Report and Report Card Summary
- Display Scheduled Report Summary
- Display Server Status Summary

## 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.

## 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. 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.

## 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. 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.

## 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. 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.

## 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. 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.

## 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.

## 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.

## Display Activity by Server

Use this task to display activities by the 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 the 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).

## 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).

## 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).

## Display Activity by Operation Server

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

**To display the activity by the 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).

## 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).

## 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.

## 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 the 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.

## 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

Manage Roles

Permissions

# Servers

This section describes how to work with **Servers**.

The section includes the following topics:

- Server Management
- Working with Server Management
- Display Server Details
- Display Server Group Details
- Manage Servers
- Manage Server Groups

**See also**

TGCentral Introduction

# Server Management

This section describes working with servers. Use the **Server Management** feature.

This section includes the following topics:

- Working with Server Management
- Display Server Details
- Display Server Group Details
- 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 levels, which is based on their assigned role.

**See also**

Servers

# Working with Server Management

Use the **Server Management** feature to do the following:

- Display Server Details
- Display Server Group Details
- Manage Servers
- Manage Server Groups

**See also**

Server Management

# Display Server Details


- Display List of Active Servers
- Refresh List of Servers
- Display Server Details
- Display Server Activity History
- Disable Scheduled Report on Server


## 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**. 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:<br>– IBM i indicates an IBM i series server<br>– Linux indicates a Linux server |

| | |
|---|---|
| Status | **Managed**: TGCentral and the agent are communicating (sharing information) and are in sync<br>**Unmanaged**: TGCentral and the agent are not communicating (not sharing information) and are not in sync<br>**Unknown**: TGCentral and the agent are communicated, but the administrator has not yet determined if the server should be managed or unmanaged<br>**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.<br><br>**Tip**: A color indicated should appear beside each server.<br>– 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).<br>– 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).<br>– A **green** indicator icon (dot) appears when TGCentral detects the server, detects a valid license, and the server is online (communicating with TGCentral).<br>– 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.

## Refresh List of 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.Refresh List of Active Servers

#### 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)

## 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.

## 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.

## 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. 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**.

**See also**

Working with Server Management

# Display Server Group Details


- Display List of Server groups
- Refresh List of Server Groups
- Display List of Servers in a Server Group
- Display Server Group Activity History


## 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**. 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.

## 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)

## 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. 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:<br>– IBM i indicates an IBM i series server<br>– Linux indicates a Linux server |
| Status | **Managed**: TGCentral and the agent are communicating (sharing information) and are in sync<br>**Unmanaged**: TGCentral and the agent are not communicating (not sharing information) and are not in sync<br>**Unknown**: TGCentral and the agent are communicated, but the administrator has not yet determined if the server should be managed or unmanaged<br>**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.<br><br>**Tip**: A color indicated should appear beside each server.<br>– 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).<br>– 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).<br>– A **green** indicator icon (dot) appears when TGCentral detects the server, detects a valid license, and the server is online (communicating with TGCentral).<br>– 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 |

## 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. 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:<br>**Completed** - Successful run<br>**Processing** - In process (with percent complete)<br>**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 |

# Manage Servers

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

- Add Server
- Delete Server
- Manage Server
- Unmanage Server
- Add Server to Group
- Run Report on Server
- Add Scheduled Report to Server
- Delete Scheduled Report from Server
- Run Report Card on Server
- Add Scheduled Report Card to Server
- Delete Scheduled Report Card from a Server
- Disable Scheduled Report Card on Server

## 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**.

## 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**.

## 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**.

## Unmanage 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.

> **Note**: 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**.

## 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**. The **List of Server Groups** dialog is displayed.
4) Select the group to which you want to add the server.
5) Click **Save**.

## 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. The **Run Report** dialog appears.
5) Select the report you want to run from the list.
6) Click **Run Now**.

## 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. 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<br>**One Day** - Once<br>**Daily** - Once a day<br>**Weekly** - Once a week<br>**Monthly** - Once a month<br>**Yearly** - Once a year |
| Time | Time at which the scheduled report should run |

7) Click **Save**.

## Delete Scheduled Report from 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. 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**.

## 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. The **Run Report Card** dialog appears.
5) Select the report card you want to run from the list.
6) Click **Run Now**.

## 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. 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<br>**One Day** - Once<br>**Daily** - Once a day<br>**Weekly** - Once a week<br>**Monthly** - Once a month<br>**Yearly** - Once a year |
| Time | Time at which the scheduled report card should run |

7) Click **Save**.

## 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. 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**.

## 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. 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**

Working with Server Management

# Manage Server Groups


- Add Server Group
- Edit Server Group
- Delete Server Group
- Add Server to Group
- Delete Server from Group
- Add Schedule Report to Server Group
- Delete Scheduled Report from Server Group
- Disable Scheduled Server Group Report


## 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**.

## 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**.

## 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**.

## 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 Server Group** option.

## 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. 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**.

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

4) Click the **+ New Schedule** button. 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<br>**One Day** - Once<br>**Daily** - Once a day<br>**Weekly** - Once a week<br>**Monthly** - Once a month<br>**Yearly** - Once a year |
| Time | Time at which the scheduled report should run |

7) Click **Save**.

## 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. 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**.

## 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. 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

Working with Server Management

# Rules

This section describes how to work with **Rules**.

This section includes the following topics:

- Rules Management
- Access Escalation Management
- Inactive Session Lockdown
- Job Activity Monitor
- Network Security
- Resource Manager
- User Profile Manager
- Detect Monitor

**See also**

TGCentral Introduction

# Rules Management

The **Rules Management** feature allows you to manage user access rules.

This section includes the following topics:

- Access Escalation Management
- Inactive Session Lockdown
- Job Activity Monitor
- Network Security
- Resource Manager
- User Profile Manager
- Detect Monitor

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

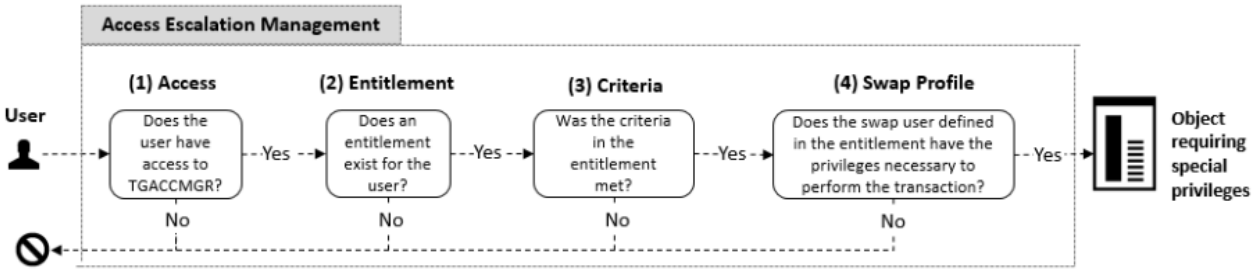
**See also**

Rules

# Access Escalation Management

The **Access Escalation Management** feature to allow the user to swap profiles for access escalation.

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




This section includes the following topics:

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

**See also**

Rules

Rules Management

# Working with Access Escalation Management

The **Access Escalation Management** feature to allow the user to swap profiles for access escalation.

This section includes the following topics:

- AEM Defaults
- Access Control
- Entitlements
- File Editor

**See also**

Access Escalation Management

# AEM Defaults

This section includes the following topics:

- Display AEM Defaults
- Manage AEM Defaults

**See also**

Access Escalation Management

# Display AEM Defaults

This section describes how to display **Access Escalation Management** (AEM) defaults.

Use this task to do the following:

- Display AEM Defaults
- Refresh List of AEM Defaults

## 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**. 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<br>**Y** - Enable tracking of changes<br>**N** - Disable tracking of changes<br>**Tip**: This flag must be set to **Y** to if you plan to run access escalation change reports.<br>**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.

## 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.

**See also**

Working with Access Escalation Management

# Manage AEM Defaults

This section describes how to work 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:

- Access the Access Escalation Defaults Interface
- Add AEM Default
- Edit AEM Defaults
- Delete AEM Default

> **Note**: To work with the AEM defaults, you must access the **Access Escalation Defaults** interface.

## Access the Access Escalation Defaults Interface

Use this task to access the **Access Escalation Defaults** interface.

**To access the Access Escalation Defaults interface**

1) Access the **Rules** interface.
2) Select **Access Escalation Mgmt** to expand the tree.
3) Select **Defaults**. The **Access Escalation Defaults** interface is displayed.

## 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**.

## 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**.

## 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 with Access Escalation Management

# Access Control

This section includes the following topics:

- Display Access Control Details
- Manage Access Control

**See also**

Access Escalation Management

# Display Access Control Details

This section describes how to display access controls.

Use this task to do the following:

- Display List of Access Controls
- Refresh List of Access Controls

## Display List of 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**. 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.

## 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.

### See also

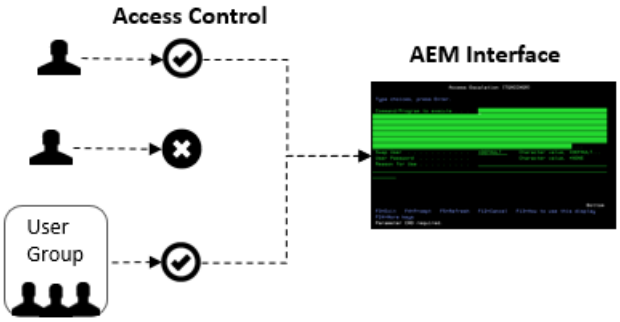
Working with Access Escalation Management

# 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:

- Access the Access Control Interface
- Add Access Control
- Edit Access Control
- Delete Access Control

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

## Access the Access Control Interface

Use this task to access the **Access Control** interface.

#### To access the Access Control interface

1) Access the **Rules** interface.
2) Select **Access Escalation Mgmt** to expand the tree.
3) Select **Access Control**. The **Access Control** interface is displayed.

## Add Access Control

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**.

## Edit Access Control

Use this task to edit access controls.

**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**.

## Delete Access Control

Use this task to delete access controls.

**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 with Access Escalation Management

# Entitlements

This section includes the following topics:

- Display Entitlement Details
- Manage Entitlements

**See also**

Access Escalation Management

# Display Entitlement Details

This section describes how to display entitlements.

Use this task to do the following:

- Display List of Entitlements
- Refresh List of Entitlements

## 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**. 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:<br>**Y** - Enabled<br>**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<br>*__PMG__ - Program<br>*__CMD__ - Command<br>*__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<br>**Y** - Password required<br>**N** - No password required |
| Alr Req? | Whether an alert is sent to the alert queue when an attempt is made to use the entitlement<br>**Y** - Alert enabled<br>**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.

## 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.

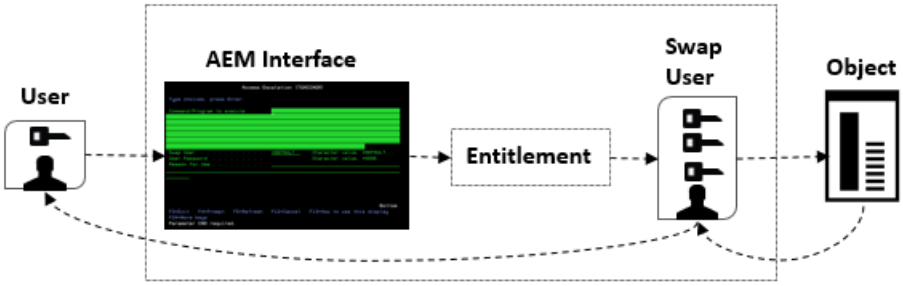
### See also

Working with Access Escalation Management

# Manage Entitlements

This section describes how to work 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:

- Access the Entitlements Interface
- Add Entitlements
- Edit Entitlements
- Delete Entitlements

**Note**: To work with the entitlements, you must access the **Entitlements** interface.

## Access the Entitlements Interface

Use this task to access the **Entitlements** interface.

#### To access the Entitlements interface

1) Access the **Rules** interface.

2) Select **Access Escalation Mgmt** to expand the tree.

3) Select **Entitlements**. The **Entitlements** interface is displayed.

## 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**.

## 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**.

## 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

# File Editor

This section includes the following topics:

- Display File Editor Details
- Manage File Editors

**See also**

Access Escalation Management

# Display File Editor Details

This section describes how to display file editors.

Use this task to do the following:

- Display File Editors
- Refresh List of File Editors

## 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**. 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 |

## 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.

### See also

Working with Access Escalation Management

# Manage File Editors

This section describes how to work 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:

- Access the File Editor Interface
- Add File Editor
- Edit File Editor
- Delete File Editor

**Note**: To work with the third-party commands, you must access the **File Editor** interface.

## Access the File Editor Interface

Use this task to access the **File Editor** interface.

#### To access the File Editor interface

1) Access the **Rules** interface.
2) Select **Access Escalation Mgmt** to expand the tree.
3) Select **File Editors**. The **File Editor** interface is displayed.

## 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**.

## 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**.

## 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 with Access Escalation Management

# Inactive Session Lockdown

The **Inactive Session Lockdown** (ISL) feature allows you to manage inactive user sessions.

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

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

This section includes the following topics:

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

**See also**

Rules

Rules Management

# Working with Inactive Session Lockdown

The **Inactive Session Lockdown** (ISL) feature allows you to manage inactive user sessions.

This section includes the following topics:

- ISL Defaults
- ISL Rules
- Disconnect Options

**See also**

Inactive Session Lockdown

# ISL Defaults

This section includes the following:

- Display ISL Defaults
- Manage ISL Defaults

**See also**

Inactive Session Lockdown

# Display ISL Defaults

This section describes how to display **Inactive Session Lockdown** (ISL) defaults.

Use this task to do the following:

- Display List of ISL Defaults
- Refresh List of ISL Defaults

## Display List of 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**. 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<br>***YES** - Enable auditing<br>***NO** - Disable auditing<br>**Tip**: Set this flag to ***YES** if you plan to run ISL usage report |
| Journal | Journal in which to store ISL usage data<br>**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):<br>***YES** - Enable alerts (create admin alert)<br>***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<br>***YES** - Warning alert enabled<br>***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<br>*__YES__ - The user's session is locked or ended, and the user's authority is revoked<br>*__NO__ - The user's session is locked or ended, but the user's authority is maintained<br>**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.

## 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.

### See also

Working with Inactive Session Lockdown

# Manage ISL Defaults

This section describes how to work 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

Use this task to do the following:


- Access the Inactive Session Lockdown Defaults Interface
- Edit ISL Default
- Add ISL Default
- Delete ISL Default


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

## Access the Inactive Session Lockdown Defaults Interface

Use this task to access the **Inactive Session Lockdown Defaults** interface.

**To access the Inactive Session Lockdown interface Defaults**

1) Expand the **Rules** menu.
2) Expand the **Inactive Sess. Lockdown** menu.
3) Select **Defaults**. The **Inactive Session Lockdown Defaults** interface is displayed.

## Edit ISL Default

Use this task to edit a default.

> **Note**: You cannot edit the server.

**To edit a default**

1) Access the **Inactive Session Lockdown Defaults** 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**.

## Add ISL Default

Use this task to add a default.

**To add a default**

1) Access the **Inactive Session Lockdown Defaults** interface.

2) Click the **Add** button.

3) Enter the necessary default attributes.

4) Click **Save**.

## Delete ISL Default

Use this task to delete a default.

**To delete a default**

1) Access the **Inactive Session Lockdown Defaults** interface.

2) Click the **Actions** button beside the default you want to delete.

3) Select **Delete**.

**See also**

Working with Inactive Session Lockdown

# ISL Rules

This section includes the following:

- Display ISL Rules
- Manage ISL Rules

**See also**

Inactive Session Lockdown

# Display ISL Rules

This section describes how to display **Inactive Session Lockdown** (ISL) rules.

Use this task to do the following:

- Display List of Inactive Session Lockdown Rules
- Refresh List of ISL Rules

## 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**. 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:<br>**ENDJOB** - End the job (user must start the job over)<br>**DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message<br>**TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message<br>**HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job)<br>**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<br>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.

## 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.

**See also**

Working with Inactive Session Lockdown

# Manage ISL Rules

This section describes how to work with the **Inactive Session Lockdown** (ISL) feature. The 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 a 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:

- Access the Inactive Session Rules Interface
- Add ISL Rule
- Edit ISL Rule
- Delete ISL Rule

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

## Access the Inactive Session Rules Interface

Use this task to access the **Inactive Session Rules** interface.

#### To access the Inactive Session Rules interface

1) Expand the **Rules** menu.
2) Expand the **Inactive Sess. Lockdown** menu.
3) Select **Inactive Session Rules**. The **Inactive Session Rules** interface is displayed.

## Add ISL Rule

Use this task to add an ISL rule.

#### To add an ISL rule

1) Access the **Inactive Session 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:<br>**ENDJOB** - End the job (user must start the job over)<br>**DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message<br>**TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message<br>**HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job)<br>**SIGNOFF** - Signoff from the server |
| User Name /Group | Enter the name of the user or group to which the rule applies<br>**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<br>Note: ***Default** represent the default disconnect option defined for all object. |
| Rule Action | Identify whether the rule includes or excludes<br>**{}**INCLUDE* - Who and what is affected by a rule<br>**{}**EXCLUDE* - Who and what is not affected by a rule |
| Description | Enter a short description |

4) Click **Save**.

## 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 **Inactive Session 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**.

# Delete ISL Rule

Use this task to delete an ISL rule.

### To delete an ISL rule

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

### See also

Working with Inactive Session Lockdown

# Disconnect Options

This section includes the following:

- Display Disconnect Options
- Manage Disconnect Options

**See also**

Inactive Session Lockdown

# Display Disconnect Options

This section describes how to display disconnect options.

Use this task to do the following:

- Display List of Disconnect Options
- Refresh List of Disconnect Options

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

| Field | Description |
|---|---|
| Server | Name of server |
| DisconnectOption | Name assigned to the disconnect option |
| Time Limit (minutes) | Time limit defined for the disconnect option |

| | |
|---|---|
| Disconnect type | Type of disconnect option:<br>**ENDJOB** - End the job (user must start the job over)<br>**DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message<br>**TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message<br>**HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job)<br>**SIGNOFF** - Signoff from the server<br><br>**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.

## 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.

**See also**

Working with Inactive Session Lockdown

# Manage Disconnect Options

This section describes how to work with disconnect options.

Use this task to do the following:

- Access the Disconnect Options Interface
- Edit Disconnect Option
- Add Disconnect Option
- Delete Disconnect Option

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

## Access the Disconnect Options Interface

Use this task to access the **Disconnect Options** interface.

**To access the Disconnect Options interface**

1) Expand the **Rules** menu.
2) Expand the **Inactive Sess. Lockdown** menu.
3) Select **Disconnect Options**. The **Disconnect Options** interface is displayed.

## 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 **Disconnect Options** 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**.

## Add Disconnect Option

Use this task to add a disconnect option.

**To add a disconnect option**

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

2) Click the **Add** button.

3) Enter the necessary disconnect option attributes.

4) Click **Save**.

## Delete Disconnect Option

Use this task to delete a disconnect option.

### To delete a disconnect option

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

2) Click the **Actions** button beside the disconnect option you want to delete.

3) Select **Delete**.

### See also

Working with Inactive Session Lockdown

# Job Activity Monitor

The **Job Activity Monitor** feature 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

Use this feature to monitor the job activity of interactive users and batch jobs running on your system. This type of monitoring is useful for auditing the activity of highly-privileged users who have access to sensitive information or who have the ability to run critical batch processing for sensitive jobs that ensure system integrity.

Summary information and detailed job log data about monitored jobs is available through an interactive screen. Both summary and detailed job activity reports are provided and have customizable run parameters to help optimize performance.

There are several types of objects activities you can monitor:

- Batch jobs (using subsystems)
- Interactive jobs (using commands)
- Activity Monitoring Rules
- User Groups

**Note**: For more information about Job Activity Monitor, see the TGAudit User Guide 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.

This section includes the following topics:

- Working with Job Activity Monitor
- Job Activity Details
- Commands
- Subsystems

## See also

Rules

Rules Management

# Working with Job Activity Monitor

The **Job Activity Monitor** feature 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 User Guide 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.

This section includes the following topics:

- Job Activity Details
- Commands
- Subsystems

**See also**

Job Activity Monitor

# Job Activity Details

This section includes the following topics:

- Display Job Activity Rule Details
- Manage Job Activity Monitor Rules

**See also**

Job Activity Monitor

# Display Job Activity Rule Details

This section describes how to display job activity rules.

Use this task to do the following:

- Display List of Job Activity Rules
- Refresh List of Job Activity Rules

## 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**. 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):<br>**0** - No messages are logged<br>**1** - Log messages with log level greater than or equal to 1<br>**2** - Log messages with log level greater than or equal to 2<br>**3** - Log messages with log level greater than or equal to 3<br>**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<br>***YES** - Enable logging<br>***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.

## 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.

**See also**

Working with Job Activity Monitor

# Manage Job Activity Monitor 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. You can also use Job Activity Monitor (JAM) rules to filter (limit) the type of job 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:


- Access the Job Activity Monitor Rules Interface
- Add Job Activity Rule
- Edit Job Activity Rule
- Delete Job Activity Rule


**Note**: To work with the JAM rules, you must access the **Job Activity Monitor Rules** interface.

## Access the Job Activity Monitor Rules Interface

Use this task to access the **Job Activity Monitor Rules** interface.

#### To access the Job Activity Monitor Rules interface

1) Expand the **Rules** menu.
2) Expand the **Job Activity Monitor** menu.
3) Select **Job Activity Monitor Rules**. The **Job Activity Monitor Rules** interface is displayed.

## Add Job Activity Rule

Use this task to add a job activity rule.

#### To add a job activity rule

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

## 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 **Job Activity Monitor 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**.

## Delete Job Activity Rule

Use this task to delete a job activity rule.

**To delete a job activity rule**

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

**See also**

Working with Job Activity Monitor

# Commands

This section includes the following topics:

- Display Command Details
- Manage Commands

**See also**

Job Activity Monitor

# Display Command Details

This section describes how to display commands.

Use this task to do the following:

- Display List of Commands
- Refresh List of Commands

## 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**. 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.

## 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.

### See also

Working with Job Activity Monitor

# 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:

- Access the Commands Interface
- Add Command
- Edit Command
- Delete Command

**Note**: To work with the JAM commands, you must access the **Commands** interface.

## Access the Commands Interface

Use this task to access the **Commands** interface.

#### To access the Job Activity Monitor Rules interface

1) Expand the **Rules** menu.
2) Expand the **Job Activity Monitor** menu.
3) Select **Commands**. The **Commands** interface is displayed.

## 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**.

## 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**.

## 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

# Subsystems

This section includes the following topics:

- Display Subsystem Details
- Manage Subsystems

**See also**

Job Activity Monitor

# Display Subsystem Details

This section describes how to display subsystems.

Use this task to do the following:

- Display List of Subsystems
- Refresh List of Subsystems

## 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**. 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:<br>*__ACTIVE__ - Collect log data for job monitoring<br>*__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.

## 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.

### See also

Working with Job Activity Monitor

# 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 tasks.

Use this task to do the following:

- Access the Subsystems Interface
- Import Subsystems
- Export Subsystem
- Add Subsystem
- Edit Subsystem
- Delete Subsystem

> **Note**: To work with the JAM subsystems, you must access the **Subsystems** interface.

## Access the Subsystems Interface

Use this task to access the **Subsystems** interface.

**To access the Job Activity Monitor Rules interface**

1) Expand the **Rules** menu.
2) Expand the **Job Activity Monitor** menu.
3) Select **Subsystems**. The **Subsystems** interface is displayed.

## 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**. 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.

## Export Subsystem

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

**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.

## 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**.

## 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**.

## 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

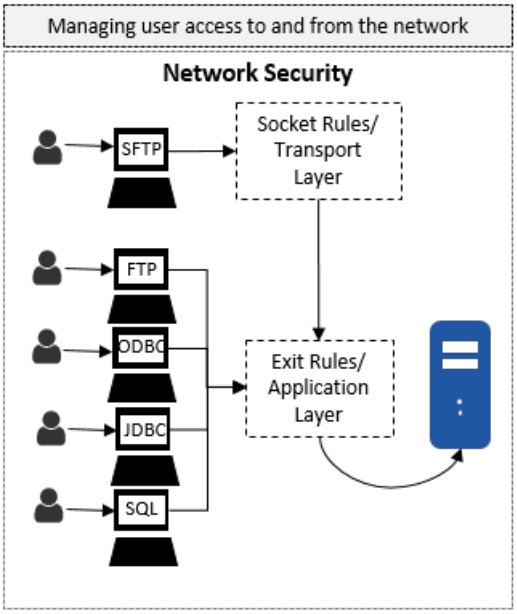
Working with Job Activity Monitor

# Network Security

The **Network Security** feature allows you to control who can access your network.

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

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




This section includes the following topics:

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

**See also**

Rules

Rules Management

# Working with Network Security

The **Network Security** feature allows you to control who can access your network.

This section includes the following topics:

- Network Defaults
- Socket Rules
- Remote Exit Rule
- Exit Points

**See also**

Network Security

# Network Defaults

This section includes the following topics:

- Display Network Defaults
- Manage Network Defaults

**See also**

Network Security

# Display Network Defaults

This section describes how to display network defaults.

Use this task to do the following:

- Display List of Network Defaults
- Refresh List of Network Defaults

## Display List of 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**. 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:<br>**Note**: Auditing is required if you plan to run network reports.<br>**{}**YES* - Auditing enabled (record audit data)<br>***NO** - Auditing disabled (do not record audit data)<br>**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:<br>***YES** - Alerts enabled<br>***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:<br>***YES** - debug enabled<br>***NO** - debug disabled |
| Primary Group Inheritance | Whether to allow primary group inheritance<br>***YES** - primary group inheritance enabled<br>***NO** - primary group inheritance disabled<br><br>**Note**: The primary group is the user ID entered in the **Group profile** field when using command **CHGUSRPRF**. The primary group is the first ID from which a user inherits privileges. |
| Supplemental Group Inheritance | Whether to allow supplemental group inheritance<br>***YES** - supplemental group inheritance enabled<br>***NO** - supplemental group inheritance disabled<br><br>**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.

## 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.

### See also

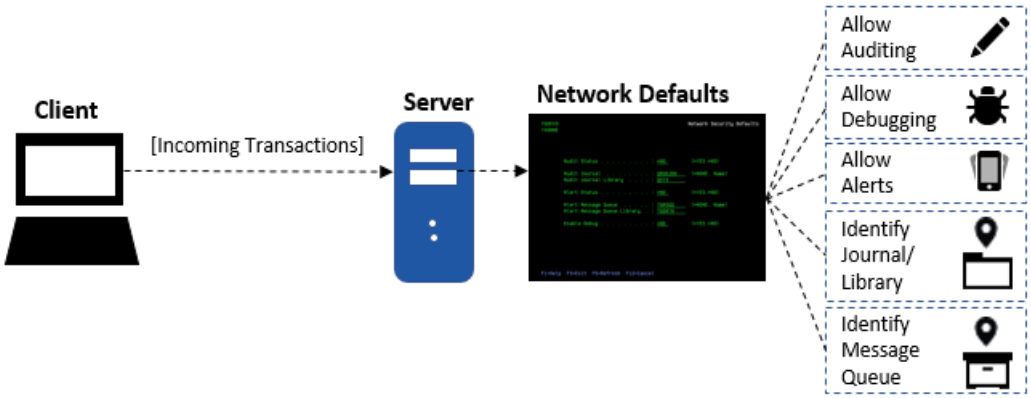
Working with Network Security

# Manage Network Defaults

This section describes how to work 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:

- Access the Network Security Defaults Interface
- Add Network Default
- Edit Network Default
- Delete Network Default

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

## Access the Network Security Defaults Interface

Use this task to access the **Network Security Defaults** interface.

**To access the Network Security Defaults interface**

1) Expand the **Rules** menu.

2) Expand the **Network Security** menu.

3) Select **Defaults**. The **Network Security Defaults** interface is displayed.

## 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**.

## 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**.

## 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 with Network Security

# Socket Rules

This section includes the following topics:

- Display Socket Rules
- Manage Socket Rules

**See also**

Network Security

# Display Socket Rules

This section describes how to display socket rules.

Use this task to do the following:

- Display List of Socket Rules
- Refresh List of Socket Rules

## 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**. 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:<br>***YES** - Alerts enabled<br>***NO** - Alerts disabled |
| Socket Action | The level at which action is taken:<br>***EXITLVL** - Exit point level<br>**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.

## 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.

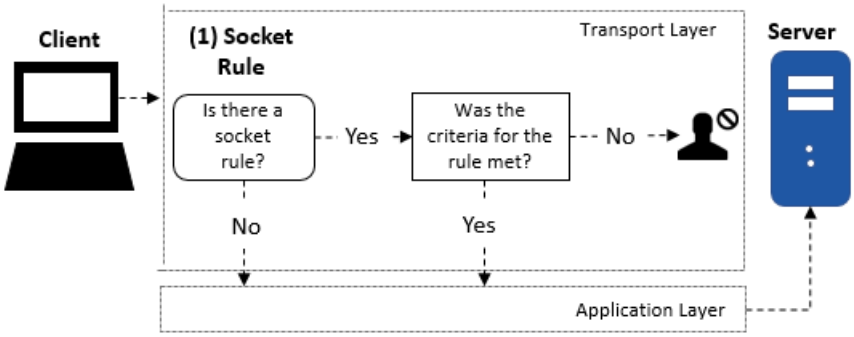
2) Click the **Refresh** button.

**See also**

Working with Network Security

# Manage Socket Rules

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




Use this task to do the following:

- Access the Socket Rules Interface
- Add Socket Rule
- Edit Socket Rule
- Delete Socket Rule

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

## Access the Socket Rules Interface

Use this task to access the **Socket Rules** interface.

#### To access the Socket Rules interface

1) Expand the **Rules** menu.
2) Expand the **Network Security** menu.
3) Select **Socket Rules**. The **Socket Rules** interface is displayed.

## Add Socket Rule

Use this task to add a socket rule.

#### To add a socket rule

1) Access the **Socket Rules** interface.

2) Click **Add**.

3) Enter the necessary rule attributes.

4) Click **Save**.

## 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**.

## 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 with Network Security

# Remote Exit Rules

This section includes the following topics:

- Display Remote Exit Rule Details
- Manage Remote Exit Rules

**See also**

Network Security

# Display Remote Exit Rule Details

This section describes how to display remote exit rules.

Use this task to do the following:

- Display List of Remote Exit Rules
- Refresh List of Remote Exit Rules

## 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**. 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:<br>***YES** - Alerts enabled<br>***NO** - Alerts disabled |
| Exit Rule Action | The level at which action is taken:<br>***EXITLVL** - Exit point level<br>**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.

## 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.

**See also**

Working with Network Security

# Manage Remote Exit Rules

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

**Example Usage:**

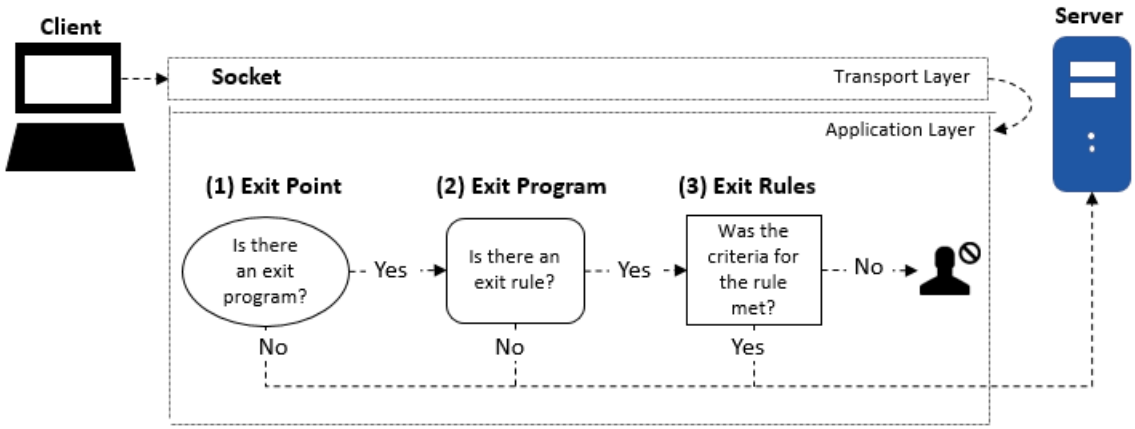
You might need a rule to reject all incoming transactions (connection) initiated by a specific user or member of a user group.

**Client-Server Communication Process via transport layer:**

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

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

**(3) Exit Rule**:  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:

- Access the Remote Exit Rules Interface
- Add Remote Exit Rules
- Edit Remote Exit Rules
- Delete Remote Exit Rules

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

## Access the Remote Exit Rules Interface

Use this task to access the **Remote Exit Rules** interface.

**To access the Remote Exit Rules interface**

1) Expand the **Rules** menu.

2) Expand the **Network Security** menu.

3) Select **Remote Exit Rules**. The **Remote Exit Rules** interface is displayed.

## 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**.

## 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**.

## 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 with Network Security

# Exit Points

This section includes the following topics:

- Display Exit Point Configuration Details
- Manage Exit Point

**See also**

Network Security

# Display Exit Point Configuration Details

This section describes how to display exit points.

Use this task to do the following:

- Display List of Exit Point Configurations
- Refresh List of Exit Point Configurations

## 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**. 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<br>*__YES__ - Record incoming transaction data in the audit journal<br>*__NO__ - Do not record incoming transaction data in the audit journal<br><br>__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.<br>*__YES__ - Apply exit rules (enable network security)<br>*__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<br>*__ALL__ - Record an alert for all (PASS and FAIL) connection attempts<br>*__FAIL__ - Record only FAIL connection attempts<br>*__NONE__ - Do not record alerts<br><br>__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<br>*__YES__ - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions<br>*__NO__ - Do not enable the intelligence engine to create rules<br><br>__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<br>*__ALL__ - Collect and display all (PASS and FAIL) incoming transactions<br>*__FAIL__ - Collect and display only rejected (FAIL) incoming transactions<br>*__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.<br>*__YES__ - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists<br>*__NO__ - No function usage rule is applied at the exit point<br>*__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<br>*__YES__ - Exit points are installed and ready for use<br>*__NO__ - Exit points are not installed<br><br>__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.

## 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.

### See also

Working with Network Security

# Manage Exit Point

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

**Analogy**

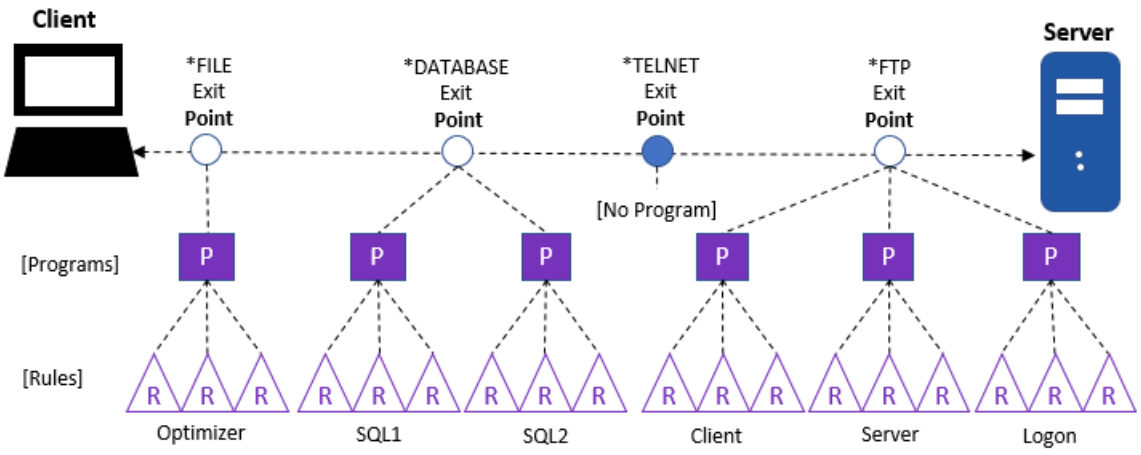
The prior paragraph uses a lot of jargon, so here is an analogy to help you conceptualize what an exit point represents. Say that your IBM server is a building. In the past, if someone wanted to access your building, they would just walk to it. Then, at some point, people started riding horses, and then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

- Access the Exit Point Configuration Interface
- Add Exit Point Configuration
- Edit Exit Point Configuration
- Delete Exit Point Configuration

- Cycle Server

> **Note**: To work with the remote exit rules, you must access the **Exit Point Configuration** interface.

## Access the Exit Point Configuration Interface

Use this task to access the **Exit Point Configuration** interface.

**To access the Exit Point Configuration interface**

1) Expand the **Rules** menu.
2) Expand the **Network Security** menu.
3) Select **Exit Point Config**. The **Exit Point Configuration** interface is displayed.

## 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**.

## 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**.

## 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**.

## 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 with Network Security

# Resource Manager

The **Resource Manager** feature allows you to create user authority schemas.

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

This section includes the following topics:

- Working with Resource Manager
- Resource Manager Defaults
- Authority Schemas
- Authority Schema Rules

**See also**

Rules

Rules Management

# Working with Resource Manager

The **Resource Manager** feature allows you to create user authority schemas.

This section includes the following topics:

- Resource Manager Defaults
- Authority Schemas
- Authority Schema Rules

**See also**

Resource Manager

# Resource Manager Defaults

This section includes the following topics:

- Display Resource Manager Defaults
- Manage Resource Manager Defaults

**See also**

Resource Manager

# Display Resource Manager Defaults

This section describes how to display **Resource Manager** defaults.

Use this task to do the following:

- Display List of Resource Manager Defaults
- Display List of Resource Manager Default Activities
- Refresh List of Resource Manager Defaults

## Display List of 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**. 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<br>**Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.<br>**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:<br>**Y** - Enable tracking of changes<br>**N** - Disable tracking of changes<br>**Tip**: Set this flag to **Y** if you plan to run the resource manager change reports.<br>**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.

## Display List of Resource Manager Default Activities

Use this task to view the activity (additions, deletions, modifications) associated with the defaults.

**To display the Resource Manager Defaults activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Resource Manager** menu.

3) Select **Defaults**. The **Resource Manager Defaults** interface is displayed.

4) Select the desired server. The activities associated with the selected server are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## 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**

1) Access the **Rules** interface.

2) Click the **Refresh** button.

**See also**

Working with Resource Manager

# Manage Resource Manager Defaults

This section describes how to work 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

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

Use this task to do the following:

- Add Resource Manager Default
- Edit Resource Manager Default
- Delete Resource Manager Default

## 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**.

## 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**.

## 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

# Authority Schemas

This section includes the following topics:

- Display Authority Schemas
- Manage Authority Schemas

**See also**

Resource Manager

# Display Authority Schemas

This section describes how to display authority schemas.

Use this task to do the following:

- Display List of Schemas
- Display List of Schema Activities
- Refresh List of Schemas

## 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**. 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 were compared to the authority schema and compliance with the schema was enforced |
| Alert Status | Whether alerts are enabled:<br>*__YES__ - Enable alerts (create admin alerts)<br>*__NO__ - Disable alerts |
| Schema Description | Description of the authority schema |
| Compliance Status | Whether the current authority levels comply with the schema<br>*__PASS__ - User authorities comply with the current authority scheme<br>*__FAIL__ - User authorities do not comply with the current authority scheme<br>**Note**: See Manage Authority Schemas 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.

## Display List of Schema Activities

Use this task to view the activity (additions, deletions, modifications) associated with the schema.

**To display the Schema activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Authority Scheme Config**. The **Authority Schema Configuration** interface is displayed.

4) Select the desired schema. The activities associated with the selected schema are displayed in the **Activity** pa ne (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## 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**

1) Access the **Rules** interface.

2) Click the **Refresh** button.

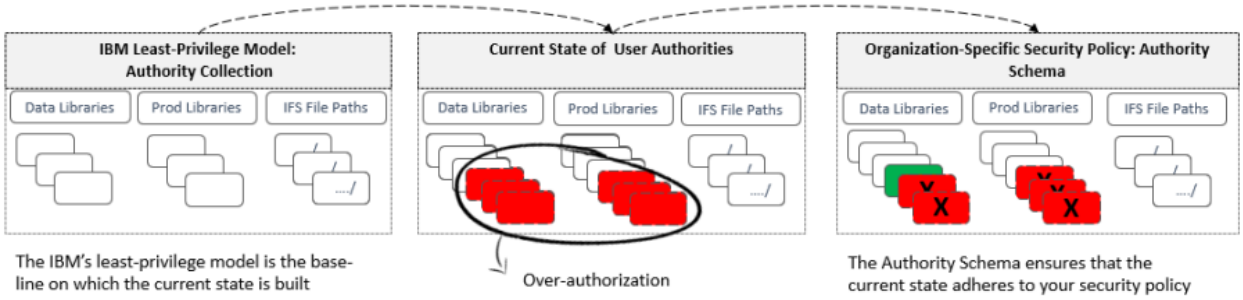
**See also**

Working with Resource Manager

# Manage Authority Schemas

This section describes how to work 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 implement user authorities. Therefore, each authority schema should be unique to an organization and be based on a well-defined security policy.

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




- Add Schema
- Edit Schema
- Delete Schema
- Run Schema Compliance Report
- Run Schema Enforcement

## 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) Complete the following fields:

| Field | Description |
|---|---|
| Server | Name of server |
| Schema ID | ID assigned to the schema |
| Schema Description | Description of the authority schema |
| Alert Status | Whether alerts are enabled:<br>***YES** - Enable alerts (create admin alerts)<br>***NO** - Disable alerts |
| Include IFS or Library Object | Identify the IFS folder or object library to which the schema applies |

4) Click **Next**.

5) Complete the following fields:

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

| Field | Description |
|---|---|
| Object Name | Name of the object or one of the following:<br>generic* - First few letters of an object name followed by an asterisk (wildcard).<br>This indicates that all objects that begin with the letters identified are to be included.<br>***ALL** - Include all objects |
| Object Library | Name of the library you want to monitor, or enter one of the following:<br>***ALL** - Include all libraries<br>***NONE** - Exclude all libraries |
| Object Type | Type of object to which the rule applies<br>***CMD** - Command<br>***CLS** - Class<br>***DTAARA** - Data area<br>***FILE** - File<br>***JOBD** - Job description<br>***JOBQ** - Job queue<br>***JRNRCV** - Journal receiver<br>***MODULE** - Module<br>***OUTQ** - Output queue<br>***PGM** - Program<br>***SBSD** - Subsystem description<br>***SQLPKG** - SQL package<br><br>**Note**: ***ALL** - Include all object types |
| ASP Name | Either the ASP (Auxiliary Storage Pool) for the system libraries<br>**Note**: If you enter ***SYSBAS**, the system ASP and all basic user ASPs are included. |
| Object Owner | Name of the object owner |
| Authorization List | Name of the authority list to which this authority schema applies, or enter ***NONE** if not applicable<br>**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<br><br>**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. |
| 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:<br>***YES** - Enable the program to adopt the authorities from the previous program<br>***NO** - Disable the program from adopting the authorities from the previous program |

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

6) Click **Next**.

7) Complete the following fields:

| Field | Description |
|---|---|
| IFS Path | Enter the file path for the IFS |

8) Click **Save**.

## 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**.

## 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**.

## 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**.

## 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

# Authority Schema Rules

This section includes the following topics:

- Display Authority Schema Rules
- Manage Authority Schema Rules

**See also**

Resource Manager

# Display Authority Schema Rules

This section describes how to display authority schema rules.

Use this task to do the following:

- Display List of Authority Schema Rules
- Display List of Authority Schema Rule Activities
- Refresh List of Authority Schema Rules

## 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**. 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<br>**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:<br>***ALL** - Include all libraries<br>***NONE** - Exclude all libraries |
| Object Name | Name of the object or one of the following:<br>generic* - First few letters of an object name followed by an asterisk (wildcard).<br>This indicates that all objects that begin with the letters identified are to be included.<br>***ALL** - Include all objects |
| Object Type | Type of object to which the rule applies<br>***CMD** - Command<br>***CLS** - Class<br>***DTAARA** - Data area<br>***FILE** - File<br>***JOBD** - Job description<br>***JOBQ** - Job queue<br>***JRNRCV** - Journal receiver<br>***MODULE** - Module<br>***OUTQ** - Output queue<br>***PGM** - Program<br>***SBSD** - Subsystem description<br>***SQLPKG** - SQL package<br><br>**Note**: ***ALL** - Include all object types |

| | |
|---|---|
| Object Owner | Name of the object owner |
| Auth List | Name of the authority list to which this authority schema applies, or enter ***NONE** if not applicable<br>**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.

## Display List of Authority Schema Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the rule.

#### To display the Authority Schema Rule activity

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Authority Scheme Config**. The **Authority Schema Configuration** interface is displayed.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of Authority 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

1) Access the **Rules** interface.

2) Click the **Refresh** button.

#### See also

Working with Resource Manager

# Manage Authority Schema Rules

This section describes how to work with **Authority Schema Rules** (details).

Use this task to do the following:

- Add Schema Rule
- Edit Schema Rule
- Delete Schema Rule

## 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:<br>generic* - First few letters of an object name followed by an asterisk (wildcard).<br>This indicates that all object that begin with the letters identified are to be included.<br>***ALL** - Include all objects |
| Object Library | Enter the name of the library you want to monitor or enter one of the following:<br>***ALL** - Include all libraries<br>***NONE** - Exclude all libraries |
| Object Type | Enter the name of the object type or one of the following:<br>***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<br>**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:<br>***YES** - Enable the program to adopt the authorities from the previous program<br>***NO** - Disable the program from adopting the authorities from the previous program |
| Exception | Identify whether the rule (detail) is an exception |

5) Click **Save**.

## 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**.

## 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

# User Profile Manager

The **User Profile Manager** (UPM) feature allows you to create blueprints on which to base user profiles.

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

This section includes the following topics:


- Working with User Profile Manager
- User Profile Manger Defaults
- Archived Profiles
- Blueprints
- Password Rules
- Profile Inactivity
- User Exclusions
- User Profiles


**See also**

Rules

Rules Management

# Working with User Profile Manager

The **User Profile Manager** (UPM) feature allows you to create blueprints on which to base user profiles.

This section includes the following topics:

- UPM Defaults
- Archived Profiles
- Blueprints
- Password Rules
- Profile Inactivity
- User Exclusions
- User Profiles

**See also**

User Profile Manager

# User Profile Manger Defaults

This section includes the following topics:

- Display UPM Defaults
- Manage UPM Defaults

**See also**

User Profile Manager

# Display UPM Defaults

This section describes how to display **User Profile Manager** (UPM) defaults.

Use this task to do the following:

- Display List of UPM Defaults
- Display List of UPM Default Activities
- Refresh List of UPM Defaults

## Display List of UPM Defaults

Use this task to view the list of defaults.

#### To display the Profile Manager Defaults

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Defaults**. The **User Profile Defaults** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Audit Journal | Journal in which to store profile manager usage data<br><br>**Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.<br><br>**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 | Indicates whether to collect data about profile changes:<br>**Y** - Enable tracking of changes<br>**N** - Disable tracking of changes<br><br>**Tip**: Set this flag to **Y** if you plan to run the resource manager change reports.<br><br>**Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules |

| | |
|---|---|
| Alerting Status | Indicates whether alerts are enabled:<br>*__YES__ - Enable alerts (create admin alert)<br>*__NO__ - Disable alerts |
| Alert Message Queue | Queue in which to store alerts |
| Alert Message Queue Library | Library in which to store the queue |
| Archive User Profile | Indicates whether to archive inactive profiles:<br>*__YES__ - Create an archive<br>*__NO__ - Do not create an archive<br><br>__Tip__: For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met:<br><br>a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.)<br>b. The user profile is associated with a blueprint<br>c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion |
| Archived Profiles Retention (days) | Number of days an archived profile is retained by the system |
| Exit Programs Installed | Indicates whether the exit programs necessary for profile management (including archiving) are installed:<br>*__YES__ - The exit programs that support user profile management are installed<br>*__NO__ - The exit programs that support user profile management are uninstalled<br><br>__Note__: See Manage UPM Defaults for instruction on adding exit programs. |
| Action | Click on the __Action__ button to see the list of tasks you can perform |

**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.

# Display List of UPM Default Activities

Use this task to view the activity (additions, deletions, modifications) associated with the user defaults.

### To display the Profile Manager Defaults activity

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Defaults**. The **User Profile Defaults** interface is displayed.

4) Select the desired server. The activities associated with the selected server are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

# Refresh List of UPM Defaults

Use this task at any time to refresh the **User Profile 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

1) Access the **User Profile Defaults** interface.

2) Click the **Refresh** button.

### See also

Working with User Profile Manager

# Manage UPM Defaults

This section describes how to work with **User Profile Manager** (UPM) defaults.

Use this task to do the following:

- Access the User Profile Defaults Interface
- Edit UPM Default Settings
- Enable Profile Auditing
- Enable Profile Alerts
- Enable Profile Archiving

**Note**: To work with the resource manager, you must access the **User Profile Defaults** interface.

## Access the User Profile Defaults Interface

Use this task to access the **User Profile Defaults** interface.

#### To access the User Profile Defaults interface

1) Access the **Rules** interface.
2) Select **User Profile Manager** to expand the tree.
3) Select **Defaults**. The **User Profile Defaults** interface is displayed.

## Edit UPM Default Settings

Use this task to edit the User Profile Defaults.

#### To edit User Profile Defaults

1) Access the **User Profile Defaults** interface.
2) Click the **Actions** button for the user profile you want to modify.
3) Select **Edit**.
4) Modify the following fields as necessary.

| Field | Description |
|---|---|
| Server | Name of server to which the default applies<br><br>**Note**: This field is for display only and cannot be modified |
| Audit Journal | Journal in which to store profile manager usage data<br><br>**Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.<br><br>**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 profile changes:<br>**Y** - Enable tracking of changes<br>**N** - Disable tracking of changes<br><br>**Tip**: Set this flag to **Y** if you plan to run the resource manager change reports.<br><br>**Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules |
| Alerting Status | Indicates whether alerts are enabled:<br>***YES** - Enable alerts (create admin alert)<br>***NO** - Disable alerts |
| Alert Message Queue | Queue in which to store alerts |
| Alert Message Queue Library | Library in which to store the queue |
| Archive User Profile | Whether to archive inactive profiles:<br>***YES** - Create an archive<br>***NO** - Do not create an archive<br><br>**Tip**: For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met:<br><br>a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.)<br>b. The user profile is associated with a blueprint<br>c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion |

| | |
|---|---|
| Archived Profiles Retention (days) | Number of days an archived profile is retained by the system |

5) Click **Save**.

## Enable Profile Auditing

Use this task to enable profile change auditing.

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

**To enable profile auditing**

1) Access the **User Profile Defaults** interface.
2) Click the **Actions** button for the user profile you want to modify.
3) Select **Edit**.
4) In the **Audit Journal** field, enter the name of the journal in which to store changes.
5) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
6) In the **Audit Configuration Changes** field, enter ***YES**.
7) Click **Save**.

> **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules

## Enable Profile Alerts

Use this task to enable profile change alerts.

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

**To enable profile alerts**

1) Access the **User Profile Defaults** interface.
2) Click the **Actions** button for the user profile you want to modify.

3) Select **Edit**.

4) In the **Alerting Status** field, enter ***YES**.

5) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.

6) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.

7) Click **Save**.

## Enable Profile Archiving

Use this task to enable archiving of inactive user profiles.

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

**To enable profile archiving**

1) Access the **User Profile Defaults** interface.

2) Click the **Actions** button for the user profile you want to modify.

3) Select **Edit**.

4) In the **Archive User Profile** field, enter ***YES**.

5) In the **Archive Profiles Retention** field, enter the number of days the archived should be retained.

6) Click **Save**.

### See also

Working with User Profile Manager

Display User Profiles

# Archived Profiles

This section includes the following topics:

- Display Archived Profile Details
- Manage Archived Profile

**See also**

User Profile Manager

# Display Archived Profile Details

This section describes how to display archive profiles.

Use this task to do the following:

- Display List of Archived Profiles
- Display List of Archived Profile Activities
- Refresh List of Archived Profiles

## Display List of Archived Profiles

Use this task to view the list of archived profiles.

#### To display the list of archived profiles

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Archived Profiles**. The **Archived Profiles** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Name of server to which the archive profile applies |
| User Name | User or user group to which the archive profile applies |
| Archived Date | Date on which the user profile was archived |
| User Description | Description of the user |
| Arch Available | Where archive is available |
| Archived Library | Name of the archive library |
| Archived File | Name of the archive file |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Archived Profile Activities

Use this task to view the activity (additions, deletions, modifications) associated with the archived profiles.

#### To display the Archived Profile activity

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Archived Profiles**. The **Archived Profiles** interface is displayed in the right pane.

4) Select the desired server. The activities associated with the selected server are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of Archived Profiles

Use this task at any time to refresh the **Archived Profiles** 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

1) Access the **Archived Profiles** interface.

2) Click the **Refresh** button.

### See also

Working with User Profile Manager

# Manage Archived Profile

This section describes how to work with an archive profile.

Use this task to do the following:

- Access the Archived Profiles Interface
- Reactivate Archived Profile
- Delete Archived File

> **Note**: To work with the user exclusions, you must access the **Archive Profiles** interface.

## Access the Archived Profiles Interface

Use this task to access the **Archive Profiles** interface.

#### To access the Archive Profiles interface

1) Access the **Rules** interface.
2) Select **User Profile Manager**.
3) Select **Archive Profiles**. The **Archive Profiles** interface is displayed.

## Reactivate Archived Profile

Use this task to reactive an archived profile.

> **Note**: Profiles are archived (retired from the system and stored in an archive file) once they meet the inactivity requirements set in the Manage Profile Inactivity Settings.

#### To reactive an archived profile

1) Access the **Archive Profiles** interface.
2) Click the **Actions** button for the archive profile you want to reactivate.
3) Select **Reactivate Profile**.
4) Click **Reactivate Profile**.

## Delete Archived File

> **Warning**: Before deleting an archive file, ensure you have a back-up of the file.

Use this task to delete an archive file.

#### To delete an archive file

1) Access the **Archive Profiles** interface.

2) Click the **Actions** button for the archive file you want to delete.

3) Select **Delete**.

4) Click **Delete**.

**See also**

Working with User Profile Manager

# Blueprints

This section includes the following topics:

- Display Blueprint Details
- Manage Blueprints

**See also**

User Profile Manager

# Display Blueprint Details

This section describes how to display blueprints.

Use this task to do the following:

- Display List of Blueprints
- Display List of Blueprint Activities
- Apply Blueprint Display Filter
- Reset Blueprint Display Filter
- Refresh List of Blueprints

## Display List of Blueprints

Use this task to view the list of blueprints.

**To display the list of blueprints**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Blueprints**. The **Work with Blueprints** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Name of server to which the blueprint applies |
| Blueprint ID | ID assigned to the blueprint |
| User group | Name of user group to which the blueprint applies |
| Prf Auth | Whether object authorities are defined:<br>***YES** - One or more object authorities are defined for the blueprint<br>***NO** - No object authorities are defined |
| Auth List | Whether authority lists are defined:<br>***YES** - One or more authority lists are defined for the blueprint<br>***NO** - No object authorities are defined |
| 3rd Party | Whether 3rd party scripts are defined:<br>***YES** - One or more 3rd party scripts are defined for the blueprint<br>***NO** - No 3rd party scripts are defined |
| Alt Sts | Whether alerts are enabled:<br>***YES** - Alerts enabled (create admin alerts)<br>***NO** - Alerts disabled |
| Compliance Date | Date and time at which the last check for authority schema compliance was performed |
| Inact Ovr | Whether inactivity overrides are enabled:<br>***YES** - Overrides are enabled<br>***NO** - Overrides disabled |

| | |
|---|---|
| Inact Prf | Whether inactive profiles exist (according to last report run):<br>**Y** - Inactive profile were found (consider running enforcement)<br>**N** - Inactive profiles were not found |
| Comp Status | Whether the current authority levels comply with the schema<br>***PASS** - User authorities comply with the current authority scheme<br>***FAIL** - User authorities do not comply with the current authority scheme |
| Blueprint Description | Description of the authority schema |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Blueprint Activities

Use this task to view the activity (additions, deletions, modifications) associated with the user defaults.

**To display the Blueprint activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Blueprints**. The **Work with Blueprints** interface is displayed in the right pane.

4) Select the desired server. The activities associated with the selected server are displayed in the **Activity** pane (at the bottom of the screen).

**Note**: A tab appears for each group of parameters: Profile Parameters, Profile Authorities, Authority Lists, 3rd Party, Inactive Overrides, Users, Non-compliant Profiles, Blueprint Permissions, Blueprint Additions.

## Apply Blueprint Display Filter

Use this task to limit the list of blueprints displayed based on selection criteria (multiple options) you define.

**To apply a filter**

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

2) Click the **Filter** button.

3) Enter the desired selection criteria in the fields provided.

4) Click the **Filter** button. The individual criterion by which you are filtering the display appear as removable options above the network activity display.

**Alternatively,** you can also apply a quick filter (single option) by clicking directly on text in the blueprint display. Again, use the **Filter** button to filter the display based on multiple options.

## Reset Blueprint Display Filter

Use this task to remove a display filter.

**To reset the filter**

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

2) Click the **Reset Filter** button.

## Refresh List of Blueprints

Use this task at any time to refresh the **Work with Blueprints** 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**

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

2) Click the **Refresh** button.

**See also**

Working with User Profile Manager

# Manage Blueprints

This section describes how to work with blueprints.


- Access the Blueprints Interface
- Add Blueprint
- Copy Blueprint
- Delete Blueprint
- Add Blueprint User
- Edit Blueprint User
- Delete Blueprint User
- Display Non-Compliant Profiles Identified in Last Blueprint Report
- Apply Non-Compliant Profile Display Filter
- Reset Non-Compliant Profile Display Filter
- Run Blueprint Compliance Report
- Run Blueprint Enforce


**Note**: To work with the blueprints, you must access the **Work with Blueprints** interface.

## Access the Blueprints Interface

Use this task to access the **Blueprints** interface.

#### To access the Blueprints interface

1) Access the **Rules** interface.

2) Select **User Profile Manager**.

3) Select **Blueprints**. The **Work with Blueprints** interface is displayed.

## Add Blueprint

Use this task to add a blueprint. There a number of details that need to be included in each blueprint, so a wizard has been designed to help you complete this multi-step process.

#### To add a blueprint

1) Access the **Blueprints** interface.

2) Click **Add** to add the following blueprint details.

| Field | Description |
|---|---|
| Server | Name of server to which the blueprint applies |
| Blueprint ID | ID you want to assign to the blueprint |

| | |
|---|---|
| Blueprint Description | Text describing the purpose of the blueprint |
| Alert Status | Indicates whether alerts are enabled:<br>***YES** - Enable alerts (create admin alerts)<br>***NO** - Disable alerts |
| User Scope | Enter the user group you want to associate with the blueprint.<br><br>**Note**: If you create a new profile based on this blueprint, the group you enter in this field will be the user group to which you can add new profiles.<br>This is also the user group whose members are updated when a blueprint is enforced. See Manage User Profiles, for information about adding a user profile based on an existing blueprint. |
| Inactivity until User Profile is disabled (days) | Number of days a profile must remain inactive profile before it is **disabled**<br><br>**Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied |
| Inactivity until User Profile is deleted (days) | Number of days a profile must remain inactive profile before it is **deleted**<br><br>**Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied |
| Object owner for objects owned by deleted profiles | Name of the user who should take over ownership of objects when/if a profile is disabled or deleted<br><br>**Note**: *DFT (Default) indicates that the standard owner defined by IBM should be applied |

3) Click **Next**.

**Tip**: To make parameters addition simpler, we've added three options:

-- Click **Add Suggested** to have the system add parameters suggested by the TG intelligence engine

-- Click **Add all default** to have the system add all IBM default parameters.

and/or

-- Click **Add Parameter** to add user-selected parameters. You decide.

**Note**: Steps **4-9** only appear if you select a parameter with the value of ***ANY**. Skip to **Step 10** in all other cases.

4) Click **Add Parameter** to add user-selected parameters.

5) Select the desired parameters from the list available.

6) Click **Add**.

7) Complete the following fields:

| Field | Description |
|---|---|

| | |
|---|---|
| Parameter Description | Description of object that triggers a violation<br><br>**Note**: Not editable. For display only. |
| Parameter Keyword | Parameter that triggers a violation<br><br>**Note**: Not editable. For display only. |
| Parameter Value | Parameter value that triggers a violation |

8) Click **Save** to return to the **User Profile Parameter Setting** interface.

9) Click **Next**.

10) Enter the necessary **User Profile Object Authorities** by completing the following fields.

(*USRPRF Object)

| Field | Description |
|---|---|
| Owner Authority | Authority-level assigned to the object owner |
| Public Authority | Authority-level assigned to a public user |

(*MSGQ Object)

| Field | Description |
|---|---|
| Object Owner | Identifies the owner of the objects |
| Owner Authority | Authority-level assigned to the object owner |
| Public Authority | Authority-level assigned to a public user |

11) Click **Next**.

12) Click **Add** to enter the necessary **Authority List Settings**.

13) Complete the following fields:

| Field | Description |
|---|---|
| Authority List | Enter the name of the authority list to which this blueprint applies<br><br>**Note**: An authority list displays the users who have the authority to access a specific object. |
| Authority Value | Enter the authority level you want to assign users who are members of the authority list:<br>***ALL** - Grant users all authorities (i.e., change, exclude, use, etc.)<br>***CHANGE** - Grant users change authority<br>***EXCLUDE** - Prohibit uses from performing operations on the object<br>***USE** - Grant access to the object attributes and allow users to use the object (but not change the object) |

14) Click **Add** to return to the **Authority List Settings** interface.

15) Click **Next**.

16) Click **Add** to add the necessary 3rd party integrations.

17) Complete the following fields:

| Field | Description |
|---|---|
| Script Type | Type of the third-party script |
| Script Statement | 3rd party script text |

18) Click **Add** to return to the **3rd Party Integration** interface.

19) Click **Next**.

20) Click **Add** to add the necessary blueprint permissions.

21) Complete the following fields:

| Field | Description |
|---|---|
| User/Group | User or user group that has permission to use the blueprint to create and change user profiles |
| Create Permissions | Whether the user/user group has permission to create new user profiles based on the blueprint<br>*__YES__ - Enable create<br>*__NO__ - Disable create |
| Change Permissions | Whether the user/user group has permission to change user profiles based on blueprint<br>*__YES__ - Enable change<br>*__NO__ - Disable change |

22) Click **Add** to return to the **Blueprint Permission** interface.

23) Click **Next**.

**Tip**: To make TG Central permission addition simpler, we've added two options:

-- Click **Add Suggested** to have the system add permissions suggested by the TG intelligence engine

and/or

-- Click **Add** to add user-define permissions. You decide.

24) Click **Add** to add the necessary TG Central blueprint permissions.

25) Complete the following fields:

| Field | Description |
|---|---|
| User | User or user group that has permission to use the blueprint to create and change user profiles |

| | |
|---|---|
| Create Permissions | Whether the user/user group has permission to create new user profiles based on the blueprint<br>*__YES__ - Enable create<br>*__NO__ - Disable create |
| Change Permissions | Whether the user/user group has permission to change user profiles based on blueprint<br>*__YES__ - Enable change<br>*__NO__ - Disable change |

26) Click **Add** to return to the **TG Central Blueprint Permission** interface.

27) Click **Save**.

## Copy Blueprint

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

**To copy a blueprint**

1) Access the **Blueprints** interface.

2) Click the **Action** button beside the blueprint you want to copy.

3) Select **Copy**.

4) Modify the parameters as necessary.

5) Press **Save**.

## Delete Blueprint

Use this task to delete a blueprint.

**To delete a blueprint**

1) Access the **Blueprints** interface.

2) Click the **Action** button beside the blueprint you want to delete.

3) Select **Delete**.

4) Press **Enter**.

## Add Blueprint User

Use this task to add a user (member) to a blueprint user group.

**To add blueprint user**

1) Access the **Blueprints** interface.

2) Select the desire blueprint to display the blueprint activities in the bottom pane.

3) Select the **Users** tab.

4) Click **Add**.

5) Complete the following fields.

| Field | Description |
|---|---|
| Name | Name of user |
| Description | Description of user |

5) Press **Save**.

## Edit Blueprint User

Use this task to edit the user details of a user (member) assigned to a blueprint group.

**To edit a blueprint user**

1) Access the **Blueprints** interface.
2) Select the desire blueprint to display the blueprint activities in the bottom pane.
3) Select the **Users** tab.
4) Click the **Action** button beside the user you want to edit.
5) Select **Edit**.
6) Modify the parameters as necessary.
7) Click **Save**.

## Delete Blueprint User

Use this task to delete a user (member) from a blueprint group.

**To delete a blueprint user**

1) Access the **Blueprints** interface.
2) Select the desire blueprint to display the blueprint activities in the bottom pane.
3) Select the **Users** tab.
4) Click the **Action** button beside the user you want to delete.
5) Select **Delete**.
6) Click **OK**.

## Display Non-Compliant Profiles Identified in Last Blueprint Report

Use this task to display blueprint compliance issues identified when the blueprint compliance report was the last run.

> **Tip**: Before you can display compliance issues you must run the blueprint compliance report.

**To display non-compliant profiles**

1) Access the **Blueprints** interface.

2) Select the desired blueprint to display the blueprint activities in the bottom pane.

3) Select the **Non-comp Profiles** tab to display the list of non-compliant profiles.

## Apply Non-Compliant Profile Display Filter

Use this task to limit the list of non-compliant profiles displayed based on selection criteria (multiple options) you define.

**To apply a filter**

1) Access the **Non-comp Profiles** tab.

2) Click the **Filter** button.

3) Enter the desired selection criteria in the fields provided.

4) Click the **Filter** button. The individual criterion by which you are filtering the display appear as removable options above the network activity display

> **Alternatively,** you can also apply a quick filter (single option) by clicking directly on text in the blueprint display. Again, use the **Filter** button to filter the display based on multiple options.

## Reset Non-Compliant Profile Display Filter

Use this task to remove a display filter.

**To reset the filter**

1) Access the **Non-comp Profiles** tab.

2) Click the **Reset Filter** button.

## Run Blueprint Compliance Report

Use this task to run the blueprint compliance report, which you can use to identify blueprint compliance issues.

**To display blueprint compliance issues**

1) Access the **Blueprints** interface.

2) Click the **Action** button beside the blueprint for which you want to display compliance issues.

3) Select **Run Compliance Report**.

4) Click **Run**.

## Run Blueprint Enforce

Use this task to enforce a blueprint.

**Tip**: Before enforcing a blueprint, first display the blueprint compliance issues to identify where non-compliance is occurring. In some cases, an issue of non-compliance might identify the need for an exclusion to be added. In other words, you might need to update the blueprint. Therefore, do not enforce a blueprint until you have completed your analysis of non-compliance issues.

**To enforce authority blueprint**

1) Access the **Blueprints** interface.
2) Click the **Action** button beside the blueprint for which you want to enforce compliance.
3) Select **Run Enforcement**.
4) Click **Run**.

## See also

Working with User Profile Manager

# Password Rules

This section includes the following topics:

- Display Password Rule Details
- Manage Password Rule Settings

**See also**

User Profile Manager

# Display Password Rule Details

This section describes how to display password rules.

Use this task to do the following:

- Display List of Password Rules
- Display List of Password Rule Activities
- Refresh List of Password Rules

## Display List of Password Rules

Use this task to view the list of password rules.

**To display the list of password rules**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Password Rule Settings**. The **Password Rule Settings** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Name of server to which the password rule applies |
| Current pwd level (QPWDLVL) | Desired password level |
| Pwd exit | Whether the exit program is installed<br><br>***YES** - Exit program present<br>***NO** - Exit program absent |
| Pwd Rule value set to *PWDSYSVAL | Whether to use default system values or custom rules<br><br>***YES** - Use default password system values<br>***NO** - Allow the admin to customize password rules<br><br>**Tip**: This value must be set to *NO if you want to use the profile manager feature to update password rules. |
| No. of mixed case letter (*MIXCASEn) | **[0-9]** - Number of mix-case letters required in the password |
| Limit repeat char (*CHRLMTREP) | Whether a password to contain characters that repeat (appears next to each other)<br><br>**Y** - Disallow consecutive use of characters<br>**N** - Allow consecutive use of characters |
| limit same char (*LMTSAMPOS) | Whether characters can be used in the same position as the previous password<br><br>**Y** - Disallow characters in the same position<br>**N** - Allow characters in the same position |

| | |
|---|---|
| Require upper/lower/ digits /special char (*REQANY3) | Whether a password is required to contain the following types of characters: uppercase, lowercase, special characters or digits<br><br>**Y** - Require character variation<br>**N** - Do not require character variation |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Password Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the selected server.

**To display the Blueprint activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Password Rule Settings**. The **Password Rule Settings** interface is displayed in the right pane.

4) Select the desired server. The activities associated with the selected server are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of Password Rules

Use this task at any time to refresh the **Password Rule Settings** 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**

1) Access the **Password Rule Settings** interface.

2) Click the **Refresh** button.

**See also**

Working with User Profile Manager

# Manage Password Rule Settings

This section describes how to work with password rules.

Use this task to do the following:

- Access the Password Rules Settings Interface
- Add Password Exit Program
- Delete Password Exit Program
- Edit Password Setting

> **Note**: To work with the user profiles, you must access the **TG User Profile Manager** interface.

## Access the Password Rules Settings Interface

Use this task to access the **Password Rules Settings** interface.

#### To access the Password Rules Settings interface

1) Access the **Rules** interface.
2) Select **User Profile Manager**.
3) Select **Password Rules Settings**. The **Password Rules Settings** interface is displayed.

## Add Password Exit Program

Use this task to add a password exit program.

#### To add a password exit program

1) Access the **Password Rules Settings** interface.
2) Click the **Add** button.
3) Complete the required fields.
4) Click **Save**.

## Delete Password Exit Program

Use this task to delete a password exit program.

#### To delete password exit program

1) Access the **Password Rules Settings** interface.
2) Click the **Actions** button for the password exit program you want to delete.
3) Select **Delete**.

## Edit Password Setting

Use this task to edit a password setting.

> **Note**: You cannot edit the server.

**To edit a password rule**

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

**See also**

Working with User Profile Manager

# Profile Inactivity

This section includes the following topics:

- Display Profile Inactivity Settings
- Manage Profile Inactivity Settings

**See also**

User Profile Manager

# Display Profile Inactivity Settings

This section describes how to display profile inactivity settings.

Use this task to do the following:

- Display List Inactivity Settings
- Display List Password Rule Activities
- Refresh List of Inactivity Settings

## Display List Inactivity Settings

Use this task to view the list of user profiles.

**To display the list of user profiles**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Profile Inactivity Settings**. The **Profile Inactivity Settings** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Name of server to which the inactivity rule applies |
| Inactivity until User Profile is disabled | Number of days before an inactive user profile is disabled |
| Inactivity until User Profile is deleted | Number of days before an inactive user profile is deleted |
| Delete profiles with password of *NONE | Whether to delete profiles that do not have an assigned password<br>***YES** - Delete the profiles<br>***NO** - Keep the profiles |
| Object owner for objects owned by deleted profiles | The name of the user who will inherit ownership of objects for deleted user profiles |
| Remove deleted Profiles from TG User Group | Whether to remove deleted profiles from TG user groups<br>***YES** - Delete the user profile from TG groups<br>***NO** - Keep the user profile as a member of TG groups |
| Remove deleted Profiles from TG Rules | Whether to remove deleted profiles from TG rules.<br>***YES** - Delete the user profile from rule definition<br>***NO** - Keep the user profile as part of rule definition |
| Alert when Inactivity is found | Whether to send an alert to the admin when inactive profiles are detected<br>***YES** - Enable alerts<br>***NO** - Disable alerts |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List Password Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the selected server.

### To display the Blueprint activity

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **Profile Inactivity Settings**. The **Profile Inactivity Settings** interface is displayed in the right pane.

4) Select the desired setting. The activities associated with the selected setting are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of Inactivity Settings

Use this task at any time to refresh the **Profile Inactivity Settings** 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

1) Access the **Profile Inactivity Settings** interface.

2) Click the **Refresh** button.

### See also

Working with User Profile Manager

# Manage Profile Inactivity Settings

This section describes how to work with Inactivity settings/rules.

Use this task to do the following:

- Access the Profile Inactivity Settings Interface
- Edit Inactivity Setting
- Run Inactivity Report
- Enforce Inactivity Setting

> **Note**: To work with the inactivity settings/rules, you must access the **Profile Inactivity Settings** interface.

## Access the Profile Inactivity Settings Interface

Use this task to access the **Profile Inactivity Settings** interface.

#### To access the Profile Inactivity Settings interface

1) Access the **Rules** interface.
2) Select **User Profile Manager**.
3) Select **Profile Inactivity Settings**. The **Profile Inactivity Settings** interface is displayed.

## Edit Inactivity Setting

Use this task to edit an inactivity setting/rule.

> **Note**: You cannot edit the server.

#### To edit an inactivity setting

1) Access the **Profile Inactivity Settings** interface.
2) Click the **Actions** button for the inactivity setting you want to modify.
3) Select **Edit**.
4) Modify the following attributes as necessary:

| Field | Description |
|---|---|
| Server | Name of server to which the inactivity rule applies |
| Inactivity until User Profile is disabled | Number of days before an inactive user profile is disabled |
| Inactivity until User Profile is deleted | Number of days before an inactive user profile is deleted |

| | |
|---|---|
| Delete profiles with password of *NONE | Whether to delete profiles that do not have an assigned password<br>***YES** - Delete the profiles<br>***NO** - Keep the profiles |
| Object owner for objects owned by deleted profiles | The name of the user who will inherit ownership of objects for deleted user profiles |
| Remove deleted Profiles from TG User Group | Whether to remove deleted profiles from TG user groups<br>***YES** - Delete the user profile from TG groups<br>***NO** - Keep the user profile as a member of TG groups |
| Remove deleted Profiles from TG Rules | Whether to remove deleted profiles from TG rules.<br>***YES** - Delete the user profile from rule definition<br>***NO** - Keep the user profile as part of rule definition |
| Alert when Inactivity is found | Whether to send an alert to the admin when inactive profiles are detected<br>***YES** - Enable alerts<br>***NO** - Disable alerts |
| Action | Click on the **Action** button to see the list of tasks you can perform. |

5) Click **Save**.

## Run Inactivity Report

Use this task to run the inactivity report.

**Tip**: Run the inactivity report prior to enforcing inactivity rules so that you have an understanding of the enforcement implications.

**To enforce an inactivity setting**

1) Access the **Profile Inactivity Settings** interface.

2) Click the **Actions** button for the inactivity rule you want to enforce.

3) Select **Run inactivity Report**.

4) Complete the following fields:

| Field | Description |
|---|---|
| Server | This is a read-only field. |
| Component | This is a read-only field. |
| Audit report | Enter ***YES** to enable auditing (tracking) |
| Users | User/group profile to include in the report |
| Days for disable user profile | Number of days a profile must remain inactive profile before it is **disabled**<br><br>**Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied |

| | |
|---|---|
| Days for delete user profile | Number of days a profile must remain inactive profile before it is **deleted**<br><br>**Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied |
| Enforcement | Enter ***NO** to display only (not enforce) compliance issues<br><br>**Tip**: Always display (run the report) and analyze before enforcing. |

5) Click **Run**.

## Enforce Inactivity Setting

Use this task to enforce an inactivity setting/rule.

> **Tip**: Run the inactivity report prior to enforcing inactivity rules so that you have an understanding of the enforcement implications.

**To enforce an inactivity setting**

1) Access the **Profile Inactivity Settings** interface.

2) Click the **Actions** button for the inactivity rule you want to enforce.

3) Select **Run Inactivity Enforcement**.

4) Complete the following fields:

| Field | Description |
|---|---|
| Server | This is a read-only field. |
| Component | This is a read-only field. |
| Audit report | Enter ***YES** to enable auditing (tracking) |
| Users | User/group profile to include in the report |
| Days for disable user profile | Number of days a profile must remain inactive profile before it is **disabled**<br><br>**Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied |
| Days for delete user profile | Number of days a profile must remain inactive profile before it is **deleted**<br><br>**Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied |
| Enforcement | Enter ***YES** to enforce the compliance issues<br><br>**Tip**: Always display (run the report) and analyze before enforcing. |

5) Click **Run**.

**See also**

## Working with User Profile Manager

# User Exclusions

This section includes the following topics:

- Display User Exclusion Details
- Manage User Exclusions

**See also**

User Profile Manager

# Display User Exclusion Details

This section describes how to display user exclusions.

Use this task to do the following:

- Display List of User Exclusions
- Display List of User Exclusion Activities
- Refresh List of User Exclusions

## Display List of User Exclusions

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

**To display the list of user exclusions**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **User Exclusions**. The **User Exclusions** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Name of server to which the user exclusion applies |
| User | User or user group to which the exclusion applies |
| Exclusion Type | Type of exclusion<br>*__ALL__ - All types<br>*__ACTIVITY__ - Exclude the user group from inactivity check<br>*__SYNC__ - Exclude the user group from synchronization with other iSeries systems |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of User Exclusion Activities

Use this task to view the activity (additions, deletions, modifications) associated with the user exclusions.

**To display user exclusion activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **User Profile Manager** menu.

3) Select **User Exclusions**. The **User Exclusions** interface is displayed in the right pane.

4) Select the desired user exclusion. The activities associated with the selected user exclusion are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of User Exclusions

Use this task at any time to refresh the **User Exclusions** 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

1) Access the **User Exclusions** interface.

2) Click the **Refresh** button.

### See also

Working with User Profile Manager

# Manage User Exclusions

This section describes how to work with user exclusions.

Use this task to do the following:

- Access the User Exclusions Interface
- Add User Exclusion
- Edit User Exclusions
- Copy User Exclusions
- Delete User Exclusion

> **Note**: To work with the user exclusions, you must access the **User Exclusions** interface.

## Access the User Exclusions Interface

Use this task to access the **User Exclusions** interface.

#### To access the User Exclusions interface

1) Access the **Rules** interface.
2) Select **User Profile Manager**.
3) Select **User Exclusions**. The **User Exclusions** interface is displayed.

## Add User Exclusion

Use this task to add a user exclusion.

#### To add a user exclusion

1) Access the **User Exclusions** interface.
2) Click **Add**. The **New User Exclusions** dialog appears.
3) Complete the following fields:

| Field | Description |
|---|---|
| Server | Name of server to which the user exclusion applies |
| User/Group | User or user group to which the exclusion applies |
| Exclusion Type | Type of exclusion<br>*__ALL__ - All types<br>*__ACTIVITY__ - Exclude the user group from inactivity check<br>*__SYNC__ - Exclude the user group from synchronization with other iSeries systems |
| Action | Click on the **Action** button to see the list of tasks you can perform |

4) Click **Save**.

## Edit User Exclusions

Use this task to edit a user exclusion.

> **Note**: You cannot edit the server.

**To edit a user exclusions**

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

## Copy User Exclusions

Use this task to copy a user exclusion.

**To copy a user exclusions**

1) Access the **User Exclusions** interface.
2) Click the **Actions** button for the user exclusion you want to modify.
3) Select **Copy**.
4) Modify the attributes as necessary:
5) Click **Save**.

## Delete User Exclusion

Use this task to delete a user exclusion.

**To delete a user exclusion**

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

**See also**

Working with User Profile Manager

# User Profiles

This section includes the following topics:

- Manage User Profiles

**See also**

User Profile Manager

# Manage User Profiles

This section describes how to work with profiles.

Use this task to do the following:

- Access the TG User Profile Manager Interface
- Create User Profile
- Change User Profile

> **Note**: To work with the user profiles, you must access the **TG User Profile Manager** interface.

## Access the TG User Profile Manager Interface

Use this task to access the **TG User Profile Manager** interface.

#### To access the TG User Profile Manager interface

1) Access the **Rules** interface.
2) Select **User Profile Manager**.
3) Select **Create/Change User Profiles**. The **TG User Profile Manager** interface is displayed.

## Create User Profile

Use this task to add a user profile.

#### To add a user profile

1) Access the **TG User Profile Manager** interface.
2) Complete the following fields:

| Field | Description |
|---|---|
| Server | Name of server to which the user profile applies |
| Action Type | Enter ***CRT** (Create) |
| Blueprint ID | Name of the blueprint on which to base the user profile |
| User Name | Name you want to assign to the user |
| User Description | Description of the user |
| Add Blueprint user group | Whether to add the user to the user group associated with the named blueprint<br>***YES** - Add the user to the blueprint user group<br>***NO** - Base the user profile on the blueprint only, but do not add the user to the blueprint user group |

3) Click **Run**.

# Change User Profile

Use this task to add a user profile.

### To change a user profile

1) Access the **TG User Profile Manager** interface.

2) Complete the following fields:

| Field | Description |
|---|---|
| Server | Name of server to which the user profile applies |
| Action Type | Enter ***CHG** (Change) |
| Blueprint ID | Name of the blueprint on which to base the user profile |
| User Name | Name you want to assign to the user |
| User Description | Description of the user |
| Add Blueprint user group | Whether to add the user to the user group associated with the named blueprint<br>***YES** - Add the user to the blueprint user group<br>***NO** - Base the user profile on the blueprint only, but do not add the user to the blueprint user group |

3) Click **Run**.

### See also

Working with User Profile Manager

# Detect Monitor

The **Detect Monitor** feature allows you to manage TGDetect monitors used for security alerts.

Monitors provide you with a means by which to track system activities that require that an individual (i.e., user or user group) or a log management tool (e.g., Sentinel, ELK, etc.) receives appropriate notifications (alerts).

This section includes the following topics:

- Working with Detect Monitors
- Command Monitor
- History Log Monitor
- Journal Monitor
- Message Queue Monitor
- SIEM Monitor
- Syslog Monitor

**See also**

Rules

Rules Management

# Working with Detect Monitors

The **Detect Monitor** feature allows you to manage TGDetect monitors used for security alerts.

This section includes the following topics:

- Display Detect Monitors
- Manage Detect Monitors

In addition, go here to learn more about each monitor type:

- Command Monitor
- History Log Monitor
- Journal Monitor
- Message Queue Monitor
- SIEM Monitor
- Syslog Monitor

**See also**

Detect Monitor

# Display Detect Monitors

This section describes how to display **Command Monitor** rule details.

Use this task to do the following:

- Display List of Detect Monitors
- Display List of Detect Monitor Activities
- Refresh List of Detect Monitors Interface

## Display List of Detect Monitors

Use this task to view the list of Detect monitors

**To display the List of Detect Monitors**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Monitors**. The **Detect Monitors** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Monitor Name | Name assigned to the monitor |
| Monitor Library | Library in which the monitor resides |
| Type | Type of monitor:<br>* **MSGQ** - Message queue monitor<br>***JRN** - Journal monitor<br>**Tip**: You can track multiple MSGQ and JRN monitors. |
| Description of monitor | Short description defining the purpose of the monitor |
| Calendar | Name of the calendar that defines when the rule is applicable |
| Protect | Whether monitor is internal (built-in):<br>**Y** - Internal (cannot be deleted)<br>**N** - Custom (can be deleted)<br>**Note**: Internal monitors are shipped with the product and cannot be deleted compare to custom message queue monitors which can be deleted. |

| | |
|---|---|
| Status | Whether monitoring is enabled:<br>*__ACTIVE__ - Monitor is enabled<br>*__INACTIVE__ - Monitor is disabled<br><br>__Note__: Only active monitors collect data for notifications purposes. |
| Daily Alerts | Number of daily alerts triggered |
| Monthly Alerts | Number of monthly alerts triggered |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Detect Monitor Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

#### To display the Detect Monitor activity

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Monitor**. The **Detect Monitors** interface is displayed in the right pane.

4) Select the desired monitor. The activities associated with the selected monitor are displayed in the **Activity** pan e (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of Detect Monitors Interface

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

1) Access the **Rules** interface.

2) Click the **Refresh** button.

#### See also

Working with Detect Monitors

# Manage Detect Monitors

Use this task to do the following:

- Access the Detect Monitors Interface
- Add Detect Monitor
- Delete Detect Monitor
- Start Detect Monitor

> **Note**: To work with the Detect monitors, you must access the **Detect Monitors** interface.

## Access the Detect Monitors Interface

Use this task to access the **Detect Monitors** interface.

#### To access the Detect Monitors interface

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Detect Monitors** menu.
3) Select **Monitor**. The **Detect Monitors** interface is displayed in the right pane.

## Add Detect Monitor

Use this task to add a detect monitor (message or journal).

#### To add a Detect monitor

1) Access the **Detect Monitors** interface.
2) Click **Add**.
3) Complete the following fields:

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Monitor Name | Name assigned to the monitor |
| Monitor Library | Library in which the  monitor resides |
| Monitor Type | Type of monitor:<br>* **MSGQ** - Message queue monitor<br>***JRN** - Journal monitor<br>**Tip**: You can track multiple MSGQ and JRN monitors. |
| Description | Short description defining the purpose of the monitor |

4) Click **Save**.

## Delete Detect Monitor

Use this task to delete a Detect monitor.

### To delete a Detect Monitor

1) Access the **Detect Monitors** interface.
2) Click the **Action** button beside the desired rule.
3) Select **Delete Monitor**.

## Start Detect Monitor

Use this task to start a Detect monitor.

> **Note**: Once started, the status of monitor will appear as ***Active**.

### To start a Detect Monitor

1) Access the **Detect Monitors** interface.
2) Click the **Action** button beside the desired rule.
3) Select **Start Monitor**.

### See also

Working with Detect Monitors

# Command Monitor

This section describes how to work with Command Monitor rules.

This section includes the following topics:

- Display Command Monitor Rules
- Manage Command Monitor Rules

**See also**

Detect Monitor

# Display Command Monitor Rules

This section describes how to display **Command Monitor** rule details.

Use this task to do the following:

- Display List of Command Monitor Rules
- Display List of Command Monitor Rule Criteria
- Display List of Command Monitor Rule Activities
- Display List of Command Monitor Rule Alerts
- Refresh List of Command Monitor Interface

## Display List of Command Monitor Rules

Use this task to view the list of command monitor rules.

#### To display the List of Command Monitor Rules

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Command Monitor Rules**. The **Command Monitors Rules** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Rule ID | Unique Identifier assigned to command rule |
| Rule Name | Name assigned to the rule |
| Calendar | Name of the calendar that defines when the rule is applicable |

| | |
|---|---|
| Daily Count | Number of daily alerts triggered by rule<br>**Note**: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered. |
| Monthly Count | Number of monthly alerts triggered by rule |
| Yearly Count | Number of yearly alerts triggered by rule |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Command Monitor Rule Criteria

Use this task to view the list of command monitor rule criteria.

**To display the List of Command Monitor Rule Criteria.**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Command Monitor Rules**. The **Command Monitors Rules** interface is displayed in the right pane.

4) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | The server to which the rule applies |
| Rule ID | Unique ID assigned to the rule for which you are displaying criteria |

| | |
|---|---|
| Command Name | Command for which you want to establish a rule |
| Library | Library in which you want to monitor using the rule |
| User Name | User/user group you want to monitor using the rule<br>**Tip**: Enter ***ALL** to monitor all users. |
| Rule Description | Description of the criteria |
| Action | Click on the **Action** button to see the list of tasks you can perform |

# Display List of Command Monitor Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

**To display the Command Monitor activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Command Monitor Rules**. The **Command Monitors Rules** interface is displayed in the right pane.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

# Display List of Command Monitor Rule Alerts

Use this task to view the list of command monitor alerts.

**To display the list of command monitor alerts**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Command Monitor Rules**. The **Command Monitors Rules** interface is displayed in the right pane.

4) Select the desired server. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Server to which the rule applies |

| | |
|---|---|
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Alert Type | Type of alert<br>*__EMAIL__ - Send an email alert to a specific user/group<br>*__MSG__ - Send a system message (message that appears when a user logs into the system)<br>*__CMD__ - Execute a command<br>*__SYSLOG__ - Send a notification to the system archive<br>*__EMAILDIST__ - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>*__TGCENTRAL__ - Send a notification to TGCentral |
| Alert Details | Recipient details |
| Msg to Send | Text included in the notification sent to the designated recipient |
| #Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter *__ALL__ to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Action | Click on the **Action** button to see the list of tasks you can perform |

## Refresh List of Command Monitor Interface

Use this task at any time to refresh the **Command Monitors 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

1) Access the **Command Monitors Rules** interface.

2) Click the **Refresh** button.

#### See also

Working with Detect Monitors

# Manage Command Monitor Rules

Use this task to do the following:

- Access the Command Monitor Rules Interface
- Add Command Monitor Rule
- Edit Command Monitor Rule
- Delete Command Monitor Rule
- Add Command Monitor Rule Criteria
- Edit Command Monitor Rule Criteria
- Delete Command Monitor Rule Criteria
- Add Command Monitor Alerts
- Edit Command Monitor Alerts
- Delete Command Monitor Alerts

**Note**: To work with the command monitor rules, you must access the **Command Monitor Rules** interface.

## Access the Command Monitor Rules Interface

Use this task to access the **Command Monitor Rules** interface.

#### To access the User Profile Defaults interface

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Detect Monitors** menu.
3) Select **Command Monitor Rules**. The **Command Monitor Rules** interface is displayed in the right pane.

## Add Command Monitor Rule

Use this task to add a command monitor rule.

#### To add a Command Monitor  rule

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

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Rule ID | Enter a unique identifier for the command rule |
| Rule Name | Enter a name for the command rule |

| | |
|---|---|
| Calendar | Enter the name of the calendar that defines when the rule is applicable<br><br>**Tip**: Enter ***NONE** if no calendar is applicable. |

4) Click **Save**.

# Edit Command Monitor Rule

Use this task to edit a command monitor rule.

**To edit a Command Monitor rule**

1) Access the **Command Monitor Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Edit**.

4) Modify the parameters as necessary.

5) Click **Save**.

# Delete Command Monitor Rule

Use this task to delete a command monitor rule.

**To delete a Command Monitor rule**

1) Access the **Command Monitor Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Delete**.

# Add Command Monitor Rule Criteria

Use this task to add a command monitor criterion.

**To add a Command Monitor rule criterion**

1) Access the **Command Monitor Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) In the **Rule Criteria** pane, click **Add**.

4) Complete the following fields:

| Field | Description |
|---|---|
| Server | The server to which the rule applies |
| Command Name | Command for which you want to establish a rule |

| | |
|---|---|
| Command Library | Library in which you want to monitor using the rule |
| Command User Name/Group | User/user group you want to monitor using the rule<br>**Tip**: Enter ***ALL** to monitor all users. |

5) Click **Save**.

# Edit Command Monitor Rule Criteria

Use this task to edit a command monitor rule criterion.

**To edit a Command Monitor rule criterion**

1) Access the **Command Monitor Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired rule criterion.

4) Select **Edit**.

5) Modify the parameters as necessary.

6) Click **Save**.

# Delete Command Monitor Rule Criteria

Use this task to delete a command monitor rule criterion.

**To delete a Command Monitor rule criterion**

1) Access the **Command Monitor Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired criterion.

4) Select **Delete**.

# Add Command Monitor Alerts

Use this task to add a command monitor alert.

**To add a Command Monitor alert**

1) Access the **Command Monitor Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) In the **Alerts** pane, click **Add**.

4) Complete the following fields:

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alert Type | Type of alert<br>***EMAIL** - Send an email alert to a specific user/group<br>***MSG** - Send a system message (message that appears when a user logs into the system)<br>***CMD** - Execute a command<br>***SYSLOG** - Send a notification to the system archive<br>***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>***TGCENTRAL** - Send a notification to TGCentral |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Number of Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter ***ALL** to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Event Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Event Frequency Measurement | Unit of measurement |

5) Click **Save**.

## Edit Command Monitor Alerts

Use this task to edit a command monitor alert.

**To edit a Command Monitor alert**

1) Access the **Command Monitor Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired alert.

4) Select **Edit**.

5) Modify the parameters as necessary.

6) Click **Save**.

## Delete Command Monitor Alerts

Use this task to delete a command monitor alert.

**To delete a Command Monitor alert**

1) Access the **Command Monitor Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired alert.

4) Select **Delete**.

**See also**

Working with Detect Monitors

# History Log Monitor

This section describes how to work with History Log rules.

This section includes the following topics:

- Display History Log Rules
- Manage History Log Rules

**See also**

Detect Monitor

# Display History Log Rules

This section describes how to display **History Log** rules.

Use this task to do the following:

- Display List of History Log Rules
- Display List of History Log Rule Criteria
- Display List of History Log Rule Activities
- Display List of History Log Rule Alerts
- Refresh List of History Log Interface

## Display List of History Log Rules

Use this task to view the list of history log rules.

### To display the List of History Log Rules

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **History Log Rules**. The **History Log Rules** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Rule ID | Unique Identifier assigned to command rule |
| Rule Name | Name assigned to the rule |
| Calendar | Name of the calendar that defines when the rule is applicable |

| | |
|---|---|
| Daily Count | Number of daily alerts triggered by rule<br>**Note**: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered. |
| Monthly Count | Number of monthly alerts triggered by rule |
| Yearly Count | Number of yearly alerts triggered by rule |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of History Log Rule Criteria

Use this task to view the list of history log rule criteria.

**To display the List of History Log Rule Criteria.**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **History Log Rules**. The **History Log Rules** interface is displayed in the right pane.

4) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | The server to which the rule applies |
| Rule ID | Unique ID assigned to the rule for which you are displaying criteria |

| | |
|---|---|
| Message File | File in which the message rule resides |
| Message Library | Library in which the message rule resides |
| Description | Description of rule |
| Omit Select | Identifies whether the rule criteria is used for selecting or omitting:<br>**S (Select)** - Rule criteria used to identify messages to include (trigger alerts)<br>**O (Omit)** - Rule criteria used to identify messages to exclude (should not trigger alerts) |
| Field Compare? | Identifies any field value filters |
| Reply | Reply sent to the recipient |
| Action | Click on the **Action** button to see the list of tasks you can perform |

# Display List of History Log Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

**To display the History Log activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **History Log Rules**. The **History Log Rules** interface is displayed in the right pane.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

# Display List of History Log Rule Alerts

Use this task to view the list of history monitor alerts.

**To display the list of History Log alerts**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **History Log Rules**. The **History Log Rules** interface is displayed in the right pane.

4) Select the desired server. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Alert Type | Type of alert<br>*__EMAIL__ - Send an email alert to a specific user/group<br>*__MSG__ - Send a system message (message that appears when a user logs into the system)<br>*__CMD__ - Execute a command<br>*__SYSLOG__ - Send a notification to the system archive<br>*__EMAILDIST__ - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>*__TGCENTRAL__ - Send a notification to TGCentral |
| Alert Details | Recipient details |
| Msg to Send | Text included in the notification sent to the designated recipient |
| #Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter *__ALL__ to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Action | Click on the **Action** button to see the list of tasks you can perform |

## Refresh List of History Log Interface

Use this task at any time to refresh the **History Log 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**

1) Access the **History Log Rules** interface.

2) Click the **Refresh** button.

**See also**

Working with Detect Monitors

# Manage History Log Rules

Use this task to do the following:

- Access the History Log Rules Interface
- Add History Log Rule
- Edit History Log Rule
- Delete History Log Rule
- Add History Log Rule Criteria
- Edit History Log Rule Criteria
- Delete History Log Rule Criteria
- Add History Log Alerts
- Edit History Log Alerts
- Delete History Log Alerts

> **Note**: To work with the command monitor rules, you must access the **History Log Rules** interface.

## Access the History Log Rules Interface

Use this task to access the **History Log Rules** interface.

#### To access the History Log Rules interface

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Detect Monitors** menu.
3) Select **History Log Rules**. The **History Log Rules** interface is displayed in the right pane.

## Add History Log Rule

Use this task to add a history log rule.

#### To add a History Log rule

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

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Rule ID | Enter a unique identifier for the command rule |
| Rule Name | Enter a name for the command rule |

| | |
|---|---|
| Calendar | Enter the name of the calendar that defines when the rule is applicable<br><br>**Tip**: Enter ***NONE** if no calendar is applicable. |

4) Click **Save**.

# Edit History Log Rule

Use this task to edit a history log rule.

**To edit a History Log rule**

1) Access the **History Log Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Edit**.

4) Modify the parameters as necessary.

5) Click **Save**.

# Delete History Log Rule

Use this task to delete a history log rule.

**To delete a History Log rule**

1) Access the **History Log Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Delete**.

# Add History Log Rule Criteria

Use this task to add a history log criterion.

**To add a History Log rule criterion**

1) Access the **History Log Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) In the **Rule Criteria** pane, click **Add**.

4) Complete the following fields:

| Field | Description |
|---|---|
| Server | The server to which the rule applies |
| Message ID | Unique ID assigned to the rule for which you are displaying criteria |

| | |
|---|---|
| Message File | File in which the message rule resides |
| Message File Library | Library in which the message rule resides |
| Message Omit or Select | Identifies whether the rule criteria is used for selecting or omitting:<br>**S (Select)** - Rule criteria used to identify messages to include (trigger alerts)<br>**O (Omit)** - Rule criteria used to identify messages to exclude (should not trigger alerts) |
| Reply | Reply sent to the recipient |

5) Click **Save**.

## Edit History Log Rule Criteria

Use this task to edit a history log rule criterion.

#### To edit a History Log rule criterion

1) Access the **History Log Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired rule criterion.

4) Select **Edit**.

5) Modify the parameters as necessary.

6) Click **Save**.

## Delete History Log Rule Criteria

Use this task to delete a history log rule criterion.

#### To delete a History Log rule criterion

1) Access the **History Log Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired criterion.

4) Select **Delete**.

## Add History Log Alerts

Use this task to add a history log alert.

#### To add a History Log alert

1) Access the **History Log Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) In the **Alerts** pane, click **Add**.

4)

Complete the following fields:

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alert Type | Type of alert<br>*__EMAIL__ - Send an email alert to a specific user/group<br>*__MSG__ - Send a system message (message that appears when a user logs into the system)<br>*__CMD__ - Execute a command<br>*__SYSLOG__ - Send a notification to the system archive<br>*__EMAILDIST__ - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>*__TGCENTRAL__ - Send a notification to TGCentral |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Number of Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter *__ALL__ to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Event Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Event Frequency Measurement | Unit of measurement |

5) Click **Save**.

# Edit History Log Alerts

Use this task to edit a history log alert.

**To edit a History Log alert**

1) Access the **History Log Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

4) Click the **Action** button beside the desired alert.

5) Select **Edit**.

6) Modify the parameters as necessary.

7) Click **Save**.

# Delete History Log Alerts

Use this task to delete a history log alert.

### To delete a History Log alert

1) Access the **History Log Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired alert.

4) Select **Delete**.

### See also

Working with Detect Monitors

# Journal Monitor

This section describes how to work with Journal Monitor rules.

This section includes the following topics:

- Display Journal Monitor Rules
- Manage Journal Monitor Rules

**See also**

Detect Monitor

# Display Journal Monitor Rules

This section describes how to display the **Journal Monitor** rules.

Use this task to do the following:

- Display List of Journal Monitor Rules
- Display List of Journal Monitor Field Filters
- Display List of Journal Monitor Rule Alerts
- Refresh List of Journal Monitor Interface

## Display List of Journal Monitor Rules

Use this task to view the list of journal monitor rules.

**To display the List of Journal Monitor Log Rules**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Journal Monitor Rules**. The **Journal Monitor Rules** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alert | Identifies whether an alert is sent:<br>**Y** - Send an alert<br>**N** - Do not send an alert |
| Code | Identifies the type of audit trail journal<br>The following journal types are currently supported:<br>**T** - Security journal<br>**U** - User-defined journal |
| Type | Identifies the type of journal entry<br><br>**Note**: Refer to the IBM Knowledge Center for a complete list of journal entry types and descriptions. |
| Calendar | Name of the calendar that defines when the rule is applicable |

| | |
|---|---|
| Description | Description of journal entry |
| Field Filter | **Note**: Field-level filters all you to apply additional granularity to your monitor rules.<br><br>**Y** - Field-level filter exists<br>**N** - No field-level filter exists |
| Daily Count | Number of daily alerts triggered by rule<br>**Note**: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered. |
| Monthly Count | Number of monthly alerts triggered by rule |
| Yearly Count | Number of yearly alerts triggered by rule |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

# Display List of Journal Monitor Field Filters

Use this task to view the list of journal monitor field filters.

**To display the List of Journal Monitor field filters**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Journal Monitor Rules**. The **Journal Monitor Rules** interface is displayed in the right pane.

4) Select the desired rule. The criteria associated with the selected rule are displayed in the **Field Filters** pane (at the bottom of the screen).

# Display List of Journal Monitor Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

**To display the Journal Monitor activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Journal Monitor Rules**. The **Journal Monitor Rules** interface is displayed in the right pane.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Display List of Journal Monitor Rule Alerts

Use this task to view the list of journal monitor alerts.

**To display the list of Journal Monitor alerts**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Journal Monitor Rules**. The **Journal Monitor Rules** interface is displayed in the right pane.

4) Select the desired server. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |

| | |
|---|---|
| Alert Type | Type of alert<br>*__EMAIL__ - Send an email alert to a specific user/group<br>*__MSG__ - Send a system message (message that appears when a user logs into the system)<br>*__CMD__ - Execute a command<br>*__SYSLOG__ - Send a notification to the system archive<br>*__EMAILDIST__ - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>*__TGCENTRAL__ - Send a notification to TGCentral |
| Alert Details | Recipient details |
| Msg to Send | Text included in the notification sent to the designated recipient |
| #Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter *__ALL__ to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Action | Click on the **Action** button to see the list of tasks you can perform |

## Refresh List of Journal Monitor Interface

Use this task at any time to refresh the **Journal Monitor 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**

1) Access the **Journal Monitor Rules** interface.

2) Click the **Refresh** button.

**See also**

Working with Detect Monitors

# Manage Journal Monitor Rules

Use this task to do the following:

- Access the Journal Monitor Rules Interface
- Add Journal Monitor Filter Criteria
- Edit Journal Monitor Filter Criteria
- Delete Journal Monitor Filter Criteria
- Add Journal Monitor Alerts
- Edit Journal Monitor Alerts
- Delete Journal Monitor Alerts

**Note**: To work with the command monitor rules, you must access the **Journal Monitor Rules** interface.

## Access the Journal Monitor Rules Interface

Use this task to access the **Journal Monitor Rules** interface.

#### To access the Journal Monitor Rules interface

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Journal Monitor Rules**. The **Journal Monitor Rules** interface.

## Add Journal Monitor Filter Criteria

Use this task to add a journal monitor filter criterion.

#### To add a Journal Monitor filter criterion

1) Access the **Journal Monitor Rules** interface.

2) Select the desired rule. The filter criteria associated with the selected rule are displayed in the **Filter** pane (at the bottom of the screen).

3) In the **Filter** pane, click **Add**.

4) Complete the following fields:

| Field | Description |
|---|---|
| Server | The server to which the rule applies |
| Rule ID | Unique ID assigned to the rule for which you are displaying criteria |
| Rule Name | Name assigned to the rule for which you are displaying criteria |
| Command Name | Command for which you want to establish a rule |

| | |
|---|---|
| Library | Library in which you want to monitor using the rule |
| User Name | User/user group you want to monitor using the rule<br>**Tip**: Enter ***ALL** to monitor all users. |
| Rule Description | Description of the criteria |
| Action | Click on the **Action** button to see the list of tasks you can perform |

5) Click **Save**.

## Edit Journal Monitor Filter Criteria

Use this task to edit a journal monitor filter criterion.

#### To edit a Journal Monitor filter criterion

1) Access the **Journal Monitor Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Filter** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired filter criterion.

4) Select **Edit**.

5) Modify the parameters as necessary.

6) Click **Save**.

## Delete Journal Monitor Filter Criteria

Use this task to delete a journal monitor filter criterion.

#### To delete a Journal Monitor filter criterion

1) Access the **Journal Monitor Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Filter** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired criterion.

4) Select **Delete**.

## Add Journal Monitor Alerts

Use this task to add a journal monitor alert.

#### To add a Journal Monitor alert

1) Access the **Journal Monitor Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) In the **Alerts** pane, click **Add**.

4)

Complete the following fields:

| Field | Description |
|---|---|
| **Field** | **Description** |
| Server | Server to which the rule applies |
| Alert Type | Type of alert<br>***EMAIL** - Send an email alert to a specific user/group<br>***MSG** - Send a system message (message that appears when a user logs into the system)<br>***CMD** - Execute a command<br>***SYSLOG** - Send a notification to the system archive<br>***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>***TGCENTRAL** - Send a notification to TGCentral |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Number of Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter ***ALL** to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Event Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Event Frequency Measurement | Unit of measurement |

5) Click **Save**.

# Edit Journal Monitor Alerts

Use this task to edit a journal monitor alert.

**To edit a Journal Monitor alert**

1) Access the **Journal Monitor Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired alert.

4) Select **Edit**.

5) Modify the parameters as necessary.

6) Click **Save**.

## Delete Journal Monitor Alerts

Use this task to delete a Journal monitor alert.

### To delete a Journal Monitor alert

1) Access the **Journal Monitor Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired alert.

4) Select **Delete**.

### See also

Working with Detect Monitors

# Message Queue Monitor

This section describes how to work with Message Queue rules.

This section includes the following topics:

- Display Message Queue Rules
- Manage Message Queue Rules

**See also**

Detect Monitor

# Display Message Queue Rules

This section describes how to display the **Message Queue** rules.

Use this task to do the following:

- Display List of Message Queue Rules
- Display List of Message Queue Rule Criteria
- Display List of Message Queue Rule Activities
- Display List of Message Queue Rule Alerts
- Refresh List of Message Queue Interface

## Display List of Message Queue Rules

Use this task to view the list of message queue rules.

#### To display the List of Message Queue Rules

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Message Queue Rules**. The **Message Queue Rules** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| MonitorName | Name assigned to the message queue (there can be multiple) |
| RuleID | Unique Identifier assigned to command rule |
| RuleName | Name assigned to the rule |

| | |
|---|---|
| Calendar | Name of the calendar that defines when the rule is applicable |
| Daily Count | Number of daily alerts triggered by rule<br>**Note**: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered. |
| Monthly Count | Number of monthly alerts triggered by rule |
| Yearly Count | Number of yearly alerts triggered by rule |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Message Queue Rule Criteria

Use this task to display the list of message queue rule criteria.

**To display the List of Message Queue Rule Criteria.**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Message Queue Rules**. The **Message Queue Rules** interface is displayed in the right pane.

4) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | The server to which the rule applies |
| Rule ID | Unique ID assigned to the rule for which you are displaying criteria |
| Message File | File in which the message rule resides |
| Message Library | Library in which the message rule resides |
| Description | Description of the criteria |
| Omit Select | Identifies whether the rule criteria is used for selecting or omitting:<br>**S (Select)** - Rule criteria used to identify messages to include (trigger alerts)<br>**O (Omit)** - Rule criteria used to identify messages to exclude (should not trigger alerts) |
| Field Compare? | Identifies any field value filters |
| Reply | Reply sent to the recipient |
| Action | Click on the **Action** button to see the list of tasks you can perform |

# Display List of Message Queue Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

**To display the Message Queue activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Message Queue Rules**. The **Message Queue Rules** interface is displayed in the right pane.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

# Display List of Message Queue Rule Alerts

Use this task to view the list of message queue alerts.

**To display the list of message queue alerts**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Message Queue Rules**. The **Message Queue Rules** interface is displayed in the right pane.

4) Select the desired server. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Alert Type | Type of alert<br>*__EMAIL__ - Send an email alert to a specific user/group<br>*__MSG__ - Send a system message (message that appears when a user logs into the system)<br>*__CMD__ - Execute a command<br>*__SYSLOG__ - Send a notification to the system archive<br>*__EMAILDIST__ - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>*__TGCENTRAL__ - Send a notification to TGCentral |
| Alert Details | Recipient details |
| Msg to Send | Text included in the notification sent to the designated recipient |
| #Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter *__ALL__ to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Action | Click on the **Action** button to see the list of tasks you can perform |

## Refresh List of Message Queue Interface

Use this task at any time to refresh the **Message Queue 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**

1) Access the **Message Queue Rules** interface.

2) Click the **Refresh** button.

**See also**

Working with Detect Monitors

# Manage Message Queue Rules

Use this task to do the following:

- Access the Message Queue Rules Interface
- Add Message Queue Rule
- Edit Message Queue Rule
- Delete Message Queue Rule
- Add Message Queue Rule Criteria
- Edit Message Queue Rule Criteria
- Delete Message Queue Rule Criteria
- Add Message Queue Alerts
- Edit Message Queue Alerts
- Delete Message Queue Alerts

**Note**: To work with the command monitor rules, you must access the **Message Queue Rules** interface.

## Access the Message Queue Rules Interface

Use this task to access the **Message Queue Rules** interface.

#### To access the Message Queue Rules interface

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Detect Monitors** menu.
3) Select **Message Queue Rules**. The **Message Queue Rules** interface.

## Add Message Queue Rule

Use this task to add a message queue rule.

#### To add a Message Queue rule

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

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Monitor Name | Name you want to assign the monitor |
| Monitor Library | Library location |

| | |
|---|---|
| Rule ID | Unique ID that identifies the rule |
| Rule Name | Name you want to assign the rule |
| Calendar | Name of the calendar that defines when the rule is applicable<br><br>**Tip**: Enter ***NONE** if no calendar is applicable. |

4) Click **Save**.

## Edit Message Queue Rule

Use this task to edit a message queue rule.

#### To edit a Message Queue rule

1) Access the **Message Queue Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Edit**.

4) Modify the parameters as necessary.

5) Click **Save**.

## Delete Message Queue Rule

Use this task to delete a message queue rule.

#### To delete a Message Queue rule

1) Access the **Message Queue Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Delete**.

## Add Message Queue Rule Criteria

Use this task to add a message queue rule criterion.

#### To add a Message Queue rule criterion

1) Access the **Message Queue Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) In the **Rule Criteria** pane, click **Add**.

4) Complete the following fields:

| Field | Description |
|---|---|

| | |
|---|---|
| Server | The server to which the rule applies |
| Message ID | Unique ID assigned to the rule criteria |
| Message File | File in which the message rule resides |
| Message File Library | Library in which the message rule resides |
| Message Omit or Select | Identifies whether the rule criteria is used for selecting or omitting:<br>**S (Select)** - Rule criteria used to identify messages to include (trigger alerts)<br>**O (Omit)** - Rule criteria used to identify messages to exclude (should not trigger alerts) |
| Reply | Reply sent to the recipient |

5) Click **Save**.

## Edit Message Queue Rule Criteria

Use this task to edit a message queue rule criterion.

#### To edit a Message Queue rule criterion

1) Access the **Message Queue Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired rule criterion.

4) Select **Edit**.

5) Modify the parameters as necessary.

6) Click **Save**.

## Delete Message Queue Rule Criteria

Use this task to delete a message queue rule criterion.

#### To delete a Message Queue rule criterion

1) Access the **Message Queue Rules** interface.

2) Select the desired rule. The criteria associated with the selected rule are displayed in the **Rule Criteria** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired criterion.

4) Select **Delete**.

## Add Message Queue Alerts

Use this task to add a message queue alert.

#### To add a Message Queue alert

1) Access the **Message Queue Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) In the **Alerts** pane, click **Add**.

4)

Complete the following fields:

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alert Type | Type of alert<br>***EMAIL** - Send an email alert to a specific user/group<br>***MSG** - Send a system message (message that appears when a user logs into the system)<br>***CMD** - Execute a command<br>***SYSLOG** - Send a notification to the system archive<br>***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts)<br>***TGCENTRAL** - Send a notification to TGCentral |
| Alt Sequence | The sequence in which alerts are sent<br>**Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence. |
| Number of Events | Number of alert events required to trigger a notification<br>**Alternatively**, enter ***ALL** to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the **Freq** field. |
| Event Frequency | Frequency of alert events required to trigger a notification<br>This field works in conjunction with the **#Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. |
| Event Frequency Measurement | Unit of measurement |

5) Click **Save**.

# Edit Message Queue Alerts

Use this task to edit a message queue alert.

#### To edit a Message Queue alert

1) Access the **Message Queue Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

4) Click the **Action** button beside the desired alert.

5) Select **Edit**.

6) Modify the parameters as necessary.

7) Click **Save**.

## Delete Message Queue Alerts

Use this task to delete a message queue alert.

### To delete a Message Queue alert

1) Access the **Message Queue Rules** interface.

2) Select the desired rule. The alerts associated with the selected rule are displayed in the **Alerts** pane (at the bottom of the screen).

3) Click the **Action** button beside the desired alert.

4) Select **Delete**.

### See also

Working with Detect Monitors

# SIEM Monitor

This section describes how to work with SIEM Monitor rules.

This section includes the following topics:

- Display SIEM Monitor Rules
- Manage SIEM Monitor Rules

**See also**

Detect Monitor

# Display SIEM Monitor Rules

This section describes how to display the **SIEM Monitor** rules.

Use this task to do the following:

- Display List of SIEM Monitor Rules
- Display SIEM Monitor Rule Activities
- Refresh List of SIEM Monitor Rules

## Display List of SIEM Monitor Rules

Use this task to view the list of Message Queue rules.

**To display the list of SIEM Monitor rules**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **SIEM Monitor Rules**. The **SIEM Monitor Rules** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Alert | Identifies whether an alert is sent:<br>**Y** - Send an alert **N** - Do not send an alert<br>**Note**: To see the SIEM log format in which the system sends alerts, refer to TGDetect Defaults |
| Code | Identifies the type of audit trail journal<br>The following journal types are currently supported:<br>**T** - Security journal<br>**U** - User-defined journal |
| Type | Identifies the type of journal entry **Note**: Refer to the IBM Knowledge Center for a complete list of journal entry types and descriptions. |
| Description | Description of journal entry |

| | |
|---|---|
| Field Filter | Identifies whether a field-level filter exists **Note**: Field-level filters all you to apply additional granularity to your monitor rules.<br>**Y** - Field-level filter exists<br>**N** - No field-level filter exists |
| Field Select | Identifies whether the data from all fields or a subset of fields is sent<br>**Note**: Not all the data (fields) in a journal entry are relevant for security monitoring purposes; therefore, it might be helpful to limit which fields are sent.<br>**Y** - Send all fields<br>**N** - Send a subset of fields |
| Daily Count | Number of daily alerts triggered by rule<br>**Note**: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered. |
| Monthly Count | Number of monthly alerts triggered by rule |
| Yearly Count | Number of yearly alerts triggered by rule |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display SIEM Monitor Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

**To display the SIEM Monitor activity**

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **SIEM Monitor Rules**. The **SIEM Monitor Rules** interface is displayed in the right pane.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of SIEM Monitor Rules

Use this task at any time to refresh the **SIEM Monitor 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

1) Access the **SIEM Monitor Rules** interface.

2) Click the **Refresh** button.

### See also

Working with Detect Monitors

# Manage SIEM Monitor Rules

Use this task to do the following:

- Access the SEIM Monitor Rules Interface
- Add SIEM Monitor Rule
- Edit SIEM Monitor Rule
- Delete SIEM Monitor Rule

> **Note**: To work with the command monitor rules, you must access the **SEIM Monitor Rules** interface.

## Access the SEIM Monitor Rules Interface

Use this task to access the **SEIM Monitor Rules** interface.

#### To access the SEI Monitor Rules interface

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Detect Monitors** menu.
3) Select **SIEM Monitor Rules**. The **SEIM Monitor Rules** interface is displayed in the right pane.

## Add SIEM Monitor Rule

Use this task to add a SIEM monitor rule.

#### To add a SIEM monitor rule

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

| Field | Description |
|---|---|
| Rule ID | Enter a unique identifier for the command rule |
| Rule Name | Enter a name for the command rule |
| Calendar | Enter the name of the calendar that defines when the rule is applicable<br><br>**Tip**: Enter ***NONE** if no calendar is applicable. |

4) Click **Save**.

## Edit SIEM Monitor Rule

Use this task to edit a SIEM monitor rule.

#### To edit SIEM monitor rule

1) Access the **SIEM Monitor Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Edit**.

4) Modify the parameters as necessary.

5) Click **Save**.

## Delete SIEM Monitor Rule

Use this task to delete a SIEM monitor rule.

### To delete a SIEM monitor rule

1) Access the **Journal Monitor Rules** interface.

2) Click the **Action** button beside the desired rule.

3) Select **Delete**.

### See also

Working with Detect Monitors

# Syslog Monitor

This section describes how to work with Syslog Monitor rules.

This section includes the following topics:

- Display Syslog Monitor Rules
- Manage Syslog Monitor Rules

**See also**

Detect Monitor

# Display Syslog Monitor Rules

This section describes how to display the **Syslog Monitor** rules.

Use this task to do the following:

- Display List of Syslog Monitor Rules
- Display List of Syslog Monitor Rule Activities
- Refresh List of Syslog Monitor Interface

## Display List of Syslog Monitor Rules

Use this task to view the list of syslog monitor rules.

#### To display the List of Syslog Monitor Rules

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Syslog Monitor Rules**. The **Syslog Monitor Rules** interface is displayed in the right pane.

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Syslog Provider Name | Name of the syslog provider |
| Syslog Provider Description | Description of the syslog provider |
| IP Address Protocol | IP address to the syslog server |
| Action | Click on the **Action** button to see the list of tasks you can perform |

**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.

## Display List of Syslog Monitor Rule Activities

Use this task to view the activity (additions, deletions, modifications) associated with the monitor.

#### To display the Syslog Monitor activity

1) Expand the **Rules** menu (in the left pane).

2) Expand the **Detect Monitors** menu.

3) Select **Syslog Monitor Rules**. The **Syslog Monitor  Rules** interface is displayed in the right pane.

4) Select the desired rule. The activities associated with the selected rule are displayed in the **Activity** pane (at the bottom of the screen).

| Field | Description |
|---|---|
| Server | Name of server to which the default applies |
| Description | Description of the activity |
| Date | Date on which the activity was performed |
| Status | Status of the activity |

## Refresh List of Syslog Monitor Interface

Use this task at any time to refresh the **Syslog Monitor 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

1) Access the **Syslog Monitor Rules** interface.

2) Click the **Refresh** button.

### See also

Working with Detect Monitors

# Manage Syslog Monitor Rules

Use this task to do the following:

- Access the SEIM Monitor Rules Interface
- Add Syslog Monitor Rule
- Edit Syslog Monitor Rule
- Delete Syslog Monitor Rule

**Note**: To work with the command monitor rules, you must access the **SEIM Monitor Rules** interface.

## Access the SEIM Monitor Rules Interface

Use this task to access the **SEIM Monitor Rules** interface.

#### To access the SEI Monitor Rules interface

1) Expand the **Rules** menu (in the left pane).
2) Expand the **Detect Monitors** menu.
3) Select **Syslog Monitor Rules**. The **Syslog Monitor Rules** interface is displayed in the right pane.

## Add Syslog Monitor Rule

Use this task to add a syslog monitor rule.

#### To add a syslog monitor rule

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

| Field | Description |
|---|---|
| Server | Server to which the rule applies |
| Syslog Provider Name | |
| Syslog Provider Description | |
| Syslog IP Address | |
| Syslog Port | |
| Syslog Protocol | |
| Message Log Format | |
| Syslog Facility | |

| | |
|---|---|
| Syslog Severity | |

4) Click **Save**.

## Edit Syslog Monitor Rule

Use this task to edit a syslog monitor rule.

### To edit a Syslog Monitor rule

1) Access the **Message Queue Rules** interface.
2) Click the **Action** button beside the desired rule.
3) Select **Edit**.
4) Modify the parameters as necessary.
5) Click **Save**.

## Delete Syslog Monitor Rule

Use this task to delete a syslog monitor rule.

### To delete a Syslog Monitor  rule

1) Access the **Syslog Monitor Rules** interface.
2) Click the **Action** button beside the desired rule.
3) Select **Delete**.

### See also

Working with Detect Monitors

# Groups

This section describes how to work with **Calendars**.

This section includes the following topics:

- Group Management
- Working with Groups
- Manage User Groups
- Manage Network Server Groups
- Manage Operation Groups
- Manage Object Groups

**See also**

TGCentral Introduction

# Group Management

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.

This section includes the following topics:

- Working with Groups
- Manage User Groups
- Manage Network/Server Groups
- Manage Operation Groups
- Manage Object Groups

**See also**

User Permissions

# 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

**See also**

Group Management

# Manage User Groups

This section describes how to work 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 List of User Groups
- Refresh List of User Groups
- Import User Group
- Export User Group
- Edit User Group
- Add User Group
- Delete User Group

## 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**. 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<br>**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.

## 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.

## 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**. 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.

## 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.

## 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**.

## 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**.

## 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 the group you want to delete.

3) Select **Delete**.

### See also

Working with Groups

# Manage Network Server Groups

This section describes how to work 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

## 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**. 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<br>**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.

## 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.

## 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**.

## 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**.

## 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**.

# Manage Operation Groups

This section describes how to work 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

## 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<br>**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.

## 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.

## 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**.

## 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**.

## 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 the group you want to delete.
3) Select **Delete**.

### See also

Working with Groups

# Manage Object Groups

This section describes how to work 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

## 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**. 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<br>**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.

## 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.

## 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**.

## 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**.

## 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 the group you want to delete.
3) Select **Delete**.

**See also**

Working with Groups

# Calendars

This section describes how to work with **Calendars**.

This section includes the following topic:

- Calendar Management
- Working with Calendars
- Manage Calendars

**See also**

TGCentral Introduction

# Calendar Management

This section describes how to work with **Calendars**. Use calendars to do the following:

- Working with Calendars
- Manage Calendars

# Working with Calendars

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

- Manage Calendars

# Manage Calendars

This section describes managing **Calendars**.

Use this task to do the following:

- Display List of Calendars
- Refresh List of Calendars
- Edit Calendar
- Add Calendar
- Delete Calendar

## 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**. 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.

## 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.

## 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**.

## 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**.

## Delete Calendar

Use this task to delete a calendar.

**To delete a calendar**

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

**See also**

Calendar Management

Working with Calendars

# Reports

This section describes how to work with **Reports**:

This section includes the following topics:

- Report Management
- Working with Reports and Report Cards
- Display TGCentral Reports
- Display List of TGCentral Report Cards
- Manage Reports
- Manage Report Cards
- Run Report
- Run Report Card

> **Note**: For a description of the individual reports, refer to the appropriate report reference guide:
>
> - TGAudit Report Reference
> - TGSecure Report Reference
> - TGDetect Report Reference
> - TGAudit for Linux Report Reference

**See also**

TGCentral Introduction

# Report Management

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.

This section includes the following topics:

- Working with Reports and Report Cards
- Manage Reports
- Manage Report Cards

**Note**: For a description of the individual reports, refer to the appropriate report reference guide:

- TGAudit Report Reference
- TGSecure Report Reference
- TGDetect Report Reference
- TGAudit for Linux Report Reference

**See also**

User Permissions

# Working with Reports and Report Cards

Use the **Report Management** feature to do the following:

### Reports

- Display TGCentral Reports
- Manage Reports
- Run Report

### Report Cards

- Display List of TGCentral Report Cards
- Manage Report Cards
- Run Report Card

> **Note**: For a description of the individual reports, refer to the appropriate report reference guide:
>
> - TGAudit Report Reference
> - TGSecure Report Reference
> - TGDetect Report Reference
> - TGAudit for Linux Report Reference

### See also

Reports

# Display TGCentral Reports

Use this task to do the following:

- Display List of Reports
- Refresh List of Reports
- Display Report Run Activity

> **Note**: For a description of the individual reports, refer to the appropriate report reference guide:
>
> - TGAudit Report Reference
> - TGSecure Report Reference
> - TGDetect Report Reference
> - TGAudit for Linux Report Reference

## 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**. 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)<br>**N** (No): Custom report (specific to the client) |
| Platform | Identifies the platform:<br>– IBM i indicates an IBM i series server<br>– 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.

## 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.

## Display Report Run Activity

Use this task after you run a report to display the report results.

**To display the report run activity**

1) Expand the **Activity** menu in the left pane.

2) Click the **Report Activity** tab. The list of run reports is displayed.

3) Click the **Action** button associated with the desired report and select **View Report**.

> **Note**: For a description of the individual reports, refer to the appropriate report reference guide:
>
> - TGAudit Report Reference
> - TGSecure Report Reference
> - TGDetect Report Reference
> - TGAudit for Linux Report Reference

**See also**

Working with Reports and Report Cards

# Display List of TGCentral Report Cards

Use this task to do the following:

- Display List of Report Cards
- Refresh List of Report Cards
- View Report Card Details
- Display Report Card Run Activity

## 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**. 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<br>**N** (No): Custom report card<br>**Note**: An **N** (No) appears in this column for all report cards you create |
| Platform | Identifies the platform:<br>– IBM i indicates an IBM i series server<br>– 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.

## 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.

## 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**.

## Display Report Card Run Activity

Use this task after you run a report card to display the report card results.

**To display the report card run activity**

1) Expand the **Activity** menu in the left pane.
2) Click the **Report Activity** tab. The list of run reports is displayed.
3) Click the **Action** button associated with the desired report card and select **View Report Card**.

> **Note**: For a description of the individual reports, refer to the appropriate report reference guide:
>
> - TGAudit Report Reference
> - TGSecure Report Reference
> - TGDetect Report Reference
> - TGAudit for Linux Report Reference

**See also**

Working with Reports and Report Cards

# Manage Reports

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

Use this task to do the following:

- Add Report
- Copy Report
- Edit Report
- Delete Report
- Schedule Report
- Schedule Report Email Notification

> **Note**: For a description of the individual reports, refer to the appropriate report reference guide:
>
> - TGAudit Report Reference
> - TGSecure Report Reference
> - TGDetect Report Reference

## 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 |
|---|---|
| Platform | Select one of the following:<br>**IBM i** - Use data from an IBM i agent (server)<br>**Linux** - Use data from a Linux agent (server) |
| Collector | Journal collector (IBM i) or table (Linux) from which report data is pulled |
| Report ID | ID assigned to the report<br>**Tip:** 30-characters max, must start with a letter, no spaces or special characters allowed |
| Report Name | A 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. 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. |

10) Click **Save**.

## 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**.

## 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.

## 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 a custom or a 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**.

## 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<br>**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<br>**Ad-hoc** - Once on a specific day and time<br>**Daily** - Once a day<br>**Weekly** - Once a week<br>**Monthly** - Once a month<br>**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.

## 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 or generate reports at any time.

**To schedule an email**

1) Access the **Reports** interface.

2) Click the **Action** button for the desired report.

3) Select **Email Report**. 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.<br>You have the following options:<br>**User**: Click the dropdown arrow beside a user group (role) to send an email to specific users<br>**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:<br>**Expression**: Select a comparison operator (e.g., =, <=, >=)<br>**Number**: Enter the number of report rows<br>**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.<br>You have the following options:<br>**User**: Click the dropdown arrow beside a user group (role) to send an email to specific users<br>**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 also**

Report Management

Manage Report Activities

Manage Settings

# Manage Report Cards

Use this task to do the following:

- Add a Report Card
- Copy Report Card
- Edit Report Card
- Delete Report Card
- Schedule Report Card
- Schedule Report Card Email Notification
- Add Exceptions to Report Card

## 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)<br>**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. 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**.

## 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**.

## 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.

## 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 a 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**.

## 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**. The **Schedule Report** dialog is displayed.
4) Complete the following fields:

| Field | Description |
|---|---|
| Server | Server on which you want to run the report<br>**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<br>**Ad-hoc** - Once on a specific day and time<br>**Daily** - Once a day<br>**Weekly** - Once a week<br>**Monthly** - Once a month<br>**Yearly** - Once a year |
| Time | Time at which to run the report card |

5) Click **Save**.

## 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.

**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**. 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.<br>You have the following options:<br>**User**: Click the dropdown arrow beside a user group (role) to send an email to specific users<br>**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:<br>**Expression**: Select a comparison operator (e.g., =, <=, >=)<br>**Number**: Enter the number of report rows<br>**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.<br>You have the following options:<br>**User**: Click the dropdown arrow beside a user group (role) to send an email to specific users<br>**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.

## 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 addition 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

# 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.

### See also

Working with Reports and Report Cards

# 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

Working with Reports and Report Cards

# Activity

This section describes how to work with **Activities**.

This section includes the following topics:

- Activity Management
- Working with Activities
- Manage Report Activities
- Manage Server Activities

**See also**

TGCentral Introduction

# Activity Management

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

- Working with Activities
- Manage Report Activities
- Manage Server Activities

> **Tip**: The features available to each user are dependent on the user's permissions levels, which is based on their assigned role.

**See also**

Permissions

# Working with Activities

Use the **Activity Management** feature to do the following:

- Manage Report Activities
- Manage Server Activities

### See also

Activity Management

# 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

## Display List of Report Activities

Use this task to view the list of report activities.

**To display the list of report activities**

1) Expand the **Activity** menu in the left pane.

2) Click the **Report Activity** tab. he **Report Activity** interface is displayed.

| Field | Description |
|---|---|
| User | Name of user who 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:<br>**Completed** - Successful run<br>**Processing** - In process (with percent complete)<br>**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.

## 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 the list of report activities**

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

## 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**.

> **Tip**: To change the color scheme, see Manage Settings.

## 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**.

## 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**.

## 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**. The list of reports associated with the report card are displayed.
4) Click on a report to view the details.

## 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.

**To email a report**

1) Access the **Report Activity** interface.
2) Click the **Action** button beside the desired report.
3) Select **Email Report**. 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 desired recipient. You have the following options:<br>**User**: Click the dropdown arrow beside a user group (role) to send an email to specific users<br>**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.

## 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.

**To email a report card**

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

3) Select **Email Report**. 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 desired recipient. You have the following options:<br>**User**: Click the dropdown arrow beside a user group (role) to send an email to specific users<br>**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.

## 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**.

## 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.

**To delete a report activity**

1) Access the **Report Activity** interface.

2) Click the **Action** button beside the desired report.

3) Select **Delete**.

## 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.).

**To delete a report activity**

1) Access the **Report Activity** interface.

2) Click the **Action** button beside the desired report.

3) Select **Run Again**.

## Run Delta Report

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

### To run a delta report

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

# Manage Server Activities

Use this task to do the following:

- Display List of Sever Activities
- Refresh List of Server Activities
- Search List of Server Activities

## 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. 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:<br>**JAM** - Activity involving a job activity rule<br>**Report** - Activity involving a report<br>**Report Card** - Activity involving a report card<br>**User** - Activity involving a user group |
| Status | Status of the activity:<br>**Completed** - Successful run<br>**Processing** - In process (with percent complete)<br>**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.

## 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.

# 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

# Real Time Events

This section describes how to work with **Real-Time Events**.

This section includes the following topics:

- Real Time Event Management
- Working with Real Time Event Management
- Manage Network Activity
- Manage Alerts

**See also**

TGCentral Introduction

# Real Time Event Management

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

- Working with Real Time Event Management
- 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**

Permissions

# Working with Real Time Event Management

Use **Real Time Event Management** to do the following:

- Manage Network Activity
- Manage Alerts

**See also**

Real Time Event Management

# 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 List of Network Activities
- Apply Network Activities Display Filter
- Reset Network Activity Display Filter

## 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**. 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.

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

| Field | Description |
|---|---|
| Server | Server on which the activity was performed |
| Type | Type of activity:<br>**JAM** - Activity involving a job activity rule<br>**Report** - Activity involving a report<br>**Report Card** - Activity involving a report card<br>**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.

## 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.

## 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.

## Apply Network Activities Display Filter

Use this task to limit the list of network activities displayed based on selection criteria (multiple options) you define.

**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. The individual criterion by which you are filtering the display appear as removable options above the network activity display.

> **Alternatively,** you can also apply a quick filter (single option) by clicking directly on text in the blueprint display. Again, use the **Filter** button to filter the display based on multiple options.

## Reset Network Activity Display 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

Working with Real Time Event Management

# 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 Alert Filter

## 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**. 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.

## 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**. 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:<br>*__CMD__ - Command executed<br>*__EMAIL__- Email sent<br>*__MSG__ - System (login) message queued<br>*__SYSLOG__ - Syslog communication initiated |

# 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.

# 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.

# 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.

# 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**

Working with Real Time Event Management

# Admin

This section describes how to work with the **Admin** feature.

This section includes the following topics:

- Administration Management
- Working with Administration Management
- Manage Users
- Manage Roles
- Manage Settings
- Manage Agent Configuration

**See also**

TGCentral Introduction

# 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:

- Working with Administration Management
- 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**

Permissions

# Working with Administration Management

Use the **Administrative Management** feature to do the following:

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

**See also**

Administration Management

# 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 User
- Disable User
- Enable User
- Delete User

## 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<br>**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.

## 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 |
|---|---|
| User Name | 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 | The initial password assigned to the user when access TGCentral **Note**: The user should change the password immediately. |
| Server Group Name | TGCentral group to which the user is assigned |
| Role | TGCentral role to which the user is assigned<br><br>**Tip**: A user's permissions 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:<br><br>**Yes** - Allow the user to log in from different machines concurrently<br><br>**No** - Do not allow the user to log in from different machines concurrently |

4) Click **Save**.

**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**.

## 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**.

## 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**.

## 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

Working with Administration Management

# 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
- Edit Role Permissions
- Delete Role

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

## 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 the role |
| Description | Description of role |
| Built-in | **Y** (Yes): Pre-built role delivered as part of the product<br>**N** (No): Custom role<br>**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.

## 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**.

## 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**.

## Edit Role Name

Use this task to 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**.

## 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.

> **Note**: You have the ability to limit access at a high-level or at a very granular level (i.e., server, menu, report, etc.).

5) Click **Save**.

## 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**

Permissions

Working with Administration Management

# Manage Settings

> ⚠ **Important**: Any actions 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:


- Mail Server Tab
  - Edit Mail Server Details
- PDF Settings Tab
  - Edit PDF Settings
- Themes Tab
  - Create Color Theme
  - Edit Color Theme
  - Copy Color Theme
  - Chose Color Theme
- Cleanup Reports Tab
  - Cleanup of Reports and Report Cards
- Update Tab
  - Updated Linux Reports
- License Tab
  - Display Licenses
  - Add TGAudit for Linux License
  - Update TGAudit for Linux License
- Advanced Tab
  - Display Custom SSL Certificate


## Mail Server Tab

### 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**.

**Tip**: Click the **Test Connection** button to test the mail server configuration.

# PDF Settings Tab

## 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 the list available.

5) Click **Save**.

# Themes Tab

## 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 **Themes** tab.

4) Click the **Add** button. 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 theme |

6) Select the desired tab.

> **Note**: There is a 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**.

## 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**.

## 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**. 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**.

### Chose Color Theme

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

#### To choose 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**. The **Edit User** dialog box appears.

4) Select the desired theme from the list available.

5) Click Save.

> **Note**: If modifications to your theme do not appear immediately in the user interface, consider clearing the browser cache.

## Cleanup Reports Tab

### Cleanup of Reports and Report Cards

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

> **Tip**: If you do not perform cleanup on a regular basis, your database size might impact system performance.

#### 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.

## Update Tab

### Updated Linux Reports

Use this task to updated Linux reports in a defined repository.

**To update Linux reports**

1) Expand the **Admin** menu in the left pane.
2) Click on **Settings**.
3) Click on the **Update** tab.
4) Enter the repository you want to update.
5) Click **Update** to update the Linux reports stored in the repository.

## License Tab

### Display Licenses

Use this task to display licenses.

**To display licenses**

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

| Field | Description |
|---|---|
| Product | The product for which a license is available for purchase |
| Type | Type license (e.g., enterprise)<br>**Note**: None is displayed if a valid license has not been identified |
| Total Licenses | Total number of licenses purchased |
| Used | Number of licenses currently in use |
| Available | Number of licenses available for use |
| Valid Until | The expiration date of license(s) |

### Add TGAudit for Linux License

Use this task to add a TGAudit for the Linux license.

> **Note**: The number of agents (entitlements) you can manage is defined by the license.

### To add TGAudit for Linux License

1) Expand the **Admin** menu in the left pane.

2) Click on **Settings**.

3) Click on the **License** tab.

4) Enter the license number provided to you by the TGAudit administrator or sales representative.

5) Click **Enter License** to add the TGAudit for the Linux license.

6) Click **Save**.

### Update TGAudit for Linux License

Use this task to update the TGAudit  license

#### To update TGAudit for Linux License

1) Expand the **Admin** menu in the left pane.

2) Click on **Settings**.

3) Click on the **License** tab.

4) Enter the license number provided to you by the TGAudit administrator or sales representative.

5) Click **Update License** to update the TGAudit for Linux license.

## Advanced Tab

### 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 **Advanced** 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.<br><br>**Note**: The following is the Trinity Guard certificate path: /opt/trinityguard/tgcentral/cert.pem |
| Private Key | The path to the client-specific private key. This is a text file that generates the digital signature.<br><br>**Note**: The following is the Trinity Guard private key path: /opt/trinityguard/tgcentral/key.pem |

#### See also

Permissions

Working with Administration Management

# Manage Agent Configuration

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

Use this task to do the following:

- Import Agent Configuration
- Export Agent Configuration

## Import Agent Configuration

**To import the agent configuration**

1) Expand the **Admin** menu (in the left pane).

2) Select **Import/Export Agent Config**. 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**.

## 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**. 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**

Permissions

Working with Administration Management

# Appendices


- APPENDIX - TGCentral Revisions
  - Version 2.4 - TGCentral User Guide Revisions
  - Version 2.3 - TGCentral User Guide Revisions
  - Version 2.2 - TGCentral User Guide Revisions
  - Version 2.1 - TGCentral User Guide Revisions
- APPENDIX - TGCentral Collectors
- APPENDIX - TGCentral Delta Reports
- APPENDIX - TGCentral Permissions
- APPENDIX - TGCentral FAQs

# APPENDIX - TGCentral Revisions

This section includes enhancement by version.


- Version 2.4 - TGCentral User Guide Revisions
- Version 2.3 - TGCentral User Guide Revisions
- Version 2.2 - TGCentral User Guide Revisions
- Version 2.1 - TGCentral User Guide Revisions

# Version 2.4 - TGCentral User Guide Revisions

TGCentral 2.4 contains the following:

**New Features**

- TGEncrypt Support

**Enhancements**

- TGAudit for Linux - Content Updates
- TGAudit for Linux - Licensing
- Database - Performance improvement
- User Profile Management - Archive Options *SAVSEC,*SAVPRF

# Version 2.3 - TGCentral User Guide Revisions

TGCentral 2.3 contains a Lightweight Directory Access Protocol (LDAP) support.

**New Features**

- LDAP support of centralized management of profiles (TGSecure integration)

**Enhancements**

- Additional reports (TGAudit integration)

**Bug Fixes**

- Report headers aligned with the incorrect data element when generating in excel (CSV) format
- Reports defined with multi-nested filter criteria failed to run on the IBM i Server.

# Version 2.2 - TGCentral User Guide Revisions

### Detect Monitors

The Detect Monitor features provided in TGDetect are now available in TGCentral.

### Resource Manager

The Resource Manager features provided in TGSecure are now available in TGCentral.

### User Profile Manager

The User Profile Manager features provided in TGSecure are now available in TGCentral.

### Linux Reports

The Linux reporting feature provided in TGAudit is now available in TGCentral. Use this feature to add reports for Linux agents. This enhancement includes the addition of the **platform** option, which you can use to designate whether a report is pulling data from an IBM or Linux server.

> **Note**: TGAudit for Linux supports 64-bit PowerLinux (ppc64le) as well as Linux on Intel/AMD(x86_64). Supported distributions include Red Hat, CentOS, Debian, Ubuntu, and SUSE.

In addition, you can utilize the TGCentral features listed below when managing your Linux servers:

- Pre-define regulation mapping for PCI, HIPAA, SOX, GDPR, etc.
- Role-based access control layer allowing you to grant granular permissions
- Customizable dashboard
- Exception management
- Delta reporting to compare report results
- Create custom reports and report cards using a wizard
- Notifications on critical events
- Email report and report cards

# Version 2.1 - TGCentral User Guide Revisions

This release includes the following:

### 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:

- Working with Inactive Session Lockdown
- Working with Resource Manager

# APPENDIX - TGCentral Collectors

u

| Collector ID | Collector Name | Collector Category | Platform |
|---|---|---|---|
| ACCESS_ESCAL_ACC_CONTROLS | Access Escalation Access Controls | Network | IBMi |
| ACCESS_ESCAL_DEFAULTS | Access Escalation Defaults | Network | IBMi |
| ACCESS_ESCAL_ENTITLEMENTS | Access Escalation Entitlements | Network | IBMi |
| ACCESS_ESCAL_FILE_EDITORS | Access Escalation File Editors | Network | IBMi |
| ACCESS_ESCALATION_USAGE | Access Escalation Usage | Network | IBMi |
| AUTH_USERS_VIA_AUTH_LISTS | Authorized Users through Authorization Lists | Resource | IBMi |
| AUTHORITY_COL_ALl | Authority Collection Report (*ALL) | Resources | IBMi |
| AUTHORITY_COL_IFS | Auth Collection For Objects IFS Report | Resources | IBMi |
| AUTHORITY_COL_OBJECT | Auth Collection For Objects Native Report | Resources | IBMi |
| AUTHORITY_COLLECTION | Authority Collection Data | Journal | IBMi |
| AUTHORITY_COMPLIANCE | Authority Compliance | Resource | IBMi |
| AUTHORITY_LIST | Authority List Data | System | IBMi |
| BLUEPRINT_3RD_PARTY_FILE | Blueprint 3rd Party Integration File | Profile | IBMi |
| BLUEPRINT_AUTH_SETTINGS_FILE | Blueprint Authority List Settings File | Profile | IBMi |
| BLUEPRINT_MASTER | Blueprint Master | Profile | IBMi |
| BLUEPRINT_NON_COMPLIANCE_USER | Blueprint Non-Compliance User Profiles | Profile | IBMi |
| BLUEPRINT_OBJECT_AUTH_FILE | Blueprint Object Authority File | Profile | IBMi |
| BLUEPRINT_PARAMETER_FILE | Blueprint Parameter File | Profile | IBMi |
| BLUEPRINT_PERMISSION_FILE | Blueprint Permission File | Profile | IBMi |
| CMD_SEC_COMMANDS | Commands Allowed/Rejected via Command Security | Resources | IBMi |
| CMD_SEC_CONF_SETTINGS | Command Security Config Settings | Resources | IBMi |
| CMD_SEC_PARAM_LEVEL | Command Security Paramater Level | Resources | IBMi |
| CMD_SEC_RULES | Command Security Config Settings | Resources | IBMi |

| | | | |
|---|---|---|---|
| CONTROLLER_ATTACHED_DEVICES | Command Security Paramater Level | Network | IBMi |
| CONTROLLER_DESCRIPTION_DATA | Controller Description Information | Network | IBMi |
| DATA_AREA_AUDITING | Audit data area changes | Network | IBMi |
| DATABASE ACCESS | Database File Access | N/A | IBMi |
| DATABASE_AUDITING | Monitor Database changes | Network | IBMi |
| DATABASE_CONTENT | Database Content | Configuration | IBMi |
| DATABASE_FIELD_ACTIVITY | Database Field Activity | Resources | IBMi |
| DATABASE_OPERATIONS | Database Operations | N/A | IBMi |
| DET_ACT_HISTORY | Detect Activity History | Network | IBMi |
| DET_DEFAULTS | Detect Defaults | Configuration | IBMi |
| DET_CMD_RULES | Command Monitor Rules | Configuration | IBMi |
| DET_JRN_SEIM_RULES | Journal Monitor Rules for SEIM | Configuration | IBMi |
| DET_JRNMON_ALERTS | Journal Monitor Alerts | Configuration | IBMi |
| DET_JRNMON_RULES | Journal Monitor Rules | Configuration | IBMi |
| DET_MON_MASTER | Monitor Master | Configuration | IBMi |
| DET_MSQ_CMD_ALR | Message Queue and Command Alerts | Configuration | IBMi |
| DET_MSQ_RULES | Message Queue Rules | Configuration | IBMi |
| DET_SEIM_PROVIDERS | SEIM Providers | Configuration | IBMi |
| DET_SNMP_TRP_PCKG | SNMP Trap Packages | Configuration | IBMi |
| DEVICE_DESCRIPTION_APPC | Device Description APPC Information | Network | IBMi |
| DEVICE_DESCRIPTION_DATA | Device Description Information | Network | IBMi |
| DTBASE_OPERATIONS_JRN | Database Operations by Journal | N/A | IBMi |
| ENCRYPT_DATABASE_FIELD | Encryption Database Field Details | Resource | IBMi |
| ENCRYPT_DATABASE_FILE | Encryption Database File Details | Resource | IBMi |
| ENCRYPT_DATABASE_FILTER | Encryption Database File Details | Resource | IBMi |
| ENCRYPT_DATABASE_RULES | Encryption Database Rule Details | Resource | IBMi |
| ENCRYPTION_DEFAULTS | Encryption Defaults | Resource | IBMi |
| EXIT_POINTS | Display Exit Point Data | Network | IBMi |
| FIELD_AUTHORITY | Display Field Level Authorities | Object | IBMi |
| IFS_ATTRIBUTES | Display the attributes for the IFS objects | Resource | IBMi |

| | | | |
|---|---|---|---|
| IFS_AUTHORITIES | Display the public and private authorities associated with the object | Resource | IBMi |
| IFS_CONTENT | IFS Content | Configuration | IBMi |
| IFS_JOURNALING | Display extended journaling information for the IFS object | Resource | IBMi |
| IFS_STATUS | Display status information about an IFS file | Resource | IBMi |
| INACTIVITY_DISCONNECTS | Inactivity Disconnections | Configuration | IBMi |
| INCOMING_TRANSACTIONS | Incoming Transactions | Network | IBMi |
| ISL_CONFIGURATION_SETTINGS | ISL Configuration Settings | Network | IBMi |
| ISL_DISCONNECT_OPTIONS | ISL Disconnect Options | Network | IBMi |
| ISL_RULES | ISL Inclusion Exclusion Rules | Network | IBMi |
| JOB_ACTIVITY_DETAILS | Job Activity Details | Log | IBMi |
| JOB_ACTIVITY_SUMMARY | Job Activity Summary | Log | IBMi |
| JOB_DESCRIPTIONS | Job Description Data | Configuration | IBMi |
| JOURNAL_AD | Object Auditing Attribute Changes | Configuration | IBMi |
| JOURNAL_AF | Authority Failures | Profile | IBMi |
| JOURNAL_AP | Programs that Adopt Authority were Executed | Configuration | IBMi |
| JOURNAL_AU | EIM Attribute Changes | Configuration | IBMi |
| JOURNAL_AX | Row and Column Access Control | Resource | IBMi |
| JOURNAL_CA | Authorization List or Object Authority Changes | Profile | IBMi |
| JOURNAL_CD | Commands Executed | Resource | IBMi |
| JOURNAL_CO | Create Operations | Resource | IBMi |
| JOURNAL_CP | User Profile Changes | Configuration | IBMi |
| JOURNAL_CQ | Change Request Descriptor Changes | Configuration | IBMi |
| JOURNAL_CU | Cluster Operation | Network | IBMi |
| JOURNAL_CV | Connection Verification | Profile | IBMi |
| JOURNAL_CY | Cryptographic Configuration Changes | Configuration | IBMi |
| JOURNAL_DI | LDAP Operations | Resource | IBMi |
| JOURNAL_DO | Delete Operations | Resource | IBMi |
| JOURNAL_DS | Changes to Service Tools Profiles | Profile | IBMi |
| JOURNAL_EV | Environment Variable Changes | Profile | IBMi |
| JOURNAL_GR | Exit Point Maintenance Operations | Resource | IBMi |

| | | | |
|---|---|---|---|
| JOURNAL_GS | Socket Descriptor Details | Resource | IBMi |
| JOURNAL_IM | Intrusion Monitor Events | Network | IBMi |
| JOURNAL_IP | Inter-process Communication Events | Network | IBMi |
| JOURNAL_IR | Actions to IP Rules | Network | IBMi |
| JOURNAL_IS | Internet Security Management Events | Network | IBMi |
| JOURNAL_JD | Job Descriptions – USER Parameter Changes | Resource | IBMi |
| JOURNAL_JS | Job Changes | Resource | IBMi |
| JOURNAL_KF | Key Ring File Changes | Configuration | IBMi |
| JOURNAL_LD | Directory Link, Unlink, and Search Operations | Resource | IBMi |
| JOURNAL_M0 | Db2 Mirror Setup Tools | Resource | IBMi |
| JOURNAL_M6 | Db2 Mirror Communication Services | Resource | IBMi |
| JOURNAL_M7 | Db2 Mirror Replication Services | Resource | IBMi |
| JOURNAL_M8 | Db2 Mirror Product Services | Resource | IBMi |
| JOURNAL_M9 | Db2 Mirror Replication State | Resource | IBMi |
| JOURNAL_ML | OfficeVision Mail Services Actions | Configuration | IBMi |
| JOURNAL_NA | Network Attribute Changes | Profile | IBMi |
| JOURNAL_ND | Directory Search Violations | Resource | IBMi |
| JOURNAL_NE | APPN Endpoint Filter Violations | Network | IBMi |
| JOURNAL_O1 | Single Optical Object Accesses | Resource | IBMi |
| JOURNAL_O2 | Dual Optical Object Accesses | Resource | IBMi |
| JOURNAL_O3 | Optical Volume Accesses | Resource | IBMi |
| JOURNAL_OM | Object Management Changes | Resource | IBMi |
| JOURNAL_OR | Objects Restored | Resource | IBMi |
| JOURNAL_OW | Object Ownership Changes | Resource | IBMi |
| JOURNAL_PA | Program Changes to Adopt Owner Authority | Configuration | IBMi |
| JOURNAL_PF | PTF Operations | Resource | IBMi |
| JOURNAL_PG | Primary Group Changes | Resource | IBMi |
| JOURNAL_PO | Printer Output Changes | Resource | IBMi |
| JOURNAL_PS | Swap Profile Events | Configuration | IBMi |
| JOURNAL_PU | PTF Object Changes | Profile | IBMi |
| JOURNAL_PW | Invalid Sign-on Attempts | Profile | IBMi |
| JOURNAL_RA | Authority Changes to Restored Objects | Configuration | IBMi |

| | | | |
|---|---|---|---|
| JOURNAL_RJ | Job Descriptions that Contain User Profile Names were Restored | Configuration | IBMi |
| JOURNAL_RO | Ownership Changes for Restored Objects | Profile | IBMi |
| JOURNAL_RP | Programs Restored that Adopt Owner Authority | Configuration | IBMi |
| JOURNAL_RQ | Change Request Descriptors Restored | Resource | IBMi |
| JOURNAL_RU | Authority Restored for User Profiles | Profile | IBMi |
| JOURNAL_RZ | Primary Group Changes for Restored Objects | Configuration | IBMi |
| JOURNAL_SD | System Directory Changes | Resource | IBMi |
| JOURNAL_SE | Subsystem Routing Entry Changes | Configuration | IBMi |
| JOURNAL_SF | Spooled File Actions | Resource | IBMi |
| JOURNAL_SG | Asynchronous Signals Processed | Network | IBMi |
| JOURNAL_SK | Secure Socket Connections | Network | IBMi |
| JOURNAL_SM | Systems Management Changes | Configuration | IBMi |
| JOURNAL_SO | Server Security User Information Actions | Configuration | IBMi |
| JOURNAL_ST | Service Tools Actions | Configuration | IBMi |
| JOURNAL_SV | System Values Changes | Configuration | IBMi |
| JOURNAL_VA | Access Control List Changes | Configuration | IBMi |
| JOURNAL_VC | Connections Started, Ended, or Rejected | Network | IBMi |
| JOURNAL_VF | Close Operations on Server Files | Resource | IBMi |
| JOURNAL_VL | Exceeded Account Limit Events | Profile | IBMi |
| JOURNAL_VN | Network Log On and Off Events | Configuration | IBMi |
| JOURNAL_VO | Actions on Validation Lists | Resource | IBMi |
| JOURNAL_VP | Network Password Errors | Profile | IBMi |
| JOURNAL_VR | Network Resource Accesses | Resource | IBMi |
| JOURNAL_VS | Server Sessions Started or Ended | Network | IBMi |
| JOURNAL_VU | Network Profile Changes | Profile | IBMi |
| JOURNAL_VV | Service Status Change Events | Network | IBMi |
| JOURNAL_X0 | Network Authentication Events | Network | IBMi |
| JOURNAL_X1 | Identity Token Events | Profile | IBMi |
| JOURNAL_XD | Directory Server Extensions | Profile | IBMi |
| JOURNAL_YC | DLO Object Changes | Resource | IBMi |
| JOURNAL_YR | DLO Object Reads | Resource | IBMi |
| JOURNAL_ZC | Object Changes | Resource | IBMi |

| | | | |
|---|---|---|---|
| JOURNAL_ZR | Object Reads | Resource | IBMi |
| KEYSTORE_DATA | KeyStore | Configuration | IBMi |
| LIBRARY_STAT | Library Statistics | Resources | IBMi |
| LINE_DESCRIPTION_DATA | Line Description Information | Configuration | IBMi |
| MESSAGE_QUEUE | Message Queue Details | Configuration | IBMi |
| MESSAGE_QUEUE_DATA | Message Queue Data | Configuration | IBMi |
| NETSERVER_CONFIG | NetServer Configuration | Network | IBMi |
| NETSERVER_SHARES | NetServer Shares | Network | IBMi |
| NETWORK_ATTRIBUTES | Network Attribute Information | Network | IBMi |
| NETWORK_CONNECTIONS | Network Connections Ipv4 and Ipv6 | Network | IBMi |
| NETWORK_EXIT_CONFIG | Exit Point Configuration Report | Network | IBMi |
| NETWORK_INTERFACE_IPV4 | Network Interface Data Ipv4 | Network | IBMi |
| NETWORK_INTERFACE_IPV6 | Network Interface Data Ipv6 | Network | IBMi |
| NETWORK_ROUTE_IPV4 | Network Route Data Ipv4 | Network | IBMi |
| NETWORK_ROUTE_IPV6 | Network Route Data Ipv6 | Network | IBMi |
| NETWORK_SERVER_DESCRIPTIONS | Network Server Description Data | Network | IBMi |
| NETWORK_SVR_ENCRYPT_STATUS | Network Server Encryption Status | Network | IBMi |
| NETWORK_TCPIP_IPV4 | TCP/IP Ipv4 Stack Attributes/Remote Exit Rule | Network | IBMi |
| NETWORK_TCPIP_IPV6 | TCP/IP Ipv6 Stack Attributes/Remote Exit Rule | Network | IBMi |
| NETWORK_TRANS_CENTRAL | Central Server Transactions | Network | IBMi |
| NETWORK_TRANS_COMMAND | Remote Command Transactions | Network | IBMi |
| NETWORK_TRANS_DATABASE | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_DATAQ | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_DDM | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_FILE | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_FTP_REXEC | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_PRINTER | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_SHOWCASE | Network Trans Showcase | Network | IBMi |
| NETWORK_TRANS_SIGNON | Remote Exit Rules | Network | IBMi |
| NETWORK_TRANS_TELNET | Remote Exit Rules | Network | IBMi |

| | | | |
|---|---|---|---|
| OBJECT_AUTHORITY | Display Object Authority | Resource | IBMi |
| OBJECT_DETAILS | Display Object Details | Resource | IBMi |
| OBJECT_STAT | Object/File Statistics | Resource | IBMi |
| OUTPUT_QUEUE | Output Queue Information | Configuration | IBMi |
| PRODUCT_INFO | Basic Information about a software product | Configuration | IBMi |
| PROFILE_COMPLIANCE | Profile Compliance Data | Profile | IBMi |
| PROFILE_INACTIVITY_SETTINGS | Profile Inactivity Settings | Profile | IBMi |
| PROFILE_MANAGER_DEFAULTS | Profile Manager Defaults | Profile | IBMi |
| PROGRAM_ADOPT | Programs that Adopt Authority | Resource | IBMi |
| PROGRAM_REFERENCE_DATA | Program Reference Data | Resource | IBMi |
| PTF_DATA | Program Temporary Fix Data | Configuration | IBMi |
| QHST_MSG_INFO | QHST History Log Information | Configuration | IBMi |
| QSYS2.ACTIVE_JOB_INFO | Active job information | Configuration | IBMi |
| QSYS2.DATA_QUEUE_ENTRIES | Data Queue Entries | Resource | IBMi |
| QSYS2.DRDA_AUTHENTICATION | DRDA and DDM User access | Configuration | IBMi |
| QSYS2.EXIT_POINT_INFO | Exit Point Information | Configuration | IBMi |
| QSYS2.EXIT_PROGRAM_INFO | Exit Program Information | Configuration | IBMi |
| QSYS2.FUNCTION_INFO | Function usage identifiers | Configuration | IBMi |
| QSYS2.FUNCTION_USAGE | Function usage configuration details. | Configuration | IBMi |
| QSYS2.GROUP_PTF_INFO | Group PTFs Information | Configuration | IBMi |
| QSYS2.JOURNAL_INFO | Journal and remote journal information | Configuration | IBMi |
| QSYS2.JOURNALED_OBJECTS | Journal object information | Resource | IBMi |
| QSYS2.LICENSE_INFO | Products license information. | Configuration | IBMi |
| QSYS2.MEDIA_LIBRARY_INFO | Media Library Status details | Configuration | IBMi |
| QSYS2.MEMORY_POOL | Memory pool details | Configuration | IBMi |
| QSYS2.MEMORY_POOL_INFO | Active memory pools | Configuration | IBMi |
| QSYS2.MESSAGE_QUEUE_INFO | Message Queue | Configuration | IBMi |

| | | | |
|---|---|---|---|
| QSYS2.NETSTAT_JOB_INFO | IPv4 and IPv6 network connection details. | Configuration | IBMi |
| QSYS2.OBJECT_LOCK_INFO | Object lock information | Configuration | IBMi |
| QSYS2.<br>OUTPUT_QUEUE_ENTRIES | Spooled file in output queue | Configuration | IBMi |
| QSYS2.RECORD_LOCK_INFO | Record lock information | Configuration | IBMi |
| QSYS2.REPLY_LIST_INFO | Current job's reply list entry information | Configuration | IBMi |
| QSYS2.<br>SCHEDULED_JOB_INFO | Job Schedule Entry information | Configuration | IBMi |
| QSYS2.<br>SERVER_SBS_ROUTING | Alternate subsystem configurations | Configuration | IBMi |
| QSYS2.<br>SERVER_SHARE_INFO | Server Share Information | Configuration | IBMi |
| QSYS2.<br>SOFTWARE_PRODUCT | Server Software Product information | Configuration | IBMi |
| QSYS2.SYSCONTROLS | Permissions or column mask defined | Configuration | IBMi |
| QSYS2.SYSCONTROLSDEP | Dependencies of row permissions and column masks | Configuration | IBMi |
| QSYS2.SYSDISKSTAT | Disk Information | Configuration | IBMi |
| QSYS2.<br>SYSTEM_STATUS_INFO | Partition information | Configuration | IBMi |
| QSYS2.SYSTMPSTG | IBM i temporary storage pool detail | Configuration | IBMi |
| QSYS2.USER_INFO | User Profile Information | Configuration | IBMi |
| QSYS2.USER_STORAGE | Storage usage by user profile | Configuration | IBMi |
| REMOTE_TRAN_SUMMARY_<br>BY_SERVER | Remote Summary Server | Network | IBMi |
| REMOTE_TRAN_SUMMARY_<br>BY_USER | Remote Summary User | Network | IBMi |
| RSC_MGR_COMPLIANCE_DA<br>TA | Resource Manager Authority Out of compliance data | Network | IBMi |
| RSC_MGR_CONFIG | Resource Manager Configuration | Network | IBMi |
| RSC_MGR_SCHEMA_DETAILS | Resource Manager Authority Schema Details | Network | IBMi |
| RSC_MGR_SCHEMA_HEADER | Resource Manager Authority Schema Header | Network | IBMi |
| SENSITIVE_DATABASE_CON<br>TENT | Sensitive Database Content | Profile | IBMi |
| SERVICE_TOOL_SECURITY_<br>ATTR | Service Tool Security Attributes | Profile | IBMi |
| SERVICE_TOOL_USERS | Service Tool User Data | Profile | IBMi |

| | | | |
|---|---|---|---|
| SOCKET_SUMMARY_BY_SERVER | Socket Summary by Server | Network | IBMi |
| SOCKET_SUMMARY_BY_USER | Socket Summary by User | Network | IBMi |
| SOCKET_TRAN_RULES | Socket Rules | Network | IBMi |
| SOCKET_TRANSACTIONS | Socket Transactions | Network | IBMi |
| SOFTWARE_RESOURCES | Installed Software Resources Data | Configuration | IBMi |
| SUBSYSTEM_AUTOSTART | Subsystem Autostart Jobs | Configuration | IBMi |
| SUBSYSTEM_COMMUNICATIONS | Subsystem Communication Entries | Configuration | IBMi |
| SUBSYSTEM_INFORMATION | Subsystem Information Details | Configuration | IBMi |
| SUBSYSTEM_JOB_QUEUE | Subsystem Job Queue | Configuration | IBMi |
| SUBSYSTEM_POOL_DATA | Subsystem Pool Data | Configuration | IBMi |
| SUBSYSTEM_PRESTART | Subsystem Prestart Jobs | Configuration | IBMi |
| SUBSYSTEM_REMOTE | Subsystem Remote Entries | Configuration | IBMi |
| SUBSYSTEM_ROUTING | Subsystem Routing Entries | Configuration | IBMi |
| SUBSYSTEM_WORKSTATION_NAMES | Subsystem Workstation Names | Configuration | IBMi |
| SUBSYSTEM_WORKSTATION_TYPES | Subsystem Workstation Types | Configuration | IBMi |
| SYS_VAL_CONFIG | System Value Configuration | Configuration | IBMi |
| SYS_VAL_DEFAULT | System Value Default | Configuration | IBMi |
| SYS_VAL_VALID | System Value Default | Configuration | IBMi |
| SYSCOLAUTH | Privileges Granted on a Column | Configuration | IBMi |
| SYSCONTROLS | Permission or Column Mask Defined | Configuration | IBMi |
| SYSCONTROLSDEP | Dependencies of Row Permissions and Column Masks | Configuration | IBMi |
| SYSCONTROLSDEP | Privileges Granted on a Row | Configuration | IBMi |
| SYSFIELDS | Columns with Field Procedures | Configuration | IBMi |
| SYSPACKAGEAUTH | Privileges Granted on a Package | Configuration | IBMi |
| SYSPROGRAMSTAT | Program, Service Program, and Module with SQL Statements | Configuration | IBMi |
| SYSROUTINEAUTH | Privileges Granted on a Routine | Configuration | IBMi |
| SYSSCHEMAAUTH | Privileges Granted on a Schema | Configuration | IBMi |
| SYSSEQUENCEAUTH | Privileges Granted on a Sequence | Configuration | IBMi |
| SYSTABAUTH | Privileges Granted on a Table or View | Configuration | IBMi |

| | | | |
|---|---|---|---|
| SYSTABLESTAT | Table Statistics Include all Partitions and Members | Configuration | IBMi |
| SYSTEM_VALUES | Display System Value Data | System | IBMi |
| SYSTOOLS. GROUP_PTF_CURRENCY | PTF Groups Installed per IBM Recommendations | Configuration | IBMi |
| SYSTOOLS. GROUP_PTF_DETAILS | PTFs within PTF Groups Installed per IBM Recommendations | Configuration | IBMi |
| SYSUDTAUTH | Privileges Granted on a Type | Configuration | IBMi |
| SYSVARIABLEAUTH | Privileges Granted on a Global Variable | Configuration | IBMi |
| SYSXSROBJECTAUTH | Privileges Granted on an XML Schema | Configuration | IBMi |
| TGMOBJINF | Object Information | Resource | IBMi |
| TG_NETWORK_GROUPS | TG Network Groups | Network | IBMi |
| TG_OBJECT_GROUPS | TG Object Groups | Network | IBMi |
| TG_OPERATION_GROUPS | TG Operation Groups | Network | IBMi |
| TG_USER_GROUPS | TG User Groups | Network | IBMi |
| USER_OBJECT_AUTHORITIES | User Profile Object Authorities | Profile | IBMi |
| USER_PRF_VIA_BLUEPRINT | User Profile via Blueprint | Profile | IBMi |
| USER_PROFILE_ACTIVITY | User Profile Activity | Profile | IBMi |
| USER_PROFILE_ARCHIVE | User Profile Archive | Profile | IBMi |
| USER_PROFILE_EXCLUSIONS | User Profile Exclusions | Profile | IBMi |
| USER_PROFILES | Display User Profile Data | Profile | IBMi |

# APPENDIX - TGCentral 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 | Journal Name, Journal Library, Journal Code and Journal Type, Alert Sequence |
| DET_JRNMON_ALERTS | Det_JrnMon_Alerts | Journal Name, Journal Library, Journal Code and Journal Type, Filter Sequence |
| DET_JRNMON_RULES | Det_JrnMon_Rules | Journal 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 |
| 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 |
| 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 |

# APPENDIX - TGCentral Permissions


- MENUS
- PAGES
- REPORTS AND REPORT CARDS


## MENUS

Use the following table to identify access levels for built-in roles.

| Permission | Admin | Super User | Help Desk | Auditor | Creator | Reader |
|---|---|---|---|---|---|---|
| **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 |
| **Inactive Session  Lockdown** | | | | | | |
| ISL Rules | A | A | A | A | D | D |
| Disconnect Options | A | A | A | A | D | D |
| Defaults | A | A | A | A | D | D |
| Authority Schema Config | A | A | A | A | D | D |
| Default | 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** |
|---|---|---|---|---|---|---|
| **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 |

**See also**

Permission

# APPENDIX - TGCentral FAQs


- Where are the log files stored?
- How do I adjust the log levels?
- How do I change the SSL certificate?
- What do I do if the TGCentral install fails?
- What if TGCentral won't load on a user's machine?
- What if I forget my admin password?
- What if a report won't stop running?
- Which TGCentral files should I backup on a daily basis?


## 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 tracks 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 tracks the events that occur between the GUI and the middle tier.

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

- tgcentral.log

## How do I adjust the log levels?

### 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**. 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**.

## Adjust TGCentral Log Files Located on Windows Machine

**To adjust the TGCentral log file:**

1) Navigate to the directory in which you have TGCentral installed (main directory).

2) Locate the tgcentral.conf file.

3) Modify the parameters as necessary.

## 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

## 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.

# 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 **Advanced** 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.

## Windows Installation

Use this task to ensure that both the "TGCentral" service is 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**. The **Run** dialog appears.

2) In the **Open** field, enter **services.msc**. The **Services** dialog appears.

3) Locate the following services and validate that the services are running:

| Name | Status must be |
|---|---|
| TGCentral | Running |

3) If they are not running, right-click the service and select **Start**.

# 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 your 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.

## 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.

## 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.

## 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**. 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. 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**. 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.

## 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