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 © 2019 Trinity Guard LLC. All rights reserved.
# Table of Contents

1. INTRODUCTION ................................................................................................................................. 10
   1.1. TGCENTRAL OVERVIEW .................................................................................................................. 10
   1.2. BENEFITS ......................................................................................................................................... 10
   1.3. FEATURES ........................................................................................................................................ 11
   1.4. ROLES ............................................................................................................................................. 11

2. GETTING STARTED ................................................................................................................................. 13
   2.1. GETTING STARTED USING TGCENTRAL ....................................................................................... 13
       2.1.1. Admin Tasks .............................................................................................................................. 13
       2.1.2. User Tasks ............................................................................................................................... 14
   2.2. LOG INTO TGCENTRAL .................................................................................................................... 15

3. DASHBOARD .......................................................................................................................................... 17
   3.1. DASHBOARD ................................................................................................................................ 17
       3.1.1. Display Report Run Activity ..................................................................................................... 17
       3.1.2. Display Report Card Run Activity .............................................................................................. 18
       3.1.3. Display Empty Report Activity ................................................................................................ 18
       3.1.4. Display Error Report Activity .................................................................................................. 19
       3.1.5. Display Run Statistics .............................................................................................................. 19
       3.1.6. Display Activity History .......................................................................................................... 19
       3.1.7. Display Report and Report Card Summary ............................................................................... 20
       3.1.8. Display Scheduled Report Summary ....................................................................................... 20
       3.1.9. Display Server Status Summary .............................................................................................. 20

4. SERVERS ............................................................................................................................................. 23
   4.1. SERVER MANAGEMENT .................................................................................................................... 23
   4.2. MANAGE SERVER ........................................................................................................................... 23
       4.2.1. Display List of Active Servers .................................................................................................... 24
       4.2.2. Refresh List of Active Servers ................................................................................................... 25
       4.2.3. Display Server Details .............................................................................................................. 25
       4.2.4. Display Server Activity History ................................................................................................ 25
       4.2.5. Add Server ................................................................................................................................. 25
       4.2.6. Delete Server ............................................................................................................................. 26
       4.2.7. Manage Server ........................................................................................................................... 26
       4.2.8. Unmanage a Server .................................................................................................................... 26
       4.2.9. Add Server to Group .................................................................................................................. 27
       4.2.10. Run Report on Server ............................................................................................................ 27
       4.2.11. Add Scheduled Report to Server ............................................................................................ 27
       4.2.12. Delete Scheduled Report from a Server .................................................................................. 28
       4.2.13. Disable Scheduled Report on Server ...................................................................................... 28
       4.2.15. Add Scheduled Report Card to Server .................................................................................... 29
       4.2.16. Delete Scheduled Report Card from a Server .......................................................................... 29
       4.2.17. Disable Scheduled Report Card on Server .............................................................................. 30

3.3. MANAGE SERVER GROUP ............................................................................................................... 30
   4.3.1. Display List of Server groups ...................................................................................................... 30
   4.3.2. Refresh List of Server Groups .................................................................................................... 31
   4.3.3. Display List of Servers in a Server Group .................................................................................. 31
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.4.</td>
<td>Display Server Group Activity History</td>
<td>31</td>
</tr>
<tr>
<td>4.3.5.</td>
<td>Add Server Group</td>
<td>31</td>
</tr>
<tr>
<td>4.3.6.</td>
<td>Edit Server Group</td>
<td>32</td>
</tr>
<tr>
<td>4.3.7.</td>
<td>Delete Server Group</td>
<td>32</td>
</tr>
<tr>
<td>4.3.8.</td>
<td>Add Server to Group</td>
<td>32</td>
</tr>
<tr>
<td>4.3.9.</td>
<td>Delete Server from Group</td>
<td>33</td>
</tr>
<tr>
<td>4.3.10.</td>
<td>Add Schedule Report to Server Group</td>
<td>33</td>
</tr>
<tr>
<td>4.3.11.</td>
<td>Delete Scheduled Report from Server Group</td>
<td>34</td>
</tr>
<tr>
<td>4.3.12.</td>
<td>Disable Scheduled Server Group Report</td>
<td>34</td>
</tr>
<tr>
<td>5.1.</td>
<td>Rules Management</td>
<td>35</td>
</tr>
<tr>
<td>5.2.</td>
<td>Job Activity Monitor</td>
<td>35</td>
</tr>
<tr>
<td>5.2.1.</td>
<td>Working with the Job Activity Monitor</td>
<td>35</td>
</tr>
<tr>
<td>5.2.2.</td>
<td>Manage Job Activity Monitoring Rules</td>
<td>36</td>
</tr>
<tr>
<td>5.2.2.1.</td>
<td>Display List of Job Activity Rules</td>
<td>36</td>
</tr>
<tr>
<td>5.2.2.2.</td>
<td>Refresh List of Job Activity Rules</td>
<td>37</td>
</tr>
<tr>
<td>5.2.2.3.</td>
<td>Edit Job Activity Rule</td>
<td>37</td>
</tr>
<tr>
<td>5.2.2.4.</td>
<td>Add Job Activity Rule</td>
<td>37</td>
</tr>
<tr>
<td>5.2.2.5.</td>
<td>Delete Job Activity Rule</td>
<td>37</td>
</tr>
<tr>
<td>5.2.3.</td>
<td>Manage Subsystems</td>
<td>38</td>
</tr>
<tr>
<td>5.2.3.1.</td>
<td>Display List of Subsystems</td>
<td>38</td>
</tr>
<tr>
<td>5.2.3.2.</td>
<td>Refresh List of Subsystems</td>
<td>39</td>
</tr>
<tr>
<td>5.2.3.3.</td>
<td>Import Subsystems</td>
<td>39</td>
</tr>
<tr>
<td>5.2.3.4.</td>
<td>Export Subsystem</td>
<td>39</td>
</tr>
<tr>
<td>5.2.3.5.</td>
<td>Edit Subsystem</td>
<td>40</td>
</tr>
<tr>
<td>5.2.3.6.</td>
<td>Add Subsystem</td>
<td>40</td>
</tr>
<tr>
<td>5.2.3.7.</td>
<td>Delete Subsystem</td>
<td>40</td>
</tr>
<tr>
<td>5.2.4.</td>
<td>Manage Commands</td>
<td>40</td>
</tr>
<tr>
<td>5.2.4.1.</td>
<td>Display List of Commands</td>
<td>41</td>
</tr>
<tr>
<td>5.2.4.2.</td>
<td>Refresh List of Commands</td>
<td>41</td>
</tr>
<tr>
<td>5.2.4.3.</td>
<td>Edit Command</td>
<td>41</td>
</tr>
<tr>
<td>5.2.4.4.</td>
<td>Add Command</td>
<td>42</td>
</tr>
<tr>
<td>5.2.4.5.</td>
<td>Delete Command</td>
<td>42</td>
</tr>
<tr>
<td>5.3.</td>
<td>Network Security</td>
<td>42</td>
</tr>
<tr>
<td>5.3.1.</td>
<td>Working with the Network Security</td>
<td>42</td>
</tr>
<tr>
<td>5.3.2.</td>
<td>Manage Network Defaults</td>
<td>43</td>
</tr>
<tr>
<td>5.3.2.1.</td>
<td>Display Network Defaults</td>
<td>43</td>
</tr>
<tr>
<td>5.3.2.2.</td>
<td>Refresh List of Network Defaults</td>
<td>44</td>
</tr>
<tr>
<td>5.3.2.3.</td>
<td>Edit Network Default</td>
<td>44</td>
</tr>
<tr>
<td>5.3.2.4.</td>
<td>Add Network Default</td>
<td>44</td>
</tr>
<tr>
<td>5.3.2.5.</td>
<td>Delete Network Default</td>
<td>45</td>
</tr>
<tr>
<td>5.3.3.</td>
<td>Manage Socket Rules</td>
<td>45</td>
</tr>
<tr>
<td>5.3.3.1.</td>
<td>Display List of Socket Rules</td>
<td>45</td>
</tr>
<tr>
<td>5.3.3.2.</td>
<td>Refresh List of Socket Rules</td>
<td>46</td>
</tr>
<tr>
<td>5.3.3.3.</td>
<td>Edit Socket Rule</td>
<td>46</td>
</tr>
<tr>
<td>5.3.3.4.</td>
<td>Add Socket Rule</td>
<td>47</td>
</tr>
<tr>
<td>5.3.3.5.</td>
<td>Delete Socket Rule</td>
<td>47</td>
</tr>
<tr>
<td>5.3.4.</td>
<td>Manage Exit Points</td>
<td>47</td>
</tr>
<tr>
<td>5.3.4.1.</td>
<td>Display List of Exit Point Configurations</td>
<td>48</td>
</tr>
<tr>
<td>5.3.4.2.</td>
<td>Refresh List of Exit Point Configurations</td>
<td>49</td>
</tr>
<tr>
<td>5.3.4.3.</td>
<td>Edit Exit Point Configuration</td>
<td>50</td>
</tr>
<tr>
<td>5.3.4.4.</td>
<td>Add Exit Point Configuration</td>
<td>50</td>
</tr>
</tbody>
</table>
What's New
This release includes the following:

Enhancements
• You can now email reports and report cards directly from the Activity interface.
• You can now set up (schedule) email notifications immediately on generation of a report.
• You can now set up (schedule) email notifications immediately on generation of a report card.
• Additional delta reports are now available. See APPENDIX C - Delta Reports for a complete lists of delta reports.

Fixes
• You can now run report cards associated with multiple user profiles
• You can now review the agent-side communication subsystem jobs using command: WRKACTJOB SBS(TGCMN).
• Jobs with message wait state corrected
1. Introduction

1.1. TGCentral Overview

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

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

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

See also

- Benefits
- Features
- Getting Started Using TGCentral

1.2. Benefits

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

TGCentral helps you do the following:

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

## 1.3. Features

The following are the major system features:

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

These features allow you to do the following:

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

## 1.4. Roles

Each user must be assigned one of the following roles:

<table>
<thead>
<tr>
<th>Role</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADMIN</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A larger organization might have many admins while a smaller organization might have a few, depending on resource availability.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See <a href="#">User Permissions</a> for a complete description of the access levels.</td>
</tr>
<tr>
<td><strong>SUPER USER</strong></td>
<td>Users in this role perform all TGCentral system actions: manage configuration, create/run/view reporting data. A super user manages rules.</td>
</tr>
<tr>
<td><strong>HELP DESK</strong></td>
<td>Users in this role manage agent groups/users, create/run/view reports, and create/run/view report cards.</td>
</tr>
<tr>
<td>Role</td>
<td>Descriptions</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>A help desk user provides troubleshooting assistance (e.g., logging in, using rules, running reports, etc.).</td>
</tr>
<tr>
<td>AUDITOR</td>
<td>Users in this role manage agent groups/users, create/run/view reports, and create/run/view report cards.</td>
</tr>
<tr>
<td></td>
<td>An auditor view rules.</td>
</tr>
<tr>
<td>CREATOR</td>
<td>Users in this role create report and report card definitions.</td>
</tr>
<tr>
<td>READER</td>
<td>Users in this role view configuration and reporting data.</td>
</tr>
</tbody>
</table>

See also

[User Permissions](#)
2. Getting Started

2.1. Getting Started Using TGCentral

TGCentral allows you to do the following for multiple agents:

- **Manager Servers** - Select which servers and server groups to monitor
- **Manager Rules** - Add and edit rules to control user access levels
- **Manage Groups** - Create groups to manage security more consistently and efficiently
- **Run Reports and Report Cards** - Run reports and report cards to monitor the security health
- **Monitor Activity** - View activities performed on a server

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

### 2.1.1. Admin Tasks

**Step 1** | **Set Agent Status to *ACTIVE**
---|---
For an agent to communicate with TGCentral, it must first be detected (seen). For TGCentral to detect an agent, its status must be set to *ACTIVE.
To set the status of an agent to *ACTIVE, see the TGCentral Installation Guide. The activation of servers is part of the TGCentral installation and configuration process.
**Tip:** If you have a TGCentral license, you can download the TGCentral Installation Guide from customer portal at TrinityGuard.com.
Step 2  Create Roles
After installation of TGCentral, one of the first tasks the admin must complete is to create roles.
You should create a role for each job category. Roles allow you to control access level.
See Manage Roles for additional instructions on creating and modifying roles.
Tip: A number of built-in roles are provided at the time of installation, See Permissions for a
description of each built-in role and its associated access level.

Step 3  Add Users
Once your project team establishes clear roles, then the administrator can begin adding users
and assigning those users to a role.
Tip: A user cannot access the system until an administrator adds the user and assign that user
login credentials (i.e., username and password)
See Manage Users for additional instructions.

2.1.2. User Tasks

Step 1  Login
Contact your TGCentral admin and obtain the TGCentral URL specific to your organization and
your unique login credentials (i.e., user name and password).
See Login into TGCentral for additional instructions.

Step 2  Add and remove servers
Determine which server(s) you want to manage. You can use TGCentral to manage as many or as
few servers as necessary.
See Manage Server for additional instructions.

Step 3  Add and edit rules
Create and edit rules. Rules control access.
Tip: You can distribute rules across multiple servers to promote consistency.
See Manager Rules for additional instructions.

Step 4  Add and edit groups
Create and edit groups. Groups allow you to work more efficiently.
Tip: You can distribute groups across multiple servers to promote consistency.
See the following topics for additional instructions:
Manage User Groups
Manage Object Groups
Manage Operation Groups

Step 5  Run reports and report cards
Run reports and report cards. Reports and report cards allow you to monitor the security health
of your system.
See the following topics for additional instructions:
Manage Reports
Manage Report Cards

Step 6  Monitor activity
Monitor activities performed on each server. Activities are the tasks performed by TGCentral users (i.e., login attempts, report runs, rule modifications, etc.). See Manage Activities for additional instructions.

Step 7 Modify user preferences
Each TGCentral user can modify their system settings to improve their user experience. See Manage Settings for additional instructions.

2.2. Log Into TGCentral

Use this task to log into TGCentral.

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

To access TGCentral

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

Note: The Sign In dialog is displayed.

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

3.1. **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:

- Display report run activity
- Display report card run activity
- Display empty report activity
- Display error report activity
- Display run statistics
- Display activity history
- Display report and report card summary
- Display scheduled report summary
- Display server status summary

### 3.1.1. Display Report Run Activity

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

**To display the report runs**

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

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

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

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed</td>
<td>The report ran successfully and is ready for viewing</td>
</tr>
<tr>
<td>Processing</td>
<td>The report is still in progress and is not ready for viewing at this time</td>
</tr>
<tr>
<td>Error</td>
<td>The report did not run successfully because of an error</td>
</tr>
</tbody>
</table>

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

**Tip**: To modify (edit) a report, see [Manage Reports](#).

---

**See also**

- [Manage Reports](#)
- [Manage Activities](#)
3.1.2. Display Report Card Run Activity

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

To display the list of report card runs

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

Note: The Report Activity pane is displayed.

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

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed</td>
<td>The report card ran successfully and is ready for viewing</td>
</tr>
<tr>
<td>Processing</td>
<td>The report card is still in progress and is not ready for viewing at this time</td>
</tr>
<tr>
<td>Error</td>
<td>The report card did not run successfully because of an error</td>
</tr>
</tbody>
</table>

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

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

See also

Manage Activities

3.1.3. Display Empty Report Activity

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

To display the list of empty reports

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

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

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

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

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

See also

Manage Reports
Manage Activities
3.1.4. Display Error Report Activity

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

To display the list of error reports
1) Select Dashboard in the left pane.
2) Click Error Reports (red icon at the top of the Dashboard pane).
3) Click the Report Activity tab.

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

Tip: Click on a column heading to sort the list in ascending or descending order.
4) Click the Action button to manage (e.g., view, delete, run again, etc.) a report.

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

See also
Manage Reports
Manage Activities

3.1.5. Display Run Statistics

Use this task to display the monthly run statistics for both reports and report cards (in a comparison graph).

Note: The run statistics are displayed graphically. The X-axis represents time, and the Y-axis represents the number of runs.

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

See also
Manage Reports
Manage Report Cards

3.1.6. 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.

Use this task to display the most recent activities.
3.1.7. Display Report and Report Card Summary

Use this task to display totals for the following:
- Built-in (standard) reports
- Custom (client-specific) reports
- Built-in report cards
- Custom report cards

To display report and report card summary

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

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

See also
- Manage Reports
- Manage Report Cards

3.1.8. Display Scheduled Report Summary

Use this task to display totals for the following:
- Ad-hoc scheduled report (scheduled to occur once)
- Daily scheduled reports (scheduled to occur daily)
- Weekly scheduled reports (scheduled to occur weekly)
- Monthly scheduled reports (scheduled to occur monthly)

To display scheduled report summary

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

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

See also
- Manage Reports
- Manage Report Cards

3.1.9. Display Server Status Summary

Use this task to display totals for the following:
- Managed servers (collecting data for monitoring purposes)
- Unmanaged servers (not collecting data for monitoring purposes)

To display server status summary

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

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

Manage Servers
Roles
User Permissions
4. Servers

4.1. Server Management

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

- Manage servers
- Manage server groups

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

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

See also
User Permissions

4.2. Manage Server

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

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

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

Report cards on Servers
- Run report card on server
- Add scheduled report card to server
- Delete scheduled report card from server
- Disable scheduled report card on server
4.2.1. Display List of Active Servers

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

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

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

To display the list of servers

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

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

3) Click the Details tab to see details (e.g., license status) specific to the server.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Name assigned to the server</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the server</td>
</tr>
<tr>
<td>OS Version</td>
<td>IBM operating version installed on the server</td>
</tr>
</tbody>
</table>
| Status         | Managed: TGCentral and the agent are communicating (sharing information) and are in sync  
                 Unmanaged: TGCentral and the agent are not communicating (not sharing information) and are not in sync  
                 Unknown: TGCentral and the agent are communicated, but the administrator has not yet determined if the server should be managed or unmanaged  
                 Note: If you see a gray dot beside the server name, it means the agent is either missing a TG product license or the license has expired.  
                 Tip: A color indicated should appear beside each server.  
                 -- A grey indicator icon (dot) appears when the server has been manually added, but TGCentral has not yet detected the TG products (e.g., TGSecure or TGAudit) necessary for integration (no agent detected).  
                 -- A red indicator icon (dot) appears when TGCentral detects the server, detects a valid license, but the server is offline (unable to communicate with TGCentral).  
                 -- A green indicator icon (dot) appears when TGCentral detects the server, detects a valid license, and the server is online (communicating with TGCentral).  
                 -- An orange indicator icon (dot) appears when TGCentral detects the server, the server is online, but a valid license is not detected (missing TGCentral license). |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Click on the <strong>Action</strong> button to see the list of tasks you can perform on the associated server</td>
</tr>
</tbody>
</table>

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

### 4.2.2. Refresh List of Active Servers

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

**To refresh the list of servers**
1. Access the **Servers** interface.
2. Click the **Refresh** button.

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

### 4.2.3. Display Server Details

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

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

### 4.2.4. Display Server Activity History

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

**To view the server activity history**

**Note**: The **Servers** interface is displayed in the right pane.
1. Access the **Servers** interface.
2. Select a server by clicking on the server name.
3. Select the **Activity History** tab.
4. View the server activity history in the bottom pane.

### 4.2.5. Add Server

Normally, you don’t need to add a server. Once you install TG software on a client (IBM) server and you set the client server status to *ACTIVE, TGCentral automatically detects the server. At which point, you only need to mark the server as managed or unmanaged. The only exception to this might be if you are performing a large implementation. In such a case, you might want to pre-populate servers (create placeholders) in TGCentral.
Creating or adding a server instance in TGCentral can be done fairly quickly; whereas, it might take much longer to prepare all the client servers for detection.

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

### To add a server

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Name you want to assign the server</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the server</td>
</tr>
<tr>
<td>OS Version</td>
<td>IBM operating version installed on the server</td>
</tr>
</tbody>
</table>
4. Click **Save**.

### 4.2.6. Delete Server

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

**To delete a server**

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

### 4.2.7. Manage Server

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

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

**To manage a server**

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

### 4.2.8. Unmanage a Server

Use this task to stop managing an active server using TGCentral. This is useful in 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.

4.2.9. Add Server to Group

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

To add a server to a group
1) Access the Servers interface.
2) Click the Action button for the server you want to add to a group.
3) Select Add to Server Group.
Note: The List of Server Groups dialog is displayed.
4) Select the group to which you want to add the server.
5) Click Save.

4.2.10. Run Report on Server

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

To run a report on a specific server
1) Access the Server interface.
2) Select a server by clicking on the server name.
3) Select the Activity History tab.
4) Click the + Run button, and select Report from the list.
Note: The Run Report dialog appears.
5) Select the report you want to run from the list.
6) Click Run Now.

4.2.11. Add Scheduled Report to Server

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

To add a scheduled report
1) Access the Server interface.
2) Select a server by clicking on the server name.
3) Select the Schedule tab.
4) Click the + New Schedule button, and select Report from the list.
Note: The Schedule Report dialog is displayed.
5) Select the report you want to schedule from the list.
6) Complete the following fields:

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

7) Click **Save**.

### 4.2.12. Delete Scheduled Report from a Server

Use this task to delete a scheduled report.

**To delete a scheduled report**

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

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

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

### 4.2.13. Disable Scheduled Report on Server

Use this task to disable a scheduled report temporarily.

**To disable a scheduled report**

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

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

4) Click the **Actions** button for the scheduled report you want to disable.
5) Select **Disable Schedule**.

### 4.2.14. Run Report Card on Server

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

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

Note: The Run Report Card dialog appears.

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

### 4.2.15. Add Scheduled Report Card to Server

Use this task to add a scheduled report card.

**To add a scheduled report card**

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

Note: The Schedule Report Card dialog is displayed.

5) Select the report card you want to schedule from the list.
6) Complete the following fields:

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

7) Click Save.

### 4.2.16. Delete Scheduled Report Card from a Server

Use this task to delete a scheduled report card.

**To delete a scheduled report card**

1) Access the Server interface.
2) Select a server by clicking on the server name.
3) Select the Schedule tab.
Note: The report cards associated with the server are displayed in the bottom pane.

4) Click the Actions button for the scheduled report card you want to delete.
5) Select Delete.

4.2.17. Disable Scheduled Report Card on Server

Use this task to disable a scheduled report card.

To disable a scheduled report card
1) Access the Server interface.
2) Select a server by clicking on the server name.
3) Select the Schedule tab.

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

4) Click the Actions button for the scheduled report card you want to disable.
5) Select Disable Schedule.

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

4.3. Manage Server Group

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

4.3.1. Display List of Server groups

Use this task to view the list of server groups.

To display the list of server groups
1) Expand the Server Management menu in the left pane.
2) Click on Server Groups.

Note: The Server Groups interface is displayed.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group Name</td>
<td>Name assigned to the server group</td>
</tr>
<tr>
<td>Date</td>
<td>Date on which the group was created</td>
</tr>
</tbody>
</table>

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

### 4.3.2. Refresh List of Server Groups

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

**To refresh the list of server groups**
1) Access the Server Groups interface.
2) Click the Refresh button.

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

### 4.3.3. Display List of Servers in a Server Group

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

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

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

### 4.3.4. Display Server Group Activity History

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

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

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

### 4.3.5. Add Server Group

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

**To add a server group**
1) Access the Server Group interface.
2) Click the Add Server Group button.
3) Enter the Server Group Name.
4) Click Next.
5) Select the server(s) you want included in the group and deselect the server(s) you want to exclude from the group.
6) Click Save.

4.3.6. Edit Server Group

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

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

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

4.3.7. Delete Server Group

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

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

4.3.8. Add Server to Group

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

To add a server to a group
1) Access the Server Groups interface.
2) Click the Actions button for the server group you want to modify.
3) Select Edit.
4) If you want to modify the Server Group Name, you can do that now.
5) Click Next.
6) Select the server(s) you want to add to the group.
7) Click Save.
Tip: Alternatively, access the Server interface, and click the Action button and select Add to ServerGroup option.

4.3.9. Delete Server from Group

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

To delete a server from a server group
1) Access the Server Groups interface.
2) Click on a server group to select it.
Note: The servers (members) associated with the server group are displayed in the bottom pane.
3) Click the Details tab.
4) Click the Action button beside the server you want to delete.
5) Select Delete.

4.3.10. Add Schedule Report to Server Group

Use this task to add a scheduled report.

To add a scheduled report to a server group
1) Access the Server Group interface.
2) Click on a server group to select it.
3) Select the Schedule tab.
Note: The reports associated with the server group are displayed in the bottom pane.
4) Click the + New Schedule button.
Note: The Schedule Report dialog is displayed.
5) Select the report you want to schedule from the list.
6) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>Start date on which the schedule is valid</td>
</tr>
<tr>
<td>End Date</td>
<td>End date on which the schedule becomes invalid</td>
</tr>
<tr>
<td>Frequency</td>
<td>How often the report should run within the designated start and end date</td>
</tr>
<tr>
<td></td>
<td><strong>One Day</strong> - Once</td>
</tr>
<tr>
<td></td>
<td><strong>Daily</strong> - Once a day</td>
</tr>
<tr>
<td></td>
<td><strong>Weekly</strong> - Once a week</td>
</tr>
<tr>
<td></td>
<td><strong>Monthly</strong> - Once a month</td>
</tr>
<tr>
<td></td>
<td><strong>Yearly</strong> - Once a year</td>
</tr>
<tr>
<td>Time</td>
<td>Time at which the scheduled report should run</td>
</tr>
</tbody>
</table>
7) Click Save.
4.3.11. Delete Scheduled Report from Server Group

Use this task to delete a scheduled report.

To delete a scheduled report from a server group

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

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

4) Click the Actions button for the scheduled report you want to delete.
5) Select Delete.

4.3.12. Disable Scheduled Server Group Report

Use this task to disable a scheduled report.

To disable a scheduled report from a server group

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

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

4) Click the Actions button for the scheduled report you want to disable.
5) Select Disable Schedule.

See also

- Manage Servers
- Manage Reports
5. Rules

5.1. Rules Management

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

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

Job Activity Monitor

Manage Job Activity Rules

Network Security

Manage Network Defaults
Manage Socket Rules
Manage Remote Exit Rules
Manage Exit Point Configuration

Access Escalation Management

Manage AEM Defaults
Manage Entitlements
Manage Access Control
Manage File Editors

See also

User Permissions

5.2. Job Activity Monitor

5.2.1. Working with the Job Activity Monitor

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

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

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

Tip: The features available to each user are dependent on the user’s permission level, which is based on their assigned role.
5.2.2. Manage Job Activity Monitoring Rules

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

- Job Activity Details Report
- Job Activity Summary Report

Use this task to do the following:
- Display the list of job activity rules
- Refresh the list of job activity rules
- Edit a job activity rule
- Add a job activity rule
- Delete a job activity rule

5.2.2.1. Display List of Job Activity Rules

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

To display the list of job activity rules

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

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

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

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

### 5.2.2.2. Refresh List of Job Activity Rules

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

**To refresh the list of job activity rules**

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

### 5.2.2.3. Edit Job Activity Rule

Use this task to edit a job activity rule.

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

**To edit a job activity rule**

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

### 5.2.2.4. Add Job Activity Rule

Use this task to add a job activity rule.

**To add a job activity rule**

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

### 5.2.2.5. Delete Job Activity Rule

Use this task to delete a job activity rule.

**To delete a job activity rule**

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

You can use the Job Activity Monitor (JAM) to monitor a subsystem. When you add a subsystem, the system captures (logs) activities for users based on their job descriptions. You can limit or modify what is captured in the job monitor log by creating a job activity rule. Job activity rules take precedence over the user’s job description. For example, if you add a subsystem, the system begins monitoring (logging) activities performed on that subsystem by each user. 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 job 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:
- Display list of subsystems
- Refresh list of subsystems
- Edit a subsystem
- Add a subsystem
- Delete a subsystem

5.2.3.1. Display List of Subsystems

Use this task to view the list of subsystems.

To display the list of subsystems

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name assigned to the server</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to subsystem</td>
</tr>
<tr>
<td>Library</td>
<td>Name assigned to the library in which the subsystem resides</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the subsystem</td>
</tr>
<tr>
<td>Log Status</td>
<td>Status of logging:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>*ACTIVE</td>
<td>Collect log data for job monitoring</td>
</tr>
<tr>
<td>*INACTIVE</td>
<td>Do not collect log data for job monitoring</td>
</tr>
</tbody>
</table>

Action | Click on the Action button to see the list of tasks you can perform on the associated subsystem

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

### 5.2.3.2. Refresh List of Subsystems

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

To refresh the list of subsystems

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

### 5.2.3.3. Import Subsystems

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

To import subsystems

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

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

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

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

### 5.2.3.4. Export Subsystem

Use this task to export a subsystem to a server or group of 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.
5.2.3.5. Edit Subsystem

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

To edit a subsystem

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

5.2.3.6. Add Subsystem

Use this task to add a subsystem.

To add a subsystem

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

5.2.3.7. Delete Subsystem

Use this task to delete a subsystem.

To delete a subsystem

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

See also

Rules Management

5.2.4. Manage Commands

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

Use this task to do the following:
- Display list of commands
- Refresh list of commands
- Edit a command
- Add a command
- Delete a command
5.2.4.1. Display List of Commands

Use this task to view the list of commands.

To display the list of commands
1) Expand the Rules menu (in the left pane).
2) Expand the Job Activity Monitor menu.
3) Select Commands.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name assigned to the server</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the command</td>
</tr>
<tr>
<td>Library</td>
<td>Library in which the command resides</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the command</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated command</td>
</tr>
</tbody>
</table>

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.

- ENDOBJ
- SIGNOFF
- ENDOJOBABN
- ENDPASTHR

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

5.2.4.2. Refresh List of Commands

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

To refresh the list of commands
1) Access the Commands interface.
2) Click the Refresh button.

5.2.4.3. Edit Command

Use this task to edit a command. Editing might involve changing the name and/or library.
To edit a command
1) Access the Commands interface.
2) Click the Actions button beside the command you want to modify.
3) Select Edit.
4) Modify the command attributes as necessary.
5) Click Save.

5.2.4.4. Add Command
Use this task to add a command.

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

5.2.4.5. Delete Command
Use this task to delete a command.

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

See also
Rules Management

5.3. Network Security

5.3.1. Working with the Network Security
This section describes how to manage network security. Network security allows you to control who accesses your network.

See also
Manage Network Defaults
Manage Socket Rules
Manage Remote Exit Rules
Manage Exit Point Configuration
5.3.2. Manage Network Defaults

This section describes working with network security defaults.

Network security defaults define the following:

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

Use this task to do the following:

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

5.3.2.1. Display Network Defaults

Use this task to view the list of rule defaults.

To display the rule defaults

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the network defaults are applicable</td>
</tr>
<tr>
<td>Audit Status</td>
<td>Whether auditing is enabled</td>
</tr>
<tr>
<td>Note: Auditing is required if you plan to run network reports.</td>
<td></td>
</tr>
<tr>
<td>*YES -</td>
<td>Auditing enabled (record audit data)</td>
</tr>
</tbody>
</table>
### Field Description

*NO - Auditing disabled (do not record audit data)

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal</td>
<td>Journal in which to store audit data</td>
</tr>
<tr>
<td>Library</td>
<td>Library in which the audit journal resides</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerting is enabled:</td>
</tr>
<tr>
<td></td>
<td>*YES - Alerts enabled</td>
</tr>
<tr>
<td></td>
<td>*NO - Alerts disabled</td>
</tr>
<tr>
<td>Message Queue</td>
<td>Queue in which to store alerts</td>
</tr>
<tr>
<td>Message Queue</td>
<td>Library in which to store alerts</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated rule</td>
</tr>
</tbody>
</table>

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

### 5.3.2.2. Refresh List of Network Defaults

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

**To refresh the list of network defaults**

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

### 5.3.2.3. Edit Network Default

Use this task to edit a network default.

**To edit a network default**

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

### 5.3.2.4. Add Network Default

Use this task to add a network default.
To add a network default
1) Access the Network Security Defaults interface.
2) Click the Add button.
3) Enter the necessary attributes.
4) Click Save.

5.3.2.5. Delete Network Default
Use this task to delete a network default.

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

See also
Working the Network Security Rules Management

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

Use this task to do the following:
- Display list of socket rules
- Refresh list of socket rules
- Edit socket rule
- Add socket rule
- Delete socket rule

5.3.3.1. Display List of Socket Rules
Use this task to view the list of socket rules.
To display the list of socket rules
1) Expand the Rules menu (in the left pane).
2) Expand the Network Security menu.
3) Select Job Socket Rules.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the socket rule is applicable</td>
</tr>
<tr>
<td>User/Group</td>
<td>User or user group that initiated the transaction</td>
</tr>
<tr>
<td>Operation/Port</td>
<td>Port from which the transaction was initiated</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address from which the transaction was initiated</td>
</tr>
<tr>
<td>Calendar</td>
<td>Applicable calendar</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerting is enabled: *YES - Alerts enabled</td>
</tr>
<tr>
<td></td>
<td>*NO - Alerts disabled</td>
</tr>
<tr>
<td>Socket Action</td>
<td>The level at which action is taken: *EXITLVL - Exit point level</td>
</tr>
<tr>
<td></td>
<td>Note: If the action failed, you will see *FAIL in this column.</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated rule</td>
</tr>
</tbody>
</table>

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

### 5.3.3.2. Refresh List of Socket Rules

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

To refresh the list of socket rules
1) Access the Socket Rules interface.
2) Click the Refresh button.

### 5.3.3.3. Edit Socket Rule

Use this task to edit a socket rule.

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

To edit a socket rule
1) Access the Socket Rules interface.
2) Click the Actions button beside the rule you want to modify.
3) Select Edit.
4) Modify the attributes as necessary:
5) Click Save.
5.3.3.4. Add Socket Rule
Use this task to add a socket rule.

To add a socket rule
1) Access the Socket Rules interface.
2) Click the Add button.
3) Enter the necessary rule attributes.
4) Click Save.

5.3.3.5. Delete Socket Rule
Use this task to delete a socket rule.

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

See also
Working the Network Security Rules Management

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

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

Client-Server Communication Process via transport layer:

(1) Exit Point (Parking Spot): An exit point is a point in the network communication process between a client and a server where control is turned over to an exit program if an exit program exists.
(2) Exit Program (Car): An exit programs can be created for each type of network communication (FTP, ODBC, JDBC, SQL, etc.). Exit programs control execution of transactions between a client and a server.

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

Use this task to do the following:
- Display_list_of_exit_point_configurations
- Refresh_list_of_exit_point_configurations
- Edit_exit_point_configuration
- Add_exit_point_configuration
- Delete_exit_point_configuration
- Cycle server

5.3.4.1. Display List of Exit Point Configurations

Use this task to view the list of exit points.

To display the list of exit points
1) Expand the Rules menu in the left pane.
2) Expand the Network Security menu.
3) Select Exit Point Config.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the socket rule is applicable</td>
</tr>
<tr>
<td>Network</td>
<td>Name of the server type</td>
</tr>
<tr>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>Audit Status</td>
<td>Whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Record incoming transaction data in the audit journal</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Do not record incoming transaction data in the audit journal</td>
</tr>
<tr>
<td>Tip:</td>
<td>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</td>
</tr>
</tbody>
</table>
### Field Description

- **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.

- Whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go into effect.
  - *YES* - Apply exit rules (enable network security)
  - *NO* - Disable exit rules (disable network security)

- Whether alerting is enabled for a specific exit point. Alerts are required if you plan to send alert notifications.
  - *ALL* - Record an alert for all (PASS and FAIL) connection attempts
  - *FAIL* - Record only FAIL connection attempts
  - *NONE* - Do not record alerts

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

- Whether the smart mode (Rules Intelligence Engine) is enabled.
  - *YES* - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions
  - *NO* - Do not enable the intelligence engine to create rules

  **Note:** The system administrator can delete rules created by the Rules Intelligence Engine at any time.

- Which incoming transactions you want to track (collect) in the **Incoming Transaction** interface.
  - *ALL* - Collect and display all (PASS and FAIL) incoming transactions
  - *FAIL* - Collect and display only rejected (FAIL) incoming transactions
  - *NONE* - Do not collect or display any incoming transactions

- A short description of the network

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

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

### 5.3.4.2. Refresh List of Exit Point Configurations

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

**To refresh the list of exit points**

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

Use this task to edit an exit point.

To edit an exit point

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

5.3.4.4. Add Exit Point Configuration

Use this task to add an exit point.

To add an exit point

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

5.3.4.5. Delete Exit Point Configuration

Use this task to delete an exit point.

To delete an exit point

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

5.3.4.6. Cycle Server

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

To cycle a server

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

See also

Working the Network Security
Rules Management
5.3.5. Manage Remote Exit Rules

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

Example Usage:

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

Client-Server Communication Process via transport layer:

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

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

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

Use this task to do the following:
- Display_list_of_remote_exit_rules
- Refresh_list_of_remote_exit_rules
- Edit_remote_exit_rules
- Add_remote_exit_rules
- Delete_remote_exit_rules

5.3.5.1. Display List of Remote Exit Rules

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

To display the list of remote exit rules

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

Note: The Remote Exit Rules interface is displayed in the right pane.
### Field | Description
--- | ---
Server | Server on which the socket rule is applicable
User/Group | User or user group that initiated the transaction
Operation Server | Server from which the transaction was initiated
Function | Function that was initiated
Client IP | IP address from which the transaction was initiated
Calendar | Applicable calendar
Alert Status | Whether alerting is enabled: 
*YES* - Alerts enabled 
*NO* - Alerts disabled
Exit Rule Action | The level at which action is taken: 
*EXITLVL* - Exit point level
**Note:** If the action failed, you will see *FAIL* in this column.
Object Details | Short description of the object to which access was attempted
Action | Click on the **Action** button to see the list of tasks you can perform on the associated rule

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

### 5.3.5.2. Refresh List of Remote Exit Rules

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

To refresh the list of remote exit rules
1) Access the Remote Exit Rules interface.
2) Click the **Refresh** button.

### 5.3.5.3. Edit Remote Exit Rules

Use this task to edit a remote exit rule.

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

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

### 5.3.5.4. Add Remote Exit Rules

Use this task to add a remote exit rule.
To add a remote exit rule
1) Access the Remote Exit Rules interface.
2) Click the Add button.
3) Enter the necessary attributes.
4) Click Save.

5.3.5.5. Delete Remote Exit Rules
Use this task to delete a remote exit rule.

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

See also
Working the Network Security
Rules Management

5.4. Access Escalation Management

5.4.1. Working with the Access Escalation Management
This section describes how to escalate user access. Use the Access Escalation Management feature to allow users to swap profiles.

See also
Manage AEM Defaults
Manage Entitlements
Manage Access Control
Manage File Editors

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

Access escalation defaults allow you to define the following:

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

Use this task to view the list of AEM defaults.

To display the list of AEM defaults:

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the AEM defaults are applicable</td>
</tr>
<tr>
<td>Default Swap User</td>
<td>The default swap user (if one is not identified)</td>
</tr>
<tr>
<td>Authentication Timeout</td>
<td>Number of minutes the AEM session will remain enabled before requiring the user to reenter a password</td>
</tr>
<tr>
<td>Transaction Journal</td>
<td>Journal in which to store journal data</td>
</tr>
<tr>
<td>Transaction Journal Library</td>
<td>Library in which the journal resides</td>
</tr>
<tr>
<td>Audit Configuration Changes</td>
<td>Whether to collect data about AEM changes</td>
</tr>
<tr>
<td></td>
<td>Y - Enable tracking of changes</td>
</tr>
<tr>
<td></td>
<td>N - Disable tracking of changes</td>
</tr>
</tbody>
</table>

Tip: This flag must be set to Y if you plan to run access escalation change reports.
**Field** | **Description**
---|---
| **Note**: There are multiple product modules (e.g., network security, access escalation, etc.) in which you can track configuration changes. Therefore, if you see *NONE* in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL*, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL*, this indicates that configuration changes are being tracked in all modules.

<table>
<thead>
<tr>
<th>Alert Message Queue</th>
<th>Queue in which to store alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Message Queue Library</td>
<td>Library in which to store the queue</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the <strong>Action</strong> button to see the list of tasks you can perform on the associated AEM default</td>
</tr>
</tbody>
</table>

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

### 5.4.2.2. Refresh List of AEM Defaults

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

**To refresh the list of AEM defaults**

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

### 5.4.2.3. Edit AEM Defaults

Use this task to edit an AEM default.

**To edit an AEM default**

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

### 5.4.2.4. Add AEM Default

Use this task to add an AEM default.

**To add an AEM default**

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

Use this task delete an AEM default.

To delete an AEM Default

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

See also

Working the Access Escalation Management

Rules Management

5.4.3. Manage User Entitlements

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

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

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

Use this task to do the following:
- Display list of entitlements
- Refresh list of entitlements
- Edit entitlements
- Add entitlements
- Delete entitlements

5.4.3.1. Display List of Entitlements

Use this task to view the list of entitlements.

To display the list of entitlements

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the socket rule is applicable</td>
</tr>
<tr>
<td>Enable Status</td>
<td>Whether the entitlement is enabled:</td>
</tr>
<tr>
<td></td>
<td>Y - Enabled</td>
</tr>
<tr>
<td></td>
<td>N - Disabled</td>
</tr>
<tr>
<td>User</td>
<td>User or user groups to which the entitlement applies</td>
</tr>
<tr>
<td>Object</td>
<td>Object or object groups to which the entitlement applies</td>
</tr>
<tr>
<td>Library</td>
<td>Library in which the object resides</td>
</tr>
<tr>
<td>Type</td>
<td>Type of object</td>
</tr>
<tr>
<td></td>
<td>*PMG - Program</td>
</tr>
<tr>
<td></td>
<td>*CMD - Command</td>
</tr>
<tr>
<td></td>
<td>*File - Database file</td>
</tr>
<tr>
<td>Swap User</td>
<td>Swap profile whose privileges will be used to execute the entitlement</td>
</tr>
<tr>
<td>Calendar</td>
<td>Applicable calendar</td>
</tr>
<tr>
<td>Aut Req?</td>
<td>Whether user must enter a password (authenticate) in order to use the entitlement</td>
</tr>
<tr>
<td></td>
<td>Y - Password required</td>
</tr>
<tr>
<td></td>
<td>N - No password required</td>
</tr>
<tr>
<td>Alr Req?</td>
<td>Whether an alert is sent to the alert queue when an attempt is made to use the entitlement</td>
</tr>
<tr>
<td></td>
<td>Y - Alert enabled</td>
</tr>
<tr>
<td></td>
<td>N - Alert Disabled</td>
</tr>
<tr>
<td>Description</td>
<td>Short description identifying the purpose of the entitlement</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the <strong>Action</strong> button to see the list of tasks you can perform on the associated rule</td>
</tr>
</tbody>
</table>

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

### 5.4.3.2. Refresh List of Entitlements

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

To refresh the list of entitlements

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

Use this task to edit an entitlement.

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

**To edit an entitlement**

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

5.4.3.4. Add Entitlements

Use this task to add an entitlement.

**To add an entitlement**

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

5.4.3.5. Delete Entitlements

Use this task to delete an entitlement.

**To delete an entitlement**

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

**See also**

[Rules Management](#)

### 5.4.4. Manage Access Control

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

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

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

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

To display the list of access control

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the access control is applicable</td>
</tr>
<tr>
<td>User</td>
<td>User or user group to which the entitlement applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address from which the transaction was initiated</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated access control</td>
</tr>
</tbody>
</table>

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

5.4.4.2. Refresh List of Access Controls

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

To refresh the list of access controls

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

5.4.4.3. Edit Access Controls

Use this task to edit an access control.

To edit an access control

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

5.4.4.4. Add Access Controls

Use this task to add an access control rule.

To add an access control

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

5.4.4.5. Delete Access Controls

Use this task to delete an access control.

To delete an access control

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

See also

Working the Access Escalation Management Rules Management

5.4.5. Manage File Editors

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

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

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

### 5.4.5.1. Display File Editors

Use this task to view the list of file editors.

**To display the list of file editors**

1. Expand the Rules menu in the left pane.
2. Expand the Access Escalation Mgmt menu.

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the file editor is applicable</td>
</tr>
<tr>
<td>Editor Command</td>
<td>Command to be executed</td>
</tr>
<tr>
<td>Editor Library</td>
<td>Library in which to execute the command</td>
</tr>
<tr>
<td>Editor Parameter</td>
<td>Parameter to be executed</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated file editor</td>
</tr>
</tbody>
</table>

### 5.4.5.2. Refresh List of File Editors

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

**To refresh the list of file editors**

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

### 5.4.5.3. Edit File Editor

Use this task to edit a file editor.

**To edit a file editor**

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

5.4.5.4. Add File Editor

Use this task to add a file editor.

To add a file editor
1) Access the File Editor interface.
2) Click the Add button.
3) Enter the necessary attributes.
4) Click Save.

5.4.5.5. Delete File Editor

Use this task to delete a file editor.

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

See also

Working the Access Escalation Management
Rules Management
6. Groups

6.1. Group Management

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

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

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

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

See also
User Permissions

6.2. Manage User Groups

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

Use this task to do the following:

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

6.2.1. Display List of User Groups

Use this task to view the list of user groups.

To display the list of user groups

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

Note: The User Groups interface is displayed in the right pane.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name of server in which the user group exists.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the user group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description assigned to the user group</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the <strong>Action</strong> button to see the list of tasks you can perform on the associated user group</td>
</tr>
</tbody>
</table>

**Note:** User group names always begin with a colon.

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

### 6.2.2. Refresh List of User Groups

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

**To refresh the list of User Groups**

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

### 6.2.3. Import User Group

Use this task to import a user group.

**To import a user group**

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

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

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

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

### 6.2.4. Export User Group

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

**To export a user group**

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

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

### 6.2.5. Edit User Group

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

**To edit a user group**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description assigned to the user group</td>
</tr>
</tbody>
</table>

5. Click **Save**.

### 6.2.6. Add User Group

Use this task to add a user group.

**To add a user group**

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

### 6.2.7. Delete User Group

Use this task to delete a user group.

**To delete a user group**

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

### 6.3. Manage Network/Server Groups

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

Use this task to do the following:

- [Display list of network groups](#)
- [Refresh list of network groups](#)
6.3.1. Display List of Network Groups

Use this task to view the list of network groups.

To display the list of network groups

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name of server in which the network group exists.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the network group</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Network group names always begin with a colon.</td>
</tr>
<tr>
<td>Description</td>
<td>Description assigned to the network group</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated network group</td>
</tr>
</tbody>
</table>

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

6.3.2. Refresh List of Network Groups

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

To refresh the list of Network Groups

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

6.3.3. Edit Network Groups

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

To edit a network group

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

Use this task to add a network group.

To add a network group

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

6.3.5. Delete Network Groups

Use this task to delete a network group.

To delete a network group

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

6.4. Manage Operation Groups

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

Use this task to do the following:

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

6.4.1. Display List of Operation Groups

Use this task to view the list of operation groups.

To display the list of operation groups

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name of server in which the operation group exists.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the operation group</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Operation group names always begin with a colon.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Description assigned to the operation group</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated operation group</td>
</tr>
</tbody>
</table>

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

### 6.4.2. Refresh List of Operation Groups

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

**To refresh the list of** Operation Groups
1) Access the **Operation Groups** interface.
2) Click the **Refresh** button.

### 6.4.3. Edit Operation Groups

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

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

### 6.4.4. Add Operation Groups

Use this task to add an operation group.

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

### 6.4.5. Delete Operation Groups

Use this task to delete an operation group.

**To delete an operation group**
1) Access the **Operation Groups** interface.
2) Click the **Actions** button for group you want to delete.
3) Select **Delete**.
6.5. Manage Object Groups

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

Use this task to do the following:

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

6.5.1. Display List of Object Groups

Use this task to view the list of object groups.

To display the list of object groups

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name of server in which the object group exists.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the object group. <strong>Note:</strong> Object group names always begin with a colon.</td>
</tr>
<tr>
<td>Description</td>
<td>Description assigned to the object group</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform on the associated object group</td>
</tr>
</tbody>
</table>

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

6.5.2. Refresh List of Object Groups

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

To refresh the list of Object Groups

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

6.5.3. Edit Object Groups

Use this task to edit an object group. Editing might involve changing the group description.
To edit an object group
1) Access the Object Groups interface.
2) Click the Actions button beside the group you want to modify.
3) Select Edit Group.
4) Modify the group attributes as necessary:
5) Click Save.

6.5.4. Add Object Groups
Use this task to add an object group.

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

6.5.5. Delete Object Groups
Use this task to delete an object group.

To delete an object group
1) Access the Object Groups interface.
2) Click the Actions button for group you want to delete.
3) Select Delete.
7. Calendar

7.1. Calendar Management

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

- Manage calendars

7.2. Manage Calendars

This section describes working with calendars.

Use this task to do the following:

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

7.2.1. Display List of Calendars

Use this task to view the list of calendars.

To display the list of object groups

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

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

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

Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.
7.2.2. Refresh List of Calendars

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

To refresh the list of Calendar
1) Access the Calendar interface.
2) Click the Refresh button.

7.2.3. Edit Calendar

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

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

7.2.4. Add Calendar

Use this task to add a calendar.

To add a calendar
1) Access the Calendar interface.
2) Click the Add button.
3) Enter the necessary attributes:
4) Click Save.

7.2.5. Delete Calendar

Use this task to delete a calendar.

To delete a calendar
1) Access the Calendar interface.
2) Click the Actions button for group you want to delete.
3) Select Delete.
8. Reporting

8.1. Reporting Management

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

- Manage reports
- Manage report cards

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

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

See also

User Permissions

8.2. Manage Reports

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

Use this task to do the following:

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

8.2.1. Display List of Reports

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

To display the list of reports

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

Note: The Reports interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Report category (i.e., Resource, Profile, Configuration, etc.)</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Name</td>
<td>Name assigned to the report</td>
</tr>
<tr>
<td>Collector ID</td>
<td>ID assigned to the collector</td>
</tr>
<tr>
<td>Collector</td>
<td>Journal collector from which report data is pulled</td>
</tr>
</tbody>
</table>
| Built-in | Y (Yes): Pre-built report (delivered as part of the product)  
                        N (No): Custom report (specific to the client) |
| Action    | Click on the Action button to see the list of tasks you can perform for the associated report  
                        (e.g., copy, run, schedule, etc.) |

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

### 8.2.2. Refresh List of Reports

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

**To refresh the list of reports**

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

### 8.2.3. Add Report

Use this task to add a custom report.

**To add a report**

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

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

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

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

**Tip:** Click the + (plus sign) icon to add additional filters.
8) Click Next.
9) Complete the following fields:

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

10) Click Save.

**8.2.4. Copy Report**

Use this task to copy a report.

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

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

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

**8.2.5. Edit Report**

Use this task to edit a custom report.

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

**To view the report details**
1) Access the Reports interface.
2) Click the Action button beside the report you want to edit.
3) Select Edit.
4) Make the necessary modifications.
Note: The edit option is only available (enabled) for custom reports.

8.2.6. Delete Report

Use this task to delete a report.

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

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

To delete a report

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

8.2.7. Run Report

Use this task to run a report.

To run a report

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

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

5) Click Run Now.

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

Use this task to run a report.

8.2.8. Schedule Report

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

To schedule a report

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

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

5) Click Save.

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

See also

Manage Server Activities

### 8.2.9. Schedule Report Email Notification

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

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

To schedule an email

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

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

4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Format</td>
<td>Select the desired report format from the options available (e.g., PDF, CSV)</td>
</tr>
<tr>
<td>Always Recipients</td>
<td>Select the desire &quot;always&quot; recipient. The user(s) you select in this field will always receive an email when the report is run. You have the following options: <strong>User:</strong> Click the dropdown arrow beside a user group (role) to send an email to specific users <strong>User Group (Role):</strong> Click the Select option beside a user group (role) to send an email to all members of a user group</td>
</tr>
</tbody>
</table>
### Field Description

**Alert Criteria**

This field consists of two parts:

- **Expression**: Select a comparison operator (e.g., =, <=, >=)
- **Number**: Enter the number of report rows

**Note**: When the number of rows in a generated report matches the alert criteria defined, the system sends the report via email to the designated recipients.

---

**Security Recipients**

Select the desired "security" recipient. The user(s) you select in this field will only receive an email when the alert criteria is met.

You have the following options:

- **User**: Click the dropdown arrow beside a user group (role) to send an email to specific users
- **User Group (Role)**: Click the Select option beside a user group (role) to send an email to all members of a user group

5) **Click Save.**

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

---

**See also**

- Report Management
- Manage Report Activities
- Manage Settings

### 8.3. Manage Report Cards

Use this task to do the following:

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

### 8.3.1. Display List of Report Cards

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

**To display the list of reports**

1) Expand the **Reporting** menu in the left pane.
2) Click on **Report Cards**.
Note: The Report Cards interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Report category (i.e., Resource, Profile, Configuration, etc.)</td>
</tr>
<tr>
<td>Report Card Name</td>
<td>Name assigned to the report</td>
</tr>
<tr>
<td>Built-in</td>
<td>Y (Yes): Pre-built report card delivered as part of the product</td>
</tr>
<tr>
<td></td>
<td>N (No): Custom report card</td>
</tr>
<tr>
<td></td>
<td>Note: An N (No) appears in this column for all report cards you create</td>
</tr>
<tr>
<td>Action</td>
<td>Click on the Action button to see the list of tasks you can perform for the associated report (e.g., copy, run, schedule, etc.)</td>
</tr>
</tbody>
</table>

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

### 8.3.2. Refresh List of Report Cards

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

To refresh the list of report cards
1) Access the Report Cards interface.
2) Click the Refresh button.

### 8.3.3. View Report Card Details

Use this task to view the report card details.

To view the report card details
1) Access the Report Cards interface.
2) Click the Action button.
3) Select View Details.

### 8.3.4. Add a Report Card

Use this task to create a report card.

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

To add a report card
1) Access the Report Cards interface.
2) Click the Add button.
3) Complete the following fields:
### Field | Description
--- | ---
Card Name | Name you want to assign the report card
Category | Name of report category to which the report will be classified (e.g., Network, Profile, Configuration, Resource)

**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:

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

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

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

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

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

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

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

8) Click **Save**.

See also
- Add Exceptions to Report Card
- Edit Report Defaults

### 8.3.5. Copy Report Card

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

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

Use this task to edit a custom report card.

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

To edit a report card

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

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

8.3.7. Delete Report Card

Use this task to delete a report card.

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

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

To delete a report card

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

8.3.8. Schedule Report Card

Use this task to schedule a report card to run.

To schedule a report card

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

Note: The Schedule Report dialog is displayed.

4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which you want to run the report</td>
</tr>
<tr>
<td></td>
<td>Tip: The Server field will not appear if a report is available only on a single server.</td>
</tr>
<tr>
<td>Start Date</td>
<td>Start date on which to begin reporting</td>
</tr>
<tr>
<td>End Date</td>
<td>End date on which to begin reporting</td>
</tr>
<tr>
<td>Frequency</td>
<td>How often the report card should run within the designated start and end date</td>
</tr>
<tr>
<td></td>
<td>Ad-hoc - Once on a specific day and time</td>
</tr>
</tbody>
</table>
### Schedule Report Card Email Notification

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

**Tip:** In addition, you can email a generated report card at any time. See [Email_Report_Card_Notification](#) for additional information.

#### To email a report card when specific criteria is met

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

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

4. Complete the following fields:

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

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 (TBD). See Edit Mail Server Details for additional information about the email server size limit.

8.3.10. Run Report Card

Use this task to run the report card.

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

To run a report card

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which you want to run the report card</td>
</tr>
</tbody>
</table>

5) Click Run Now.

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

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

See also

Activity Management

8.3.11. Add Exceptions to Report Card

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

Example usage:

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

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

To add an exception to a report card

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

See also

Report Management
Manage Report Activities
Manage Settings
9. Activity

9.1. Activity Management

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

- Manage report activities
- Manager server activities

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

See also
User Permissions

9.2. Manage Report Activities

Use this task to do the following:

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

9.2.1. Display List of Report Activities

Use this task to view the list of report activities.

To display list of report activities

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

Note: The Report Activity interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Name of user whom ran the report or report card last or the word &quot;SCHEDULED&quot; will appear in this field to indicate that this was a scheduled report</td>
</tr>
<tr>
<td>Server</td>
<td>Server from which the report data was obtained</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
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

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of the activity:</td>
<td></td>
</tr>
<tr>
<td>Completed</td>
<td>Successful run</td>
</tr>
<tr>
<td>Processing</td>
<td>In process (with percent complete)</td>
</tr>
<tr>
<td>Error</td>
<td>An error stopped the report from completing</td>
</tr>
</tbody>
</table>

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

### 9.2.2. Refresh List of Report Activities

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

**To refresh list of report activities**

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

### 9.2.3. View Report as HTML

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

**To view as HTML**

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

### 9.2.4. View Report as PDF

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

**To view as PDF**

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

### 9.2.5. View Report Messages

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

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

9.2.6. View Report Card Details

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

To view report card details

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

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

4) Click on a report to view the details.

9.2.7. Email Report Notification

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

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

To email a report

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

Note: The Email Report dialog box is displayed.

4) Complete the following fields:

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

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 (TBD). See Edit Mail Server Details for additional information about the email server size limit.

9.2.8. Email Report Card Notification

Use this task to email a report to a designated recipient.
**Tip:** Alternatively, you can schedule emails to generate automatically each time a report card is run. See [Schedule Report Card Email Notification](#) for additional information.

**To email a report card**

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

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

4) Complete the following fields:

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

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 (TBD). See [Edit Mail Server Details](#) for additional information about the email server size limit.

**9.2.9. Export Report as CSV**

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

**To export as CSV file**

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

**9.2.10. Delete Report from List of Activities**

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

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

**To delete a report activity**

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

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

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

To delete a report activity

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

9.2.12. Run Delta Report

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

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

To run a delta report

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

Note: The Select Report dialog is displayed.

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

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

See also

Manage Reports
Manage Report Cards
Manage Settings

9.3. Manage Server Activities

Use this task to do the following:

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

9.3.1. Display List of Sever Activities

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

To display the list of activities

1) Expand the Activity menu in the left pane.
2) Click the Activity tab.
Note: The Server Activity interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Name of the user who performed the activity</td>
</tr>
<tr>
<td>Server</td>
<td>Server on which the activity was performed</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the activity</td>
</tr>
<tr>
<td>Date</td>
<td>Date on which the activity was performed</td>
</tr>
<tr>
<td>Type</td>
<td>Type of activity:</td>
</tr>
<tr>
<td></td>
<td>JAM - Activity involving a job activity rule</td>
</tr>
<tr>
<td></td>
<td>Report - Activity involving a report</td>
</tr>
<tr>
<td></td>
<td>Report Card - Activity involving a report card</td>
</tr>
<tr>
<td></td>
<td>User - Activity involving a user group</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the activity:</td>
</tr>
<tr>
<td></td>
<td>Completed - Successful run</td>
</tr>
<tr>
<td></td>
<td>Processing - In process (with percent complete)</td>
</tr>
<tr>
<td></td>
<td>Error - An error stopped the report from completing</td>
</tr>
</tbody>
</table>

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

9.3.2. Refresh List of Server Activities

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

To refresh the list of activities
1) Access the Activity interface.
2) Click the Activity tab.
3) Click the Refresh button.

9.3.3. Search List of Server Activities

Use this search for a specific activity.

To search the list of activities
1) Access the Activity interface.
2) Click the Activity tab.
3) Enter the desired search term in the Search field.

See also
Manage Report Activities
Manage Reports
10. Real Time Events

10.1. Real Time Event Management

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

- Manage Network Activity
- Manage Job Activity

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

See also
User Permissions

10.2. Manage Network Activity

This section describes working network activities.

Use this task to do the following:

- Display list of network activities
- Refresh list of network activities
- Search network activities

10.2.1. Display List of Network Activities

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

To display the list of network activities

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the activity was performed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of activity:</td>
</tr>
<tr>
<td></td>
<td>JAM - Activity involving a job activity rule</td>
</tr>
<tr>
<td></td>
<td>Report - Activity involving a report</td>
</tr>
<tr>
<td></td>
<td>Report Card - Activity involving a report card</td>
</tr>
<tr>
<td></td>
<td>User - Activity involving a user group</td>
</tr>
<tr>
<td>User</td>
<td>Name of user performed the activity</td>
</tr>
</tbody>
</table>
Tip: Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order.

## 10.2.2. Refresh List of Network Activities

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

**To refresh the list of activities**

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

## 10.2.3. Search List of Network Activities

Use this 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.

See also

Real Time Event Management
10.3. Manage Job Activity

This section describes working job activities.

Use this task to do the following:
- Display list of job activities
- Refresh list of job activities
- Search job activities

10.3.1. Display List of Job Activities

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

To display the list of job activities

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

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

3) Select the desired server group to display a list of server members in the bottom pane.
4) Select the desired server.
5) Select the Activity tab to display the list of job activities associated with the selected server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server on which the activity was performed</td>
</tr>
<tr>
<td>Report Name</td>
<td>Name of the report or report card generated</td>
</tr>
<tr>
<td>Date</td>
<td>Date on which the report or report card was run</td>
</tr>
</tbody>
</table>
| Status    | Status of the activity: Completed - Successful run  
|           | Processing - In process (with percent complete)     
|           | Error - An error stopped the report from completing |
| Action    | Click on the Action button to see the list of tasks you can perform for the associated report/report card |

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

10.3.2. Refresh List of Job Activities

Use this task at any time to refresh the list of job activities. 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 Job Activity.
3) Click the Refresh button.

### 10.3.3. Search List of Job Activities

Use this search for a specific activity.

*To search the list of activities*

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

*See also*

[Real Time Event Management](#)
11. Admin

11.1. Administration Management

This section describes how to manage TGCentral users, which is separate and distinct from the management of IBM i users.

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

Use this feature to do the following:

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

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

See also

User Permissions

11.2. Manage Users

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

Use this task to do the following:

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

11.2.1. Display List of Users

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

To display the list of users

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

Note: The Users interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Login ID assigned to the TGCentral user</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>Full name of user</td>
</tr>
</tbody>
</table>
| Email | User's email address  
**Note:** This will be used for notifications. |
| Group | TGCentral group to which the user is assigned |
| Role | TGCentral role to which the user is assigned  
**Tip:** A user's [permission level](#) is dependent on the role assigned to the user. |
| Language | Language in which interface text should be presented |
| Date | Date on which the user was granted access (added) to TGCentral |
| Action | Click on the **Action** button to see the list of tasks you can perform for the associated user  
**Tip:** Click on a column heading to sort the column items in ascending order. Click a heading again to sort the items in descending order. |

**See also**

[User Permissions](#)

### 11.2.2. Add User

Use this task to add a new TGCentral user.

**To add a user**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>ID you want to assign the new user</td>
</tr>
<tr>
<td>Full Name</td>
<td>Full name of user</td>
</tr>
</tbody>
</table>
| Email | User's email address  
**Note:** This will be used for notifications. |
| Password | Initial password assigned to the user  
**Note:** The user should change the password immediately. |
| Server Group | TGCentral group to which the user is assigned |
| Role | TGCentral role to which the user is assigned  
**Tip:** A user's [permission level](#) is dependent on the role assigned to the user. |
| Language | Language in which interface text should be presented |
| Allow Multiple Access | Select the appropriate option:  
Yes - Allow the user to log in from different machines concurrently  
No - Do not allow the user to log in from different machines concurrently |
4) Click Save.

See also
User Permissions

11.2.3. Edit User
Use this task to edit an existing TGCentral user.

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

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

To disable a user
1) Access the Users interface.
2) Click the Action button.
3) Select Disable User.

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

To enable a user
1) Access the Users interface.
2) Click the Action button.
3) Select Enable User.

11.2.6. Delete User
Use this task to delete a TGCentral user.

To delete a user
1) Access the Users interface.
2) Click the Action button.
3) Select Delete User.

See also
User Permissions
Administration Management
11.3. Manage Roles

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

Use this task to do the following:

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

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

### 11.3.1. Display List of Roles

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

**To display the list of roles**

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

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

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

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

### 11.3.2. Add Role

Use this task to add a new TGCentral role.

**To add a role**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name you want to assign the role (30-character max)</td>
</tr>
<tr>
<td>Description</td>
<td>Description of role (100-character max)</td>
</tr>
</tbody>
</table>

4) Click **Save**.

### 11.3.3. Copy Role

Use this task to clone a TGCentral role.

**To clone a role**

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

### 11.3.4. Edit Role Name

Use this task 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**.

### 11.3.5. Edit Role Permissions

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

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

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

**To edit the role permissions**

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

See also
11.3.6. Delete Role

Use this task to delete a TGCentral role.

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

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

To delete a role

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

See also

User Permissions
Administration Management

11.4. Manage Settings

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

In addition, not all user roles have access to this interface. If you are unable to access the Admin feature, contact your system administrator.

Use this task to do the following:

- Chose color theme
- Edit color scheme
- Reset color scheme to default
- Display custom SSL certificate
- Edit database password
- Edit PDF settings
- Edit mail server details

11.4.1. Chose Color Theme

Use this task to change the user interface 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 setting tab.
4) Select the desired theme from list available.

11.4.2. Edit Color Scheme of Delta Report

Use this task to modify the color scheme used to represent different element in the delta report.
**To modify the color scheme**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Added</td>
<td>Enter the HEX (hexadecimal) color you want to use in the delta report to represent added records</td>
</tr>
<tr>
<td>Record Deleted</td>
<td>Enter the HEX color you want to use in the delta report to represent delete records</td>
</tr>
<tr>
<td>Update Before</td>
<td>Enter the HEX color you want to use in the delta report to represent data before it is modified</td>
</tr>
<tr>
<td>Update After</td>
<td>Enter the HEX color you want to use in the delta report to represent data after it is modified</td>
</tr>
</tbody>
</table>
5) Click Save.

**11.4.3. Reset Color Scheme to Default**

Use this task to reset the color scheme used in the delta report back to the default color scheme.

**To reset the color scheme**

1) Expand the Admin menu in the left pane.
2) Click on Settings.
3) Click on the Color Scheme tab.
4) Click on the Restore Default.

**11.4.4. Display Custom SSL Certificate**

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

**To display a custom SSL Certificate**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File</td>
<td>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.</td>
</tr>
<tr>
<td>Private Key</td>
<td>The path to the client-specific private key. This is a text file that generates the digital signature.</td>
</tr>
</tbody>
</table>

**11.4.5. Edit Database Password**

Use this task to change the password used by the administrator to access the TGCentral database.
To modify the database password
1) Expand the Admin menu in the left pane.
2) Click on Settings.
3) Click on the Database tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Password</td>
<td>Enter the new database password</td>
</tr>
<tr>
<td>Repeat Database Password</td>
<td>Enter the new database password again for verification purposes</td>
</tr>
</tbody>
</table>

4) Click Change Database Password.

11.4.6. Edit PDF Settings

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

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

11.4.7. 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.

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

5) Click Save.
11.5. Manage Agent Configuration

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

Use this task to import or export the following:

**Job Activity Monitor**
- Activity monitor rules
- Subsystems
- Commands

**Groups**
- User groups
- Network/server groups
- Object groups

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

**Access Escalation Management (AEM)**
- Entitlements
- Access controls
- File editors
- AEM defaults

**Calendar**
- Calendar

11.5.1. Import Agent Configuration

To import the agent configuration
1) Expand the Admin menu (in the left pane).
2) Select Import/Export Agent Config.
Note: The Import/Export Agent Configuration interface is displayed in the right pane.

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

11.5.2. Export Agent Configuration

Use this task to export the following:

To import the agent configuration
1) Expand the Admin menu (in the left pane).
2) Select Import/Export Agent Config.

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

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

See also

User Permissions
Administration Management
12. Troubleshooting

12.1. FAQs

Where is the log file stored?
How do I adjust the log levels?
How do I change the SSL certificate?
What if the TGCentral logon page doesn't appear after installation on a Linux server?
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 (processing)?
What if I do if my PostgreSQL is corrupted?
Which TGCentral files should I backup on a daily basis?

12.1.1. Where are the log files stored?

Trinity Guard Log Files
The log files are stored in the following directory: /Trinityguard/Logs/
This directory stores the log file that track the events that occur between the middle tier and the IBM i server.
In this directory, you should find the following 4 log files:
  - tgagent.log — Identifies requests made by the agent to TGCentral and includes information about the routing of those requests
  - tgrequest.log — Information about the execution (running) of reports and report cards on the agent
  - tgtasks.log — Information about the creation of reports and report cards created on the agent
  - tgjam_sync.log — Information about the Job Activity Monitor (JAM), including the import/export of job activity rules

TGCentral Log Files
The log files are stored in the following directory: /TGCentral-1.XX/log/
This directory stores the log file that track the events that occur between the GUI and the middle tier.
In this directory, you should find the following log file:
  - tgcentral.log
12.1.2. How do I adjust the log levels?

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

Use this task to adjust the log levels. By default, only CRITICAL issues are logged. If you would like lower the log lever (include more issues), you must adjust the log level.

**Note:** The log files have a max size in bytes of 1,024,000 with a backup count of 5. The rotation process is automatic.

To adjust the log levels

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

**Note:** The **TGCentral Configuration** interface is displayed.
5) Enter the desired log level in the **Log Status** field.

**Note:** By default, the log status is set to **CRITICAL**.

12.1.2.2. Adjust TGCentral Log Files Located on Windows Machine

To adjust the TGCentral log file:

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

12.1.2.3. Adjust TGCentral Log Files Located on Linux Machine

To adjust the TGCentral log file

1) From the command line, enter the following:
   ```
   cd tgcentral-1.x.x
   ```
2) From the command line, enter the following:
   ```
   sudo nano tgcentral.conf
   ```
3) Edit the parameters as necessary.
4) Press **Ctrl + x**.
5) Press **y** to save the changes.
6) **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.

12.1.2.4. Adjust TGCentral Log Files Located on Windows Machine

To adjust the TGCentral log file
1) From the command line, enter the following:
   cd tgcentral-1.x.x
2) From the command line, enter the following:
   sudo nano tgcentral.conf
3) Edit the parameters as necessary.

### 12.1.3. How do I change the SSL certificate?

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

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

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

#### 12.1.4.1. Linux Installation

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

To troubleshoot the missing TGCentral logon page on a Linux machine
1) Ensure that the "tgcentral" process is running by executing the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>ps -A</td>
<td>grep tgcentral</td>
</tr>
</tbody>
</table>

   `tguser@tgubuntu1:~/tgcentral-1.1.11$ ps -A | grep tgcentral
   1365 pts/0 00:00:29 tgcentral` 

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

   `sudo sh start.sh`

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>sudo service postgresql status</td>
<td>Your results will not be identical, but should look similar to the following:</td>
</tr>
</tbody>
</table>
4) If the service is not running, access the terminal and use the following command:

```bash
sudo service postgresql start
```

### 12.1.4.2. Windows Installation

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

To troubleshoot the missing TGCentral logon page on a Windows machine

1) On your keyboard press, the **Windows** key + **R**.

**Note:** The Run dialog appears.

2) In the **Open** field, enter `services.msc`.

**Note:** The Services dialog appears.

3) Locate the following services and validate that the services are running:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status must be</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL</td>
<td>Running</td>
</tr>
<tr>
<td>TGCentral</td>
<td>Running</td>
</tr>
</tbody>
</table>

3) If they are not running, right click the service and select **Start**.

### 12.1.5. What do I do if the TGCentral install fails?

Use this task when your install fails.

To troubleshoot the TGCentral installation

1) Ensure all system requirement have been met.

**Note:** See the TGCentral Installation guide for prerequisites, which is available from the Customer Portal at [TrinityGuard.com](http://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](http://TrinityGuard.com).
12.1.6. What if TGCentral won't load on a user's machine?

Use this task if you are unable to connect to the TGCentral server.

**Note:** Complete these steps on the server on which TGCentral is installed.

1) Access the Control Panel.
2) Select System and Security.
3) Select Windows Firewall.
4) Select Allow an app or feature through Windows Firewall.
5) Click Change settings.
6) Click Allow another app.
7) Click Browse.
8) Navigate to the directory in which TGCentral is installed (main directory), and choose *tg.exe* to add it to the list of allowed apps.
9) Once you add *tg.exe* to the list, check (select) all three options: Domain, Private, Public.
10) Click OK.

**Note:** If you are using Linux, complete similar steps according to your firewall configuration. Ensure that your firewall is not excluding the *tgcentral* service on Linux.

12.1.7. What if I forget my admin password?

Unfortunately, the admin password is encrypted and cannot be retrieved if lost. Companies often have security policies that address the preservation and tracking of administrative passwords; therefore, contact your local security officer for assistance.

12.1.8. What if a report won't stop running?

Use this task to stop a report from running and to diagnose what might be causing the delay.

**To stop a report from running:**

1) Log into TGCentral.
2) In the left pane, select Activity.

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

3) Click the Action button beside the report that shows the status of Processing.
4) Select Delete.

**Option 1: Message Wait (MSGW)**

**To diagnose if the message wait (MSGW) time is causing the issue:**

1) Sign into your IBM i server.
2) At the Selection or command prompt, enter WRKACTJOB SBS(TGCMN) to access a list of working jobs.

**Note:** The Work with Activity Jobs interface is displayed.

3) Locate any jobs with the status MSGW (message wait).
4) In the Opt column beside the job, enter 7 (Display message).
5) Enter *NOMAX*
6) Press Enter.

**Note:** This changes the message wait time to *NOMAX.*
Option 2: Print file (PRTF)

To diagnose if the print file (PRTF) is causing the issue:
1) Sign into your IBM i server.
2) At the Selection or command prompt, enter CHGPRTF FILE(QPRINT) MAXRCDS(*NOMAX).
   Note: This changes the printer file size to *NOMAX.

Option 3: Log File (LOGCLPGM)

To diagnose if the log file (LOGCLPGM) is causing the issue:
1) Sign into your IBM i server.
2) At the Selection or command prompt, enter JOBD(TGPROD/TGAGENT) LOG(0 99 *NOLIST) LOGCLPGM(*NO) and JOBD(TGPROD/TGREQUEST) LOG(0 99 *NOLIST) LOGCLPGM(*NO).
   Note: This change the log level of the job descriptions (TGREQUEST and TGAGENT in library TGPROD) to the minimum.

12.1.9. What if I do if my PostgreSQL is corrupted?

   Restore tgcentraldb database. For more information, refer to the PostgreSQL documentation.

12.1.10. Which TGCentral files should I backup on a daily basis?

   Follow the recommends provided by your security office. However, for your convenience, we recommend that you include the following in your regular backup procedures:
   - Config files
   - Database files
   - Logs files
# 13. APPENDIX - Collectors

<table>
<thead>
<tr>
<th>Collector Category</th>
<th>Collector Name</th>
<th>Collector ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Active job information</td>
<td>QSYS2.ACTIVE_JOB_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Active memory pools</td>
<td>QSYS2.MEMORY_POOL_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Alternate subsystem configurations</td>
<td>QSYS2.SERVER_SBS_ROUTING</td>
</tr>
<tr>
<td>Configuration</td>
<td>Columns with field procedures</td>
<td>SYSFIELDS</td>
</tr>
<tr>
<td>Configuration</td>
<td>Current job's reply list entry information</td>
<td>QSYS2.REPLY_LIST_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Dependencies of row permissions and column masks</td>
<td>SYSCONTROLSDEP</td>
</tr>
<tr>
<td>Configuration</td>
<td>Disk Information</td>
<td>QSYS2.SYSDISKSTAT</td>
</tr>
<tr>
<td>Configuration</td>
<td>DRDA and DDM User access</td>
<td>QSYS2.DRDA_AUTHENTICATION</td>
</tr>
<tr>
<td>Configuration</td>
<td>Function usage identifiers</td>
<td>QSYS2.FUNCTION_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Function usage configuration details.</td>
<td>QSYS2.FUNCTION_USAGE</td>
</tr>
<tr>
<td>Configuration</td>
<td>Group PTFs Information</td>
<td>QSYS2.GROUP_PTF_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>IBM i temporary storage pool detail</td>
<td>QSYS2.SYSTMPSTG</td>
</tr>
<tr>
<td>Configuration</td>
<td>IPv4 and IPv6 network connection details.</td>
<td>QSYS2.NETSTAT_JOB_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Job Description Data</td>
<td>JOB_DESCRIPTIONS</td>
</tr>
<tr>
<td>Configuration</td>
<td>Job Schedule Entry information</td>
<td>QSYS2.SCHEDULED_JOB_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Journal and remote journal information</td>
<td>QSYS2.JOURNAL_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>KeyStore</td>
<td>Keystore_Data</td>
</tr>
<tr>
<td>Configuration</td>
<td>Memory pool details</td>
<td>QSYS2.MEMORY_POOL</td>
</tr>
<tr>
<td>Configuration</td>
<td>Media Library Status details</td>
<td>QSYS2.MEDIA_LIBRARY_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Message Queue Information</td>
<td>MESSAGE_QUEUE</td>
</tr>
<tr>
<td>Configuration</td>
<td>Object lock information</td>
<td>QSYS2.OBJECT_LOCK_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Output Queue Information</td>
<td>OUTPUT_QUEUE</td>
</tr>
<tr>
<td>Configuration</td>
<td>Partition information</td>
<td>QSYS2.SYSTEM_STATUS_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Permission or column mask defined</td>
<td>SYSCONTROLS</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a column</td>
<td>SYSCOLAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a package</td>
<td>SYSPACKAGEAUTH</td>
</tr>
<tr>
<td>Collector Category</td>
<td>Collector Name</td>
<td>Collector ID</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a routine</td>
<td>SYSRoutineAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a row</td>
<td>SYSSControlDEP</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a schema</td>
<td>SYSSchemaAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a sequence</td>
<td>SYSSequenceAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a table or view</td>
<td>SYSTableAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a type</td>
<td>SYSSdtaUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on a global variable</td>
<td>SYSSvariableAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Privileges granted on an XML schema</td>
<td>SYSSxROBJECTAUTH</td>
</tr>
<tr>
<td>Configuration</td>
<td>Products license information.</td>
<td>QSYS2.LICENSE_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Program, service program, and module with SQL statements</td>
<td>SYSPROgramSTAT</td>
</tr>
<tr>
<td>Configuration</td>
<td>PTF Groups installed per IBM Recommendations</td>
<td>SYSTOOLS.GROUP_PTF_CURRENCY</td>
</tr>
<tr>
<td>Configuration</td>
<td>PTFs within PTF Groups installed per IBM Recommendations</td>
<td>SYSTOOLS.GROUP_PTF_DETAILS</td>
</tr>
<tr>
<td>Configuration</td>
<td>Record lock information</td>
<td>QSYS2.RECORD_LOCK_INFO</td>
</tr>
<tr>
<td>Configuration</td>
<td>Spooled file in output queue</td>
<td>QSYS2.OUTPUT_QUEUE_ENTRIES</td>
</tr>
<tr>
<td>Configuration</td>
<td>Storage usage by user profile</td>
<td>QSYS2.USER_STORAGE</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Autostart Jobs</td>
<td>SUBSYSTEM_AUTOSTART</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Communication Entries</td>
<td>SUBSYSTEM_COMMUNICATIONS</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Information Details</td>
<td>SUBSYSTEM_INFORMATION</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Job Queue</td>
<td>SUBSYSTEM_JOB_QUEUE</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Pool Data</td>
<td>SUBSYSTEM_POOL_DATA</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Prestart Jobs</td>
<td>SUBSYSTEM_PRESTART</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Remote Entries</td>
<td>SUBSYSTEM_REMOTE</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Routing Entries</td>
<td>SUBSYSTEM_ROUTING</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Workstation Names</td>
<td>SUBSYSTEM_WORKSTATION_NAMES</td>
</tr>
<tr>
<td>Configuration</td>
<td>Subsystem Workstation Types</td>
<td>SUBSYSTEM_WORKSTATION_TYPES</td>
</tr>
<tr>
<td>Configuration</td>
<td>Table statistics include all partitions and members</td>
<td>SYSTableSTAT</td>
</tr>
<tr>
<td>Configuration</td>
<td>User Profile Information</td>
<td>QSYS2.USER_INFO</td>
</tr>
<tr>
<td>DataAudit</td>
<td>Audit data area changes</td>
<td>DATA_AREA_AUDITING</td>
</tr>
<tr>
<td>DataAudit</td>
<td>Monitor Database changes</td>
<td>DATABASE_AUDITING</td>
</tr>
<tr>
<td>Collector Category</td>
<td>Collector Name</td>
<td>Collector ID</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>IFS</td>
<td>Display extended journaling information for the IFS object</td>
<td>IFS_JOURNALINGj</td>
</tr>
<tr>
<td>IFS</td>
<td>Display status information about an IFS file</td>
<td>IFS_STATUS</td>
</tr>
<tr>
<td>IFS</td>
<td>Display the attributes for the IFS objects</td>
<td>IFS_ATTRIBUTES</td>
</tr>
<tr>
<td>IFS</td>
<td>Display the public and private authorities associated with the object</td>
<td>IFSAuthorities</td>
</tr>
<tr>
<td>Journal</td>
<td>Access Control List Changes</td>
<td>JOURNAL_VA</td>
</tr>
<tr>
<td>Journal</td>
<td>Actions on Validation Lists</td>
<td>JOURNAL_VO</td>
</tr>
<tr>
<td>Journal</td>
<td>Actions to IP Rules</td>
<td>JOURNAL_IR</td>
</tr>
<tr>
<td>Journal</td>
<td>APPN Endpoint Filter Violations</td>
<td>JOURNAL_NE</td>
</tr>
<tr>
<td>Journal</td>
<td>Asynchronous Signals Processed</td>
<td>JOURNAL_SG</td>
</tr>
<tr>
<td>Journal</td>
<td>Authority Changes to Restored Objects</td>
<td>JOURNAL_RA</td>
</tr>
<tr>
<td>Journal</td>
<td>Authority Collection Data</td>
<td>AUTHORITY_COLLECTION</td>
</tr>
<tr>
<td>Journal</td>
<td>Authority Failures</td>
<td>JOURNAL_AF</td>
</tr>
<tr>
<td>Journal</td>
<td>Authority Restored for User Profiles</td>
<td>JOURNAL_RU</td>
</tr>
<tr>
<td>Journal</td>
<td>Authorization List or Object Authority Changes</td>
<td>JOURNAL_CA</td>
</tr>
<tr>
<td>Journal</td>
<td>Change Request Descriptor Changes</td>
<td>JOURNAL_CQ</td>
</tr>
<tr>
<td>Journal</td>
<td>Change Request Descriptors Restored</td>
<td>JOURNAL_RQ</td>
</tr>
<tr>
<td>Journal</td>
<td>Changes to Service Tools Profiles</td>
<td>JOURNAL_DS</td>
</tr>
<tr>
<td>Journal</td>
<td>Close Operations on Server Files</td>
<td>JOURNAL_VF</td>
</tr>
<tr>
<td>Journal</td>
<td>Cluster Operation</td>
<td>JOURNAL_CU</td>
</tr>
<tr>
<td>Journal</td>
<td>Commands Executed</td>
<td>JOURNAL_CD</td>
</tr>
<tr>
<td>Journal</td>
<td>Connection Verification</td>
<td>JOURNAL_CV</td>
</tr>
<tr>
<td>Journal</td>
<td>Connections Started, Ended, or Rejected</td>
<td>JOURNAL_VC</td>
</tr>
<tr>
<td>Journal</td>
<td>Create Operations</td>
<td>JOURNAL_CO</td>
</tr>
<tr>
<td>Journal</td>
<td>Cryptographic Configuration Changes</td>
<td>JOURNAL_CY</td>
</tr>
<tr>
<td>Journal</td>
<td>Delete Operations</td>
<td>JOURNAL_DO</td>
</tr>
<tr>
<td>Journal</td>
<td>Directory Link, Unlink, and Search Operations</td>
<td>JOURNAL_LD</td>
</tr>
<tr>
<td>Journal</td>
<td>Directory Search Violations</td>
<td>JOURNAL_ND</td>
</tr>
<tr>
<td>Journal</td>
<td>Directory Server Extensions</td>
<td>JOURNAL_XD</td>
</tr>
<tr>
<td>Journal</td>
<td>DLO Object Changes</td>
<td>JOURNAL_YC</td>
</tr>
<tr>
<td>Journal</td>
<td>DLO Object Reads</td>
<td>JOURNAL_YR</td>
</tr>
<tr>
<td>Collector Category</td>
<td>Collector Name</td>
<td>Collector ID</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Journal</td>
<td>Dual Optical Object Accesses</td>
<td>JOURNAL_O2</td>
</tr>
<tr>
<td>Journal</td>
<td>EIM Attribute Changes</td>
<td>JOURNAL_AU</td>
</tr>
<tr>
<td>Journal</td>
<td>Environment Variable Changes</td>
<td>JOURNAL_EV</td>
</tr>
<tr>
<td>Journal</td>
<td>Exceeded Account Limit Events</td>
<td>JOURNAL_VL</td>
</tr>
<tr>
<td>Journal</td>
<td>Exit Point Maintenance Operations</td>
<td>JOURNAL_GR</td>
</tr>
<tr>
<td>Journal</td>
<td>Identity Token Events</td>
<td>JOURNAL_X1</td>
</tr>
<tr>
<td>Journal</td>
<td>Internet Security Management Events</td>
<td>JOURNAL_IS</td>
</tr>
<tr>
<td>Journal</td>
<td>Inter-process Communication Events</td>
<td>JOURNAL_IP</td>
</tr>
<tr>
<td>Journal</td>
<td>Intrusion Monitor Events</td>
<td>JOURNAL_IM</td>
</tr>
<tr>
<td>Journal</td>
<td>Invalid Sign-on Attempts</td>
<td>JOURNAL_PW</td>
</tr>
<tr>
<td>Journal</td>
<td>Job Changes</td>
<td>JOURNAL_JS</td>
</tr>
<tr>
<td>Journal</td>
<td>Job Descriptions – USER Parameter Changes</td>
<td>JOURNAL_ID</td>
</tr>
<tr>
<td>Journal</td>
<td>Job Descriptions that Contain User Profile Names were Restored</td>
<td>JOURNAL_RJ</td>
</tr>
<tr>
<td>Journal</td>
<td>Key Ring File Changes</td>
<td>JOURNAL_KF</td>
</tr>
<tr>
<td>Journal</td>
<td>LDAP Operations</td>
<td>JOURNAL_DI</td>
</tr>
<tr>
<td>Journal</td>
<td>Network Attribute Changes</td>
<td>JOURNAL_NA</td>
</tr>
<tr>
<td>Journal</td>
<td>Network Authentication Events</td>
<td>JOURNAL_X0</td>
</tr>
<tr>
<td>Journal</td>
<td>Network Log On and Off Events</td>
<td>JOURNAL_VN</td>
</tr>
<tr>
<td>Journal</td>
<td>Network Password Errors</td>
<td>JOURNAL_VP</td>
</tr>
<tr>
<td>Journal</td>
<td>Network Profile Changes</td>
<td>JOURNAL_VU</td>
</tr>
<tr>
<td>Journal</td>
<td>Network Resource Accesses</td>
<td>JOURNAL_VR</td>
</tr>
<tr>
<td>Journal</td>
<td>Object Auditing Attribute Changes</td>
<td>JOURNAL_AD</td>
</tr>
<tr>
<td>Journal</td>
<td>Object Changes</td>
<td>JOURNAL_ZC</td>
</tr>
<tr>
<td>Journal</td>
<td>Object Management Changes</td>
<td>JOURNAL_OM</td>
</tr>
<tr>
<td>Journal</td>
<td>Object Ownership Changes</td>
<td>JOURNAL_OW</td>
</tr>
<tr>
<td>Journal</td>
<td>Object Reads</td>
<td>JOURNAL_ZR</td>
</tr>
<tr>
<td>Journal</td>
<td>Objects Restored</td>
<td>JOURNAL_OR</td>
</tr>
<tr>
<td>Journal</td>
<td>OfficeVision Mail Services Actions</td>
<td>JOURNAL_ML</td>
</tr>
<tr>
<td>Journal</td>
<td>Optical Volume Accesses</td>
<td>JOURNAL_O3</td>
</tr>
<tr>
<td>Journal</td>
<td>Ownership Changes for Restored Objects</td>
<td>JOURNAL_RO</td>
</tr>
<tr>
<td>Collector Category</td>
<td>Collector Name</td>
<td>Collector ID</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Journal</td>
<td>Primary Group Changes</td>
<td>JOURNAL_PG</td>
</tr>
<tr>
<td>Journal</td>
<td>Primary Group Changes for Restored Objects</td>
<td>JOURNAL_RZ</td>
</tr>
<tr>
<td>Journal</td>
<td>Printer Output Changes</td>
<td>JOURNAL_PO</td>
</tr>
<tr>
<td>Journal</td>
<td>Program Changes to Adopt Owner Authority</td>
<td>JOURNAL_PA</td>
</tr>
<tr>
<td>Journal</td>
<td>Programs Restored that Adopt Owner Authority</td>
<td>JOURNAL_RP</td>
</tr>
<tr>
<td>Journal</td>
<td>Programs that Adopt Authority were Executed</td>
<td>JOURNAL_AP</td>
</tr>
<tr>
<td>Journal</td>
<td>PTF Object Changes</td>
<td>JOURNAL_PU</td>
</tr>
<tr>
<td>Journal</td>
<td>PTF Operations</td>
<td>JOURNAL_PF</td>
</tr>
<tr>
<td>Journal</td>
<td>Row and Column Access Control</td>
<td>JOURNAL_AX</td>
</tr>
<tr>
<td>Journal</td>
<td>Secure Socket Connections</td>
<td>JOURNAL_SK</td>
</tr>
<tr>
<td>Journal</td>
<td>Server Security User Information Actions</td>
<td>JOURNAL_SO</td>
</tr>
<tr>
<td>Journal</td>
<td>Server Sessions Started or Ended</td>
<td>JOURNAL_VS</td>
</tr>
<tr>
<td>Journal</td>
<td>Service Status Change Events</td>
<td>JOURNAL_VV</td>
</tr>
<tr>
<td>Journal</td>
<td>Service Tools Actions</td>
<td>JOURNAL_ST</td>
</tr>
<tr>
<td>Journal</td>
<td>Single Optical Object Accesses</td>
<td>JOURNAL_O1</td>
</tr>
<tr>
<td>Journal</td>
<td>Socket Descriptor Details</td>
<td>JOURNAL_GS</td>
</tr>
<tr>
<td>Journal</td>
<td>Spooled File Actions</td>
<td>JOURNAL_SF</td>
</tr>
<tr>
<td>Journal</td>
<td>Subsystem Routing Entry Changes</td>
<td>JOURNAL_SE</td>
</tr>
<tr>
<td>Journal</td>
<td>Swap Profile Events</td>
<td>JOURNAL_PS</td>
</tr>
<tr>
<td>Journal</td>
<td>System Directory Changes</td>
<td>JOURNAL_SD</td>
</tr>
<tr>
<td>Journal</td>
<td>System Values Changes</td>
<td>JOURNAL_SV</td>
</tr>
<tr>
<td>Journal</td>
<td>Systems Management Changes</td>
<td>JOURNAL_SM</td>
</tr>
<tr>
<td>Journal</td>
<td>User Profile Changes</td>
<td>JOURNAL_CP</td>
</tr>
<tr>
<td>Log</td>
<td>Job Log Details</td>
<td>JOB_LOGDETAILS</td>
</tr>
<tr>
<td>Log</td>
<td>Job Log Summary</td>
<td>JOB_LOG_SUMMARY</td>
</tr>
<tr>
<td>Network</td>
<td>Controller Attached Device Information</td>
<td>CONTROLLER_ATTACHED_DEVICES</td>
</tr>
<tr>
<td>Network</td>
<td>Controller Description Information</td>
<td>CONTROLLER_DESCRIPTION_DATA</td>
</tr>
<tr>
<td>Network</td>
<td>Device Description APPC Information</td>
<td>DEVICE_DESCRIPTION_APPC</td>
</tr>
<tr>
<td>Network</td>
<td>Device Description Information</td>
<td>DEVICE_DESCRIPTION_DATA</td>
</tr>
<tr>
<td>Network</td>
<td>Line Description Information</td>
<td>LINE_DESCRIPTION_DATA</td>
</tr>
<tr>
<td>Network</td>
<td>Network Attribute Information</td>
<td>NETWORK_ATTRIBUTES</td>
</tr>
<tr>
<td>Collector Category</td>
<td>Collector Name</td>
<td>Collector ID</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Network</td>
<td>Network Connections Ipv4 and Ipv6</td>
<td>NETWORK CONNECTIONS</td>
</tr>
<tr>
<td>Network</td>
<td>Network Interface Data Ipv4</td>
<td>NETWORK_INTERFACE_IPV4</td>
</tr>
<tr>
<td>Network</td>
<td>Network Interface Data Ipv6</td>
<td>NETWORK_INTERFACE_IPV6</td>
</tr>
<tr>
<td>Network</td>
<td>Network Route Data Ipv4</td>
<td>NETWORK_ROUTE_IPV4</td>
</tr>
<tr>
<td>Network</td>
<td>Network Route Data Ipv6</td>
<td>NETWORK_ROUTE_IPV6</td>
</tr>
<tr>
<td>Network</td>
<td>Network Server Description Data</td>
<td>NETWORK_SERVER DESCRIPTIONS</td>
</tr>
<tr>
<td>Network</td>
<td>Network Server Encryption Status</td>
<td>NETWORK_SVR_ENCRYPT_STATUS</td>
</tr>
<tr>
<td>Network</td>
<td>TCP/IP Ipv4 Stack Attributes</td>
<td>NETWORK_TCPIP_IPV4</td>
</tr>
<tr>
<td>Network</td>
<td>TCP/IP Ipv6 Stack Attributes</td>
<td>NETWORK_TCPIP_IPV6</td>
</tr>
<tr>
<td>Object</td>
<td>Authorized Users through Authorization Lists</td>
<td>AUTH_USERS_VIA_AUTH_LISTS</td>
</tr>
<tr>
<td>Object</td>
<td>Display Field Level Authorities</td>
<td>FIELD_AUTHORITY</td>
</tr>
<tr>
<td>Object</td>
<td>Display Object Authority</td>
<td>OBJECT_AUTHORITY</td>
</tr>
<tr>
<td>Object</td>
<td>Display Object Details</td>
<td>OBJECTDETAILS</td>
</tr>
<tr>
<td>Object</td>
<td>Message Queue Data Details</td>
<td>MESSAGE_QUEUE_DATA</td>
</tr>
<tr>
<td>Object</td>
<td>Program Reference Data</td>
<td>PROGRAM_REFERENCE_DATA</td>
</tr>
<tr>
<td>System</td>
<td>Authority List Data</td>
<td>AUTHORITY_LIST</td>
</tr>
<tr>
<td>System</td>
<td>Basic Information about a software product</td>
<td>PRODUCT_INFO</td>
</tr>
<tr>
<td>System</td>
<td>Display Exit Point Data</td>
<td>EXIT_POINTS</td>
</tr>
<tr>
<td>System</td>
<td>Display System Value Data</td>
<td>SYSTEM_VALUES</td>
</tr>
<tr>
<td>System</td>
<td>Installed Software Resources Data</td>
<td>SOFTWARE RESOURCES</td>
</tr>
<tr>
<td>System</td>
<td>Program Temporary Fix Data</td>
<td>PTF_DATA</td>
</tr>
<tr>
<td>System</td>
<td>Service Tool User Data</td>
<td>SERVICE_TOOL_USERS</td>
</tr>
<tr>
<td>Users</td>
<td>Display User Profile Data</td>
<td>USER_PROFILES</td>
</tr>
<tr>
<td>Users</td>
<td>Programs that Adopt Authority</td>
<td>PROGRAM_ADOPT</td>
</tr>
<tr>
<td>Users</td>
<td>User Profile Object Authorities</td>
<td>USER_OBJECT_AUTHORITIES</td>
</tr>
</tbody>
</table>
# 14. APPENDIX - Permissions

- **Build in roles**
- **Custom roles**

## 14.1. Built-in Roles

**MENUS**

Use the following table to identify access levels for built-in roles.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Management - D(eny)/A(llow)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers Menu</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Servers Group Menu</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Rules - D(eny)/A(llow)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job Activity Monitor</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Job Activity Monitor Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Subsystems</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Commands</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Network Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Socket Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Remote Exit Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Exit Point Config</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Defaults</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access Escalation Mgmt</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Entitlement</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Access Control</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>File Editors</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Defaults</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Groups -**

**D(eny)/A(llow)**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Network Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Operation Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Object Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Reporting -**

**D(eny)/A(llow)**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Menu</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Report Cards Menu</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

**Real Time Events -**

**D(eny)/A(llow)**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Activity</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Alerts</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Admin -**

**D(eny)/A(llow)**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Menu</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Roles Menu</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Settings Menu</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import/Export Agent Conf.</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Add Server</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit IP Address</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Add to Server Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Run Report</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Run Report Card</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Server</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Manage/Unmanaged Server</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>View Report of Report Card</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>View PDF Format</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export CSV</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Run Report or Report Card</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Run Again</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delta Report</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>View Servers Details</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Add Schedule</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Enable/Disable Schedule</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Schedule</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>View Servers Details</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Servers Group**

**Server Management - D(eny)/A(llow)**
<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Server Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Server Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Run Report in Server Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Run Report in Card in Server Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Server Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Rules - D(eny)/A(llow)**

### Job Activity Monitor

#### JAM Rules

<table>
<thead>
<tr>
<th>Action</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

#### Subsystems

<table>
<thead>
<tr>
<th>Action</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

#### Commands

<table>
<thead>
<tr>
<th>Action</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

### Network Security

#### Socket Rules

<table>
<thead>
<tr>
<th>Action</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Remote Exit Rules</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Exit Point Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Exit Program</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Remove Exit Program</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Cycle Server</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Network Security Defaults</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Access Escalation Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Entitlement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>File Editors</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add New</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Access Esc. Defaults**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Groups - D{eny}/A{llow}**

### User Groups

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Group</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Add User</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit User</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete User</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

### Network Groups

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Add Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

### Operation Groups

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Add Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>Object Groups</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Group</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Add Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Detail</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Reporting - D(eny)/A(llow)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Report</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Report Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Edit Report Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Add Report to Schedule</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Copy Report Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Delete Report Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Run Report</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Import</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Export</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Email Report</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td><strong>Report Card</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Report Card Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>View/Edit Report Card Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Add Report Card to Schedule</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Copy Report Card Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Delete Report Card Definition</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Run Report Card</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Import</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Export</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>Email Report Card</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

### Activity - D(eny)/A(llow)

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Report Activity</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>View Activity Log</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>View Messages</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>View Report</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>View Report Card</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>View PDF</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Export CSV</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Delete Run</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Run Again</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delta Reports</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>A</td>
</tr>
<tr>
<td>Email Report</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

### Real Time Events - D(eny)/A(llow)

### Network Activity

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Remote Exit Rule</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

### Admin - D(eny)/A(llow)

### Users

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add User</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit User</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete User</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Enable/Disable User</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>Roles</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Role</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Edit Role</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Delete Role</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Copy Role</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Import/Export Agent Conf.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import Job Activity Rules</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Job Activity Rules</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Job Activity Subsystems</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Job Activity Subsystems</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Job Activity Commands</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Job Activity Commands</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Network Security Socket Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Network Security Socket Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Network Security Remote Exit Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Network Security Remote Exit Rules</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Access Escalation Entitlements</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Access Escalation Entitlements</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Access Escalation Access Control</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Access Escalation Access Control</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import User Groups</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export User Groups</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>Super User</td>
<td>Help Desk</td>
<td>Auditor</td>
<td>Creator</td>
<td>Reader</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Import Network Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Network Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Operation Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Operation Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Object Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Object Groups</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Import Calendar</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Export Calendar</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

### REPORTS AND REPORT CARDS

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E(xclude)/V(iew)/R(un)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category: Configuration</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V</td>
</tr>
<tr>
<td>Category: Log</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>Category: Network</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V</td>
</tr>
<tr>
<td>Category: Profile</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V</td>
</tr>
<tr>
<td>Category: Resource</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V</td>
</tr>
<tr>
<td>Custom Categories</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V/R</td>
<td>V</td>
</tr>
</tbody>
</table>

| **Report Cards**                  |       |            |           |         |         |        |
| E(xclude)/V(iew)/R(un)            |       |            |           |         |         |        |
| Category: Analysis                | V/R   | V/R        | V/R       | V/R     | V/R     | V      |
| Category: IFS Reports             | V/R   | V/R        | V/R       | V/R     | V/R     | V      |
| Category: Regulations             | V/R   | V/R        | V/R       | V/R     | V/R     | V      |
| Custom Categories                 | V/R   | V/R        | V/R       | V/R     | V/R     | V      |
## 14.2. Custom Roles

Use the following table as a template to build custom roles.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>Super User</th>
<th>Help Desk</th>
<th>Auditor</th>
<th>Creator</th>
<th>Reader</th>
</tr>
</thead>
</table>

### 15. APPENDIX - Delta Reports

<table>
<thead>
<tr>
<th>Collector_ID</th>
<th>Report_ID</th>
<th>Correlation Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access_Escal_Acc_Controls</td>
<td>Access_Controls_Config</td>
<td>User Name</td>
</tr>
<tr>
<td>Access_Escal_Defaults</td>
<td>Defaults_Config</td>
<td>Journal Name</td>
</tr>
<tr>
<td>Access_Escal_Entitlements</td>
<td>Entitlements_Config</td>
<td>User Name, Object Name, Object Library, Object Type</td>
</tr>
<tr>
<td>Access_Escal_File_Editors</td>
<td>File_Editors_Config</td>
<td>Edit Command, Edit Library</td>
</tr>
<tr>
<td>Auth_Users_via_Auth_Lists</td>
<td>Auth_Users_via_Auth_Lists</td>
<td>Object, Library, Type, Auth List User</td>
</tr>
<tr>
<td>Blueprint_Auth_Settings_File</td>
<td>Blueprint_Auth_Settings</td>
<td>Blueprint ID, Authority List</td>
</tr>
<tr>
<td>Blueprint_Master</td>
<td>Blueprint_Master</td>
<td>Blueprint ID, User Group</td>
</tr>
<tr>
<td>Blueprint_Non_Compliance_User</td>
<td>Blueprint_Non_Cmpl</td>
<td>Blueprint ID, User Name, Violation Category, Violation Keyword</td>
</tr>
<tr>
<td>Blueprint_Object_Auth_File</td>
<td>Blueprint_Object_Auth_File</td>
<td>Blueprint ID, Profile Object owner</td>
</tr>
<tr>
<td>Blueprint_Parameter_File</td>
<td>Blueprint_Parameter_File</td>
<td>Blueprint ID, User Parameter</td>
</tr>
<tr>
<td>Blueprint_Permissions_File</td>
<td>Blueprint_Permissions_File</td>
<td>Blueprint ID, Authorized User/Group</td>
</tr>
<tr>
<td>Blueprint_3rd_Party_File</td>
<td>Blueprint_3rd_Party_File</td>
<td>Blueprint ID, Script Type, Script Statement</td>
</tr>
<tr>
<td>Controller_Attached_Devices</td>
<td>Controller_Attached_Devices</td>
<td>Device Name, Device Category, Device Type</td>
</tr>
<tr>
<td>Controller_Description_Data</td>
<td>Controller_Description_Data</td>
<td>Controller Name, Controller Category</td>
</tr>
<tr>
<td>Det_Cmd_Rules</td>
<td>Det_Cmd_Rules</td>
<td>Rule ID, Command Name, Command Library, Command User</td>
</tr>
<tr>
<td>Det_Defaults</td>
<td>Det_Defaults</td>
<td>Journal Name</td>
</tr>
<tr>
<td>Det_JrnMon_Alerts</td>
<td>Det_JrnMon_Alerts</td>
<td>Journal Name, Journal Library, Journal Code and Journal Type, Filter Sequence</td>
</tr>
<tr>
<td>Det_Mon_Master</td>
<td>Det_Mon_Master</td>
<td>Monitor Name, Monitor Library, Monitor Type</td>
</tr>
<tr>
<td>Det_Msg_Cmd_Alr</td>
<td>Det_Msg_Cmd_Alr</td>
<td>Monitor Name, Monitor Library, Monitor Type, Rule Name, Alert Sequence</td>
</tr>
<tr>
<td>Collector_ID</td>
<td>Report_ID</td>
<td>Correlation Fields</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Det_Msq_Rules</td>
<td>Det_Msq_Rules</td>
<td>Rule ID, Message Queue, Message Queue Library, Message ID</td>
</tr>
<tr>
<td>Det_SEIM_Providers</td>
<td>Det_SEIM_Providers</td>
<td>syslog provider Name</td>
</tr>
<tr>
<td>Device_Description_APPC</td>
<td>Device_Description_APPC</td>
<td>Device Name, Device Category</td>
</tr>
<tr>
<td>Device_Description_Data</td>
<td>Device_Description_Data</td>
<td>Device Name, Device Category</td>
</tr>
<tr>
<td>ISL_Configuration_Settings</td>
<td>ISL_Configuration</td>
<td>Disconnect Option</td>
</tr>
<tr>
<td>ISL_Disconnect_Options</td>
<td>ISL_Disconnect</td>
<td></td>
</tr>
<tr>
<td>ISL_Rules</td>
<td>ISL_Monitor_Rules</td>
<td>Rule Type, Object Name, Object Library</td>
</tr>
<tr>
<td>Network_Exit_Config</td>
<td>Exit_Point_Config_Report</td>
<td>Server Name, Exit Point, Exit Format</td>
</tr>
<tr>
<td>Network_Svr_Encrypt_Status</td>
<td>Network_Svr_Encrypt_Status</td>
<td>TCPIP App ID</td>
</tr>
<tr>
<td>Profile_Compliance</td>
<td>Profile_Compliance_Report</td>
<td>BluePrint ID, User Name, Violation Category, Violation Keyword</td>
</tr>
<tr>
<td>Profile_Inactivity_Settings</td>
<td>Profile_Inactivity_Settings</td>
<td>Only one record</td>
</tr>
<tr>
<td>Profile_Manager_Defaults</td>
<td>Profile_Manager_Defaults</td>
<td>Only one record</td>
</tr>
<tr>
<td>QSYS2.ACTIVE_JOB_INFO</td>
<td>QSYS2_ACTIVE_JOB_INFO</td>
<td>Job Name</td>
</tr>
<tr>
<td>QSYS2.DRDA_AUTHENTICATION</td>
<td>QSYS2_DRDA_AUTHENTICATION</td>
<td>User Name, Server Name</td>
</tr>
<tr>
<td>QSYS2.FUNCTION_INFO</td>
<td>QSYS2_FUNCTION_INFO</td>
<td>Function ID</td>
</tr>
<tr>
<td>QSYS2.FUNCTION_USAGE</td>
<td>QSYS2_FUNCTION_USAGE</td>
<td>Function ID, User Name</td>
</tr>
<tr>
<td>QSYS2.GROUP_PTF_INFO</td>
<td>QSYS2_GROUP_PTF_INFO</td>
<td>PTF_G00001</td>
</tr>
<tr>
<td>QSYS2.JOURNAL_INFO</td>
<td>QSYS2_JOURNAL_INFO</td>
<td>Journal Name, Journal Library</td>
</tr>
<tr>
<td>QSYS2.LICENSE_INFO</td>
<td>QSYS2_LICENSE_INFO</td>
<td>LICPGM, FEATURE</td>
</tr>
<tr>
<td>QSYS2.MEDIA_LIBRARY_INFO</td>
<td>QSYS2_MEDIA_LIBRARY_INFO</td>
<td>DEVICE, DEVICE TYPE</td>
</tr>
<tr>
<td>QSYS2.MEMORY_POOL</td>
<td>QSYS2_MEMORY_POOL</td>
<td>POOL_NAME</td>
</tr>
<tr>
<td>QSYS2.REPLY_LIST_INFO</td>
<td>QSYS2_REPLY_LIST_INFO</td>
<td>MSGID</td>
</tr>
<tr>
<td>QSYS2.SCHEDULED_JOB_INFO</td>
<td>QSYS2_SCHEDULED_JOB_INFO</td>
<td>SCDJOBNAME</td>
</tr>
<tr>
<td>QSYS2.SERVER_SBS_ROUTING</td>
<td>QSYS2_SERVER_SBS_ROUTING</td>
<td>User Name, DRDADDSBS</td>
</tr>
<tr>
<td>QSYS2.SYSCONTROLS</td>
<td>QSYS2_SYSCONTROLS</td>
<td>SCHEMA</td>
</tr>
<tr>
<td>QSYS2.SYSCONTROLSDEP</td>
<td>QSYS2_SYSCONTROLSDEP</td>
<td>SCHEMA</td>
</tr>
<tr>
<td>QSYS2.SYSDISKSTAT</td>
<td>QSYS2_SYSDISKSTAT</td>
<td>UNITNBR</td>
</tr>
<tr>
<td>Collector_ID</td>
<td>Report_ID</td>
<td>Correlation Fields</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>QSYS2.SYSTEM_STATUS_INFO</td>
<td>QSYS2_SYSTEM_STATUS_INFO</td>
<td>Only one record</td>
</tr>
<tr>
<td>QSYS2.SYSTMPSTG</td>
<td>QSYS2_SYSTMPSTG</td>
<td>BKTNBR,GLBBKTNAME</td>
</tr>
<tr>
<td>QSYS2.USER_INFO</td>
<td>QSYS2_USER_INFO</td>
<td>USER NAME</td>
</tr>
<tr>
<td>QSYS2.USER_STORAGE</td>
<td>QSYS2_USER_STORAGE</td>
<td>USER NAME</td>
</tr>
<tr>
<td>Rsc_Mgr_Compliance_Data</td>
<td>Rsc_Mgr_Compliance_Data</td>
<td>SCMID Filesys Path ASPNAME</td>
</tr>
<tr>
<td>Rsc_Mgr_Config</td>
<td>Rsc_Mgr_Config</td>
<td>Only one record</td>
</tr>
<tr>
<td>Rsc_Mgr_Schema_Details</td>
<td>Rsc_Mgr_Schema_Details</td>
<td>Schema ID File Systems, IFS Path, Auxiliary Storage</td>
</tr>
<tr>
<td>Rsc_Mgr_Schema_Header</td>
<td>Rsc_Mgr_Schema_Header</td>
<td>Schema ID</td>
</tr>
<tr>
<td>Socket_Tran_Rules</td>
<td>Socket_Rules_Report</td>
<td>User, Port, Operation, IP Address</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>SYSTABLESTAT_Delete_Operations</td>
<td>Library Name, Long File Name</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>SYSTABLESTAT_Deleted_Records</td>
<td>Library Name, Long File Name</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>SYSTABLESTAT_Insert_Operations</td>
<td>Library Name, Long File Name</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>SYSTABLESTAT_Large_Files</td>
<td>Library Name, Long File Name</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>SYSTABLESTAT_Read_Operations</td>
<td>Library Name, Long File Name</td>
</tr>
<tr>
<td>TG_Network_Groups</td>
<td>TG_Network_Groups_Report</td>
<td>Network Group Name, Network Name</td>
</tr>
<tr>
<td>TG_Object_Groups</td>
<td>TG_Object_Groups_Report</td>
<td>Object Group Name, OBJSYS,OBJNM,OBJLB,OBJTYP,OBJIFS</td>
</tr>
<tr>
<td>TG_User_Groups</td>
<td>TG_User_Groups_Report</td>
<td>User Group Name, User Name</td>
</tr>
<tr>
<td>User_Profile_Archive</td>
<td>User_Profile_Archive</td>
<td>User Name</td>
</tr>
<tr>
<td>User_Profile_Exclusions</td>
<td>User_Profile_Exclusions</td>
<td>User Name</td>
</tr>
</tbody>
</table>