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 © 2022 Trinity Guard LLC. All rights reserved.
1. What's New ................................................................. 7
2. TGSecure Introduction ............................................. 8
   2.1 Historical Perspective of Security ............................ 9
   2.2 Features .............................................................. 10
   2.3 Rules Decision Algorithm ...................................... 12
   2.4 Rules Suggestion Engine ........................................ 14
3. Getting Started ........................................................ 15
   3.1 Log Into TGSecure ................................................ 17
   3.2 Working with TGSecure .......................................... 18
4. Network Security ........................................................ 20
   4.1 Network Security Defaults ...................................... 22
      4.1.1 Working with Network Security Default Settings ...... 23
      4.1.2 Display Network Security Defaults ....................... 24
      4.1.3 Manage Network Security Defaults ....................... 26
      4.1.4 Run Network Security Reports ............................. 31
   4.2 Exit Point Configuration ...................................... 32
      4.2.1 Working with Exit Points .................................. 34
      4.2.2 Display List of Exit Points ............................... 35
      4.2.3 Manage Exit Points ......................................... 37
      4.2.4 Run Exit Points Report ................................... 45
   4.3 Incoming Transactions .......................................... 47
      4.3.1 Working with Transactions ................................ 48
      4.3.2 Display List of Incoming Transactions .................... 49
      4.3.3 Manage Incoming Transactions ............................ 52
      4.3.4 Run Transactions (*TRN) Report ......................... 59
      4.3.5 Run Socket Transaction (*SOC) Reports ................. 62
   4.4 Socket Rules ....................................................... 65
      4.4.1 Working with Socket Rules ............................... 66
      4.4.2 Display List of Socket Rules .............................. 67
      4.4.3 Manage Socket Rules ...................................... 69
      4.4.4 Run Socket Rule Reports .................................. 74
   4.5 Exit Rules ........................................................... 76
      4.5.1 Working with Exit Rules .................................. 77
      4.5.2 Display List of Exit Rules ................................ 78
      4.5.3 Manage Exit Rules .......................................... 80
      4.5.4 Run Exit Rule Reports .................................... 85
   4.6 AI Rules ............................................................. 87
      4.6.1 Working with AI Rules ..................................... 88
      4.6.2 Display List of AI Rules ................................... 89
      4.6.3 Manage AI Rules ............................................ 92
5. Access Escalation Management .................................... 97
   5.1 Access Escalation Defaults .................................... 98
      5.1.1 Working with Access Escalation Management Defaults .. 99
      5.1.2 Display Access Escalation Defaults ...................... 100
      5.1.3 Manage Access Escalation .................................. 102
      5.1.4 Run Access Escalation Report ................................ 104
   5.2 Entitlements ......................................................... 105
      5.2.1 Working with Entitlements .................................. 106
      5.2.2 Display List of Entitlements ............................... 107
      5.2.3 Manage Entitlements ........................................ 110
      5.2.4 Run Entitlement Reports ................................... 113
   5.3 Access Control ...................................................... 116
      5.3.1 Working with Access Control ............................... 117
      5.3.2 Display Who Has Access to the AEM Interface .......... 118
      5.3.3 Manage Access Control .................................... 120
      5.3.4 Run Access Control Reports ................................ 123
         5.3.4.1 Execute an Entitlement Using the AEM Interface .. 125
   5.4 File Editor .......................................................... 126
      5.4.1 Working with File Editor ................................... 127
      5.4.2 Display List of File Editors ............................... 128
6. Inactive Session Lockdown .......................... 133
   6.1 Inactive Session Lockdown Defaults ............. 134
   6.1.1 Working with Inactive Session Lockdown Defaults . 135
   6.1.2 Display Inactive Session Lockdown Defaults . 136
   6.1.3 Manage Inactive Session Lockdown ............... 138
   6.1.4 Run Inactive Session Lockdown Reports ....... 143
   6.2 Inactive Session Rules .......................... 146
   6.2.1 Working with Inactive Session Rules .......... 147
   6.2.2 Display Inactive Session Rules ............... 148
   6.2.3 Manage Inactive Session Rules ................. 151
   6.2.4 Run Inactive Session Rules Reports .......... 154
   6.3 Disconnection Options .......................... 156
   6.3.1 Working with Disconnect Options .............. 157
   6.3.2 Display Disconnect Options .................... 158
   6.3.3 Manage Disconnect Options .................... 160
   6.3.4 Run Disconnect Option Reports ............... 163

7. Resource Manager .................................. 165
   7.1 Resource Manager Defaults ...................... 166
   7.1.1 Working with Resource Manager Defaults ....... 167
   7.1.2 Display Resource Manager Defaults .......... 168
   7.1.3 Manage Resource Manager Defaults ............ 170
   7.1.4 Run Resource Manager Reports ............... 172
   7.2 Authority Schemas ............................. 175
   7.2.1 Working with Authority Schemas ............... 176
   7.2.2 Display Authority Schemas .................... 177
   7.2.3 Manage Authority Schemas ..................... 181
   7.2.4 Run Authority Schema Reports ............... 191
   7.3 Authority Collections .......................... 195
   7.3.1 Working with Authority Collections .......... 196
   7.3.2 Display Authority Collection Configuration .... 197
   7.3.3 Manage Authority Collection Configuration .... 199
   7.3.4 Run Authority Collection Reports ............ 202

8. User Profile Management .......................... 206
   8.1 Profile Management Defaults .................... 207
   8.1.1 Working with User Profile Management Defaults .... 208
   8.1.2 Display User Profile Management Defaults .... 209
   8.1.3 Manage User Profile Management Defaults .... 211
   8.1.4 Run User Profile Management Reports ......... 215
   8.2 Blueprints ............................ 217
   8.2.1 Working with Blueprints ...................... 218
   8.2.2 Display Blueprints .......................... 219
   8.2.3 Manage Blueprints .......................... 222
   8.2.4 Run Blueprint Reports ....................... 235
   8.3 User Exclusions .............................. 245
   8.3.1 Working with User Exclusions ................ 246
   8.3.2 Display User Exclusions ...................... 247
   8.3.3 Manage User Exclusions ...................... 249
   8.3.4 Run User Exclusion Reports .................. 252
   8.4 Archived Profiles ............................ 254
   8.4.1 Working with Archived Profiles .............. 255
   8.4.2 Display Archived Profiles .................... 256
   8.4.3 Manage Archived Profiles .................... 259
   8.4.4 Run Archived Profile Reports ............... 261
   8.5 Inactive Profiles ............................ 263
   8.5.1 Working with Inactive Profiles .............. 264
   8.5.2 Display Inactive Profile Settings ............ 265
   8.5.3 Manage Inactive Profiles .................... 266
   8.5.4 Run Inactive Profile Reports ............... 269
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6</td>
<td>User Profiles</td>
<td>272</td>
</tr>
<tr>
<td>8.6.1</td>
<td>Working with User Profiles</td>
<td>273</td>
</tr>
<tr>
<td>8.6.2</td>
<td>Manage User Profiles</td>
<td>274</td>
</tr>
<tr>
<td>8.6.3</td>
<td>Run User Profile Reports</td>
<td>276</td>
</tr>
<tr>
<td>8.7</td>
<td>Password Rules</td>
<td>280</td>
</tr>
<tr>
<td>8.7.1</td>
<td>Working with Password Rules</td>
<td>281</td>
</tr>
<tr>
<td>8.7.2</td>
<td>Manage Password Rules</td>
<td>282</td>
</tr>
<tr>
<td>9.1</td>
<td>Command Security Defaults</td>
<td>286</td>
</tr>
<tr>
<td>9.1.1</td>
<td>Working with Command Security Defaults</td>
<td>287</td>
</tr>
<tr>
<td>9.1.2</td>
<td>Display Command Security Defaults</td>
<td>288</td>
</tr>
<tr>
<td>9.1.3</td>
<td>Manage Command Security Defaults</td>
<td>290</td>
</tr>
<tr>
<td>9.2</td>
<td>Command Security Rules</td>
<td>294</td>
</tr>
<tr>
<td>9.2.1</td>
<td>Working with Command Security Rules</td>
<td>295</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Display List of Command Security Rules</td>
<td>296</td>
</tr>
<tr>
<td>9.2.3</td>
<td>Manage Command Security Rules</td>
<td>299</td>
</tr>
<tr>
<td>9.3</td>
<td>Command Security Reports</td>
<td>303</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Working with Command Security Reports</td>
<td>304</td>
</tr>
<tr>
<td>9.3.2</td>
<td>Run Command Security Reports</td>
<td>305</td>
</tr>
<tr>
<td>10.</td>
<td>System Value Management</td>
<td>308</td>
</tr>
<tr>
<td>10.1</td>
<td>System Value Defaults</td>
<td>309</td>
</tr>
<tr>
<td>10.1.1</td>
<td>Working with System Value Management Defaults</td>
<td>310</td>
</tr>
<tr>
<td>10.1.2</td>
<td>Display System Value Defaults</td>
<td>311</td>
</tr>
<tr>
<td>10.1.3</td>
<td>Manage System Value Defaults</td>
<td>313</td>
</tr>
<tr>
<td>10.2</td>
<td>System Values Rules</td>
<td>316</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Working with System Values Rules</td>
<td>317</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Display List of System Value Rules</td>
<td>318</td>
</tr>
<tr>
<td>10.2.3</td>
<td>Manage System Value Rules</td>
<td>320</td>
</tr>
<tr>
<td>10.3</td>
<td>System Value Reports</td>
<td>323</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Working with System Value Management Reports</td>
<td>324</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Run System Value Management Reports</td>
<td>325</td>
</tr>
<tr>
<td>11.</td>
<td>Reports</td>
<td>328</td>
</tr>
<tr>
<td>11.1</td>
<td>Working with TGSecure Reports</td>
<td>329</td>
</tr>
<tr>
<td>11.2</td>
<td>Display List of TGSecure Reports</td>
<td>330</td>
</tr>
<tr>
<td>11.3</td>
<td>Run TGSecure Reports</td>
<td>332</td>
</tr>
<tr>
<td>11.4</td>
<td>Create TGSecure Reports</td>
<td>335</td>
</tr>
<tr>
<td>11.5</td>
<td>Manage TGSecure Reports</td>
<td>340</td>
</tr>
<tr>
<td>12.</td>
<td>Groups</td>
<td>343</td>
</tr>
<tr>
<td>12.1</td>
<td>Working with Groups</td>
<td>344</td>
</tr>
<tr>
<td>12.2</td>
<td>User Groups</td>
<td>345</td>
</tr>
<tr>
<td>12.2.1</td>
<td>Working with User Groups</td>
<td>346</td>
</tr>
<tr>
<td>12.2.2</td>
<td>Display List of User Groups</td>
<td>347</td>
</tr>
<tr>
<td>12.2.3</td>
<td>Display List of Users in a Group</td>
<td>350</td>
</tr>
<tr>
<td>12.2.4</td>
<td>Manage User Groups</td>
<td>352</td>
</tr>
<tr>
<td>12.2.5</td>
<td>Manage Users in a Group</td>
<td>355</td>
</tr>
<tr>
<td>12.2.6</td>
<td>Run User Groups Report</td>
<td>358</td>
</tr>
<tr>
<td>12.3</td>
<td>Network Groups</td>
<td>360</td>
</tr>
<tr>
<td>12.3.1</td>
<td>Working with Network/Server Groups</td>
<td>361</td>
</tr>
<tr>
<td>12.3.2</td>
<td>Display List of Network/Server Groups</td>
<td>362</td>
</tr>
<tr>
<td>12.3.3</td>
<td>Display List of Networks in a Group</td>
<td>364</td>
</tr>
<tr>
<td>12.3.4</td>
<td>Manage Network/Server Groups</td>
<td>366</td>
</tr>
<tr>
<td>12.3.5</td>
<td>Manage Networks in a Group</td>
<td>369</td>
</tr>
<tr>
<td>12.3.6</td>
<td>Run Network Groups Report</td>
<td>371</td>
</tr>
<tr>
<td>12.4</td>
<td>Operation Groups</td>
<td>373</td>
</tr>
<tr>
<td>12.4.1</td>
<td>Working with Operation Groups</td>
<td>374</td>
</tr>
<tr>
<td>12.4.2</td>
<td>Display List of Operation Groups</td>
<td>375</td>
</tr>
<tr>
<td>12.4.3</td>
<td>Display List of Operations in a Group</td>
<td>377</td>
</tr>
<tr>
<td>12.4.4</td>
<td>Manage Operation Groups</td>
<td>379</td>
</tr>
<tr>
<td>12.4.5</td>
<td>Manage Operations in a Group</td>
<td>381</td>
</tr>
<tr>
<td>12.4.6</td>
<td>Run Operation Groups Report</td>
<td>383</td>
</tr>
</tbody>
</table>
What's New

<table>
<thead>
<tr>
<th>Version 2.5 - TGSecure User Guide Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>This release includes the following:</td>
</tr>
<tr>
<td>Enhancements</td>
</tr>
<tr>
<td>System Value Management (SYS)</td>
</tr>
<tr>
<td>• Added support for numeric data</td>
</tr>
<tr>
<td>Command Security (CMD)</td>
</tr>
<tr>
<td>• Added granular parameter restriction per rule (CMD/Lib/User/IP)</td>
</tr>
<tr>
<td>• Added option to use function key F2 to add exits out of sync</td>
</tr>
</tbody>
</table>

See also

APPENDIX - TGSecure Revisions
TGSecure Introduction

This section includes the following topics:

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

See also

Getting Started
Historical Perspective of Security

Before we talk about what TGSecure is or does, let's talk about where it fits. When the IBM® AS/400 was introduced in 1988, client/server configurations and Internet-based networks were not widely used. At that time, AS/400 servers were accessed through locally attached terminals. Security was controlled through the following structure:

- **Physical Security** - Restrict access by setting up the server in a secure computer room
- **User Authorities** - Restrict the user's ability to execute OS/400 or user-defined commands
- **Object Authorities** - Restrict the user's ability to execute commands on objects
- **Application Authorities** - Restrict the user's ability to access data or commands

Times have changed and so has the server. Today, many IBM i systems are accessed via remote connections, which require additional security structure:

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

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

See also

- TGSecure Introduction
- IBM System Values (external IBM Knowledge base topic)
Features

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

### Network Security

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

- Manage Socket Rules
- Manage Exit Rules

### Access Escalation Management

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

- Manage Entitlements
- Manage Access Control

### Reports

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

> **Note:** See Manage TGSecure Reports for more information.
Groups

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

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

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

See also

TGSecure Introduction
**Rules Decision Algorithm**

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

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

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

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

**Check 4: Evaluate Network (Target Server)**
1) Check rules for a specific target IP
2) Check rules for a generic IP (e.g., 11.111*)
3) Check rules for network group
4) Check rules that apply to all networks (*ALL)
Check 5: Evaluate Object
1) Check rules for a specific object
2) Check rules for a generic object (e.g., /home/etv /*...)
3) Check rules for an object group
4) Check rules that apply to all objects (*ALL)

See also

TGSecure Introduction

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

For information about how to run reports, see Working with TGSecure Reports.
Rules Suggestion Engine

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

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

Rule Example

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

Rule Suggestion Example

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

Rule Suggestion Interface

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

See also

Manage Incoming Transactions
Manage Exit Rules
Manage Socket Rules
Getting Started

This topic discusses the following:

- **Actions**
- **Process Flow**
- **Implementation Tasks**

**Actions**

The following TGSecure features allow you to do the following:

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

**Process Flow**

**Implementation Tasks**

There is no single linear process for implementing TGSecure, but the following describes how a typical implementation might work. It's important to remember that security management is an iterative process.
<table>
<thead>
<tr>
<th>1</th>
<th><strong>Monitor Network Access</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>To enhance security, you first need to understand who is accessing your network.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Incoming Transactions module</strong> of TGSecure allows you to display the incoming transactions requesting access and executing commands on the server.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th><strong>Create Groups</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>With the vast number of elements that impact security, it might be necessary to group items together for efficiency.</td>
<td></td>
</tr>
<tr>
<td>For example, it might not be efficient to create an entitlement for each user. It would be more efficient to apply a single entitlement to a group of users. The same would hold true for a single rule being applied to a group of networks.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Grouping</strong> module of TGSecure allows you to create groups for the following elements:</td>
<td></td>
</tr>
<tr>
<td>- Users</td>
<td></td>
</tr>
<tr>
<td>- Networks</td>
<td></td>
</tr>
<tr>
<td>- Operations</td>
<td></td>
</tr>
<tr>
<td>- Objects</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th><strong>Manage Network Access</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Once you have a better awareness of who and how your system is accessed and you have created what you feel are logical and useful groupings, you can begin limiting network access.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Exit Point</strong> and <strong>Socket Rules</strong> modules of TGSecure allows you to apply rules to manage network access:</td>
<td></td>
</tr>
<tr>
<td>- Application layer (exit rules)</td>
<td></td>
</tr>
<tr>
<td>- Transport layer (socket rules)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th><strong>Implement Least-privilege Model</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Once the appropriate users have access to your system, you then want to ensure that these users have the appropriate level of authority to perform assigned tasks, but no more than that.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Access Escalation Management</strong> (AEM) module of TGSecure allows you to create entitlements to manage system access.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th><strong>Run Reports</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring your server and system remain secure involves continuous and proactive monitoring.</td>
<td></td>
</tr>
<tr>
<td>The Reporting module of TGSecure allows you to run built-in reports and create custom reports to monitor the security health of your server and system.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: The built-in reports available to you are dependent on your license agreement.</td>
<td></td>
</tr>
</tbody>
</table>

**See also**

- Log Into TGSecure
- Features
Log Into TGSecure

Use this task to log into TGSecure.

To log into TGSecure

1) Sign into your IBM i server.
2) At the Selection or command prompt, enter TGMENU.
3) Press Enter. The TG - Main menu is displayed.
4) At the Selection or command prompt, enter 2 (TGSecure). The TGSecure Main menu is displayed.

See also

Getting Started

Working with TGSecure
Working with TGSecure

Follow these steps:

**Step 1: Setup network security**
- Working with Network Security Default Settings
- Working with Transactions
- Working with Exit Points
- Working with Socket Rules
- Working with Exit Rules
- Working with Network/Server Groups

**Step 2: Setup Access Escalation**
- Working with Access Escalation Management Defaults
- Working with Entitlements
- Working with Access Control
- Working with File Editor

**Step 3: Setup Inactive Session Lockdown**
- Working with Inactive Session Lockdown Defaults
- Working with Inactive Session Rules
- Working with Disconnect Options

**Step 4: Setup Resource Manager**
- Working with Resource Manager Defaults
- Working with Authority Schemas
- Working with Authority Collections

**Step 5: Setup User Profile Manager**
- Working with User Profiles
- Working with Blueprints
- Working with User Exclusions
- Working with Archived Profiles
- Working with Inactive Profiles
- Working with User Profiles
- Working with Password Rules

**Step 6: Setup Command Security**
- Working with Command Security Defaults
- Working with Command Security Rules
- Working with Command Security Reports

See also
Getting Started
Network Security

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

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

To access the **Network Security** interface

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

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

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

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

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

Getting Started
Network Security Defaults

Use the **Network Security Defaults** feature to define the following:

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

This section includes the following topics:

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

**See also**

Network Security
Working with Network Security Default Settings

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

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

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

**To access the Network Security Defaults interface**

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

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 11 (Network Security Defaults).

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

**See also**

Network Security Defaults
Display Network Security Defaults

Use this task to display Network Security default settings.

To display the network security defaults

1) Access the TGSecure Main menu.

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

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

4) At the Selection or command prompt, enter 11 (Network Security Defaults).


<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Audit Status                 | Whether auditing is enabled globally (for all exit points). Auditing is required if you plan to run network security reports.                                                                                                      *YES* - Record incoming transaction data in the audit journal  
*NO* - Do not record incoming transaction data in the audit journal  

**Tip:** If auditing is disabled at the network security (module) level, then auditing will not occur. The module-level setting takes precedence. However, if auditing is enabled at the module level, you must also enable auditing at the secondary level (each exit point) if you want to record auditing data for a specific exit point.  
See Manage Exit Points for information about setting the audit status for an individual exit point. |
| Audit Journal                | Journal in which to store network security audit data                                                                                                                                                                                                                     |
| Note:                        | The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.                                                                                                                                                                                |
| Audit Journal Library        | Library in which the journal resides                                                                                                                                                                                                                                        |
| Audit Configuration Changes  | Whether to collect data about network (internal) security changes                                                                                                                                                                                                          Y - Enable tracking of changes  
N - Disable tracking of changes                                                                 |
| Tip:                         | Set this flag to Y if you plan to run network security change reports.                                                                                                                                                                                                   |

**Tip:** There are multiple TGSecure modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE* in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL*, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL*, this indicates that configuration changes are being tracked in all modules.
| Alert Status | Whether alerting is enabled globally (for all exit points). Alerting is required if you plan to send alert notifications.  
*YES* - Enable alerts for all (PASS and FAIL) connection attempts  
*NO* - Disable alerts  
*Tip:* If alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. See **Manage Exit Points** for information about setting the alert status for an individual exit point. |
| Alert Message Queue | Queue in which to store alerts  
*Tip:* You can change the queue if you are using a third-party application for message monitoring. |
| Alert Message Queue Library | Library in which the queue is located |
| TELNET AutoSignon Allowed | Whether auto signon is enabled  
*YES* - Enabled auto signon  
*NO* - Disable auto signon  
*ENCPWD* - Enable auto sign and encrypt password  
*PWDRQD* - Enable auto signon |
| Primary Group Inheritance | Whether to allow primary group inheritance  
*YES* - Enable profile primary group inheritance  
*NO* - Disable profile primary group inheritance  
*Note:* The primary group is the user ID entered in the **Group** profile field when using command **CHGUSRPRF**. The primary group is the first ID from which a user inherits privileges. |
| Supplemental Group Inheritance | Whether to allow supplemental group inheritance  
*YES* - Enable supplemental group inheritance  
*NO* - Disable supplemental group inheritance  
*Note:* The supplemental groups are user IDs entered in the **Supplemental** group field when using command **CHGUSRPRF**. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges. |
| Enable Debug | Whether to collect data for a debug log  
*YES* - Enable debug log  
*NO* - Disable debug log  
*Note:* The debug log is not required but might help with troubleshooting issues. |

See also

- Working with Network Security Default Settings
Manage Network Security Defaults

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

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

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

Access the Network Security Defaults Interface

**To access the with Network Security Defaults interface**

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

Enable Network Security Auditing

Use this task to enable network security auditing.

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

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

**To enable network security auditing**

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

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

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

To enable network security configuration change tracking

1) Access the Network Security Defaults interface.

2) In the Audit Configuration Changes field, enter Y.

3) Press Enter.

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

Enable Network Security Alerts

Use this task to enable network security alerts.

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

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

To enable network security alerts

1) Access the Network Security Defaults interface.

2) In the Alert Status field, enter *YES.

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

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

5) Press Enter.

Enable Network Security Debug Log

Use this task to enable the network security debugging log.

Note: The debug log is not required but might help with troubleshooting issues.
To enable network security debugging log

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

2) In the **Enable Debug** field, enter **"YES."**

3) Press **Enter**.

Enable TELNET Auto Signon

Use this task to enable TELNET auto signon.

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

Enabling TELNET auto signon is a three-step process:

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

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

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

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

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **WRKSYSVAL QRMTSIGN**.

3) Press **Enter**. The **Work with System Values** interface is displayed.

4) In the **Option** column beside the **QRMTSIGN** system value, enter **2** (Change).

5) Press **Enter**. The **Change System Value** interface is displayed.

6) In the **Remote sign-on control** field, enter **"VERIFY."**

7) Press **Enter** twice.

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

1) Access the **Main** menu.

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

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

4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).

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

6) In the **Telnet AutoSignon Allowed** field, enter **"YES."**

7) Press **Enter**.

**Step 3: Update the Network Security Configuration for TELNET auto signon**
1) Access the **Main** menu.

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

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

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

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

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

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

---

### Enable Group Profile Inheritance

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

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

**To enable group profile inheritance**

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

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

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

3) In some cases, a user might inherit privileges from multiple users. In such a case, enter "YES in Supplemental Group Inheritance field."
Note: Supplemental groups are user IDs entered in the **Supplemental group** field when using command CHGUSRPRF. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.

4) Press **Enter**.

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

**See also**

*Working with Network Security Defaults*
Run Network Security Reports

Use this task to generate the Network Security reports.

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

To run the Network Security Reports

1) Access the TGSecure Main menu.

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

3) Press Enter.

4) At the Selection or command prompt, enter 20 (Network Reports).

5) Press Enter.

6) At the Selection or command prompt, enter the category of the report type you want to run.

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Transaction Reports</td>
</tr>
<tr>
<td>2</td>
<td>Summary Reports</td>
</tr>
<tr>
<td>3</td>
<td>Configuration Reports</td>
</tr>
<tr>
<td>4</td>
<td>Configuration Reports</td>
</tr>
</tbody>
</table>

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

7) Press Enter.

8) Choose the desired report from the list.

9) Press Enter.

See also

Working with Network Security Default Settings
Exit Point Configuration

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

Analogy

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

Client-Server Communication Process via transport layer:

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

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

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

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

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

This section includes the following topics:
• Working with Exit Points
• Display List of Exit Points
• Manage Exit Points
• Run Exit Points Report

See also

Network Security
Working with Exit Points

Use the Exit Points feature to do the following:

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

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

To access the Network Security Configuration interface

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

See also

Exit Point Configuration
**Display List of Exit Points**

Use this task to display the list of exit points.

**To display the list of exit points**

1) Access the TGSecure Main menu.

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

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

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

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

---

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

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Server</td>
<td>Name of the server type</td>
</tr>
</tbody>
</table>
| Audit Status   | Whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports  
                     *YES - Record incoming transaction data in the audit journal  
                     *NO - Do not record incoming transaction data in the audit journal  
                     **Tip:** If auditing is disabled at the module level, then this setting is ignored. In other words, if auditing is disabled at the network security (module) level, then auditing will not occur even if auditing is enabled at the exit point (secondary) level. The module-level setting takes precedence. However, if auditing is enabled at the module level, you must also enable alerting at the secondary level if you want to record auditing data for a specific exit point.  
                     **Note:** See Manage Network Security Defaults for information about enabling/disabling auditing globally. |
| Sec Status | Whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go in to effect.  
                     *YES - Apply exit rules (enable network security)  
                     *NO - Disable exit rules (disable network security)  
                     **Tip:** If alerts are disabled at the module level, then this setting is ignored. In other words, if alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point.  
                     **Note:** See Manage Network Security Defaults for information about enabling/disabling alerting globally. |
| Alert Status | Whether alerting is enabled for a specific exit point. Alerts are required if you plan to send alert notifications  
                     *ALL - Record an alert for all (PASS and FAIL) connection attempts  
                     *FAIL - Record only FAIL connection attempts  
                     *NONE - Do not record alerts  
                     **Tip:** If alerts are disabled at the module level, then this setting is ignored. In other words, if alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point.  
                     **Note:** See Manage Network Security Defaults for information about enabling/disabling alerting globally. |
| **Smart Mode** | Whether the smart mode (Rules Intelligence Engine) is enabled  
*YES* - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions  
*NO* - Do not enable the intelligence engine to create rules  

**Note:** The system administrator can delete rules created by the Rules Intelligence Engine at any time. |
|-----------------|-------------------------------------------------------------------------------------------------------|
| **Collector Status** | Which incoming transactions you want to track (collect) in the **Incoming Transaction** interface  
*ALL* - Collect and display all (PASS and FAIL) incoming transactions  
*FAIL* - Collect and display only rejected (FAIL) incoming transactions  
*NONE* - Do not collect or display any incoming transactions |
| **Function Usage** | Whether an IBM function usage rule is being applied at the exit point. This indicator is important because it helps to identify conflicts between exit rules and function usage rules. If there is a conflict (e.g., an exit rule states to do one thing, but a function usage rule states to do something different), then the system might produce an unexpected outcome.  
*YES* - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists  
*NO* - No function usage rule is applied at the exit point  
*NA* - Not applicable because IBM does not provide a function usage rule for this exit point |
| **Exit Inst?** | Whether the exit point is installed on the server  
*YES* - Exit points are installed and ready for use  
*NO* - Exit points are not installed  

**Note:** The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to *YES*. |
| **Network Description** | A short description of the network |

**See also**

*Working with Exit Point*
Manage Exit Points

Use this task to manage exit points.

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

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

Access the Work with Network Security Configuration Interface

To access the Work with Network Security Configuration

1) Access the TGSecure Main menu.

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

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

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

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

Display Exit Point Details

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

To display exit point details

1) Access the Network Security Configuration interface.

2) In the OPT column for the desired exit point, enter 5 (Display).

3) Press Enter.
<table>
<thead>
<tr>
<th>Network Server</th>
<th>Name of the server type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit Point</td>
<td>Name assigned to the exit point</td>
</tr>
<tr>
<td>Exit Format</td>
<td>IBM format associated with the exit point</td>
</tr>
<tr>
<td>Exit Description</td>
<td>Description of the exit point</td>
</tr>
</tbody>
</table>

**Exit Program Installed**

<table>
<thead>
<tr>
<th>Indicators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>YES</strong> - Exit points are installed and ready for use</td>
<td>Indicates whether the exit point is installed on the server</td>
</tr>
<tr>
<td><strong>NO</strong> - Exit points are not installed</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The exit rules associated with the exit point are not applied until the exit point is installed and the Security Status is set to **YES.**

**Function Usage Rule**

Indicates whether an IBM function usage rule is being applied at the exit point. This indicator is important because it helps to identify conflicts between exit rules and function usage rules. If there is a conflict (e.g., an exit rule states to do one thing, but a function usage rule states to do something different), then the system might produce an unexpected outcome.

- **YES** - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists
- **NO** - No function usage rule is applied at the exit point
- **NA** - Not applicable because IBM does not provide a function usage rule for this exit point

**Audit Status**

Indicates whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports.

- **YES** - Record incoming transaction data in the audit journal
- **NO** - Do not record incoming transaction data in the audit journal

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

**Note:** See Manage Network Security Defaults for information about enabling/disabling auditing globally.

**Security Status**

Indicates whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go into effect.

- **YES** - Apply exit rules (enable network security)
- **NO** - Disable exit rules (disable network security)
Enable Exit Point Auditing

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

Prerequisite

Auditing must be enabled in the Network Security Module.

To enable auditing for an exit point

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

Enable Exit Point Security

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

Prerequisite

Note: See Manage Network Security Defaults.
Create the exit rules you want to apply.

**Note:** See Manage Exit Rule.

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

**To enable security for an exit point**

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

2) In the **OPT** column for the desired exit point, enter 2 (Edit).

3) Press **Enter**.

4) In the **Security Status** field, enter ‘YES’.

5) Press **Enter**.

**Enable Exit Point Alerts**

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

**Prerequisite**

Alerts must be enabled in the Network Security module.

**Note:** See Manage Network Security Defaults.

**To enable alerts for an exit point**

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

2) In the **OPT** column for the desired exit point, enter 2 (Edit).

3) Press **Enter**.

4) In the **Alert Status** field, enter one of the following:
   - ‘{‘*ALL’} - Record an alert for all (PASS and FAIL) connection attempts
   - ‘{‘*FAIL’} - Record only FAIL connection attempts

5) Press **Enter**.

**Enable Exit Point Collection**

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

**To enable incoming transaction collection for an exit point**
1) Access the **Network Security Configuration** interface.

2) In the **OPT** column for the desired exit point, enter **2** (Edit).

3) Press **Enter**.

4) In the **Alert Status** field, enter one of the following:
   - **(*)ALL** - Collect and display all (PASS and FAIL) incoming transactions
   - **(*)FAIL** - Collect and display only rejected (FAIL) incoming transactions

5) Press **Enter**.

### Add Exit Program to Exit Point

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

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

#### To add exit program to exit point

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

2) In the **OPT** column for the desired exit point, enter **11** (Add Exit Program).

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

### Add Exit Programs to Exit Points (Mass Update)

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

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

#### To add an exit program to exit points

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

2) Press the **F20** (Add Exit Programs) function key.

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

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

4) Press **Enter**.
Remove Exit Program from Exit Point

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

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

To remove an exit program from exit point

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

Remove Exit Programs from Exit Points (Mass Update)

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

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

To remove an exit program from exit points

1) Access the Network Security Configuration interface.
2) Press the F21 (Remove Exit Programs) function key.
   Tip: For function keys higher than F12, you must use a combination of the Shift key and the appropriate function key. For example, to select F21, you must hold down the Shift key and F9.
3) Enter *All to remove all exit programs or enter a specific server type.
4) Press Enter.

Cycle Server

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

To cycle a single server

1) Access the Network Security Configuration interface.
2) In the OPT column for the desired exit point, enter 13 (Cycle Server).
3) Press Enter.
4) Ensure that the correct server is selected.
5) Enter one of the following options:
– Y - Initiate cycling immediately (run in interactive mode)
– N - Place cycling request in the queue (run as part of a job queue)

6) Press Enter.

**Cycle Servers (Mass Update)**

Use this task to restart multiple servers.

**To cycle multiple servers**

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

2) Press the **F19** (Cycle Servers) function key.

   ![Tip](image)

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

3) Enter *All to cycle all servers or identify a specific server type.

4) Enter **Y** to execute the cycling immediately or **N** to add it a batch.

5) Press Enter.

**Update all Exit Points (Mass Update)**

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

**To update all exit points**

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

2) Press the **F7** (Update all) function key.

3) Modify the setting as necessary.

![Note](image)

Note: All editable settings are underlined.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Status</td>
<td>Indicates whether auditing is enabled. Auditing is required if you plan to run network security reports. <em>YES</em> - Record incoming transaction data in the audit journal for all installed exit points. <em>NO</em> - Do not record incoming transaction data in the audit journal for all installed exit points. <em>SAME</em> - Do not perform a mass update of the Audit Status. In other words, skip this setting.</td>
</tr>
</tbody>
</table>

Tip: See **Manage Network Security Defaults** for information about enabling auditing globally. Global defaults take precedence over local settings.
<table>
<thead>
<tr>
<th>Security Status</th>
<th>Indicates whether the exit rules associated with the exit point should be applied.</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>YES</em></td>
<td>Apply exit rules for all installed exit points</td>
</tr>
<tr>
<td><em>NO</em></td>
<td>Do not apply exit rules for all installed exit points</td>
</tr>
<tr>
<td><em>SAME</em></td>
<td>Do not perform a mass update of the Security Status. In other words, skip this setting during the mass update.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alert Status</th>
<th>Indicates whether alerting is enabled. Alerting is required if you plan to send alert notifications.</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ALL</em></td>
<td>Record an alert for all (PASS and FAIL) connection attempts</td>
</tr>
<tr>
<td><em>FAIL</em></td>
<td>Record only FAIL alerts for all installed exit points</td>
</tr>
<tr>
<td><em>NONE</em></td>
<td>Do not record alerts for all installed exit points</td>
</tr>
<tr>
<td><em>SAME</em></td>
<td>Do not perform a mass update of the Alert Status. In other words, skip this setting during the mass update.</td>
</tr>
</tbody>
</table>

**Tip:** See Manage Network Security Defaults for information about enabling alerting globally. Global defaults take precedence over local settings.

<table>
<thead>
<tr>
<th>Smart Mode</th>
<th>Indicates whether the smart mode (Rules Intelligence Engine) is enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>YES</em></td>
<td>Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions</td>
</tr>
<tr>
<td><em>NO</em></td>
<td>Do not enable the intelligence engine to create rules</td>
</tr>
<tr>
<td><em>SAME</em></td>
<td>Do not perform a mass update of the Smart Mode. In other words, skip this setting during the mass update.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Indicates which incoming transactions are tracked (collect) in the Incoming Transaction interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ALL</em></td>
<td>Collect and display all (PASS and FAIL) connection attempts</td>
</tr>
<tr>
<td><em>FAIL</em></td>
<td>Collect and display only FAIL connection attempts</td>
</tr>
<tr>
<td><em>NONE</em></td>
<td>Do not collect or display any connection attempts</td>
</tr>
<tr>
<td><em>SAME</em></td>
<td>Do not perform a mass update of the Collector Status. In other words, skip this setting during the mass update.</td>
</tr>
</tbody>
</table>

4) Press Enter.

**See also**

Working with Exit Point
Run Exit Points Report

Use this task to generate the following exit point reports:

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

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

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

Access the Network Reports Interface

To access the Access Escalation Reports interface

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

Run Exit Point Configuration Report

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

To run the Exit Point Configuration Report

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

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

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

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

**Run Exit Point Configuration Changes Report**

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

<table>
<thead>
<tr>
<th>Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.</th>
</tr>
</thead>
</table>

**To run the Exit Point Configuration Change Report**

1) Access the **Network Reports** interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

<table>
<thead>
<tr>
<th>Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Tip: Place your cursor in a field and press <strong>F1</strong> (Help) to access a field description. Press <strong>F4</strong> (Prompt) for a list of valid field options.</th>
</tr>
</thead>
</table>

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

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

**See also**

*Working with Exit Points*
Incoming Transactions

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

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

This section includes the following topics:

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

See also

Network Security
Working with Transactions

Use the Transaction feature to do the following:

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

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

To access the Incoming Transactions interface

1) Log into TGSecure. The Main menu appears.

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

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

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

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

See also

Incoming Transactions
Display List of Incoming Transactions

Use this task to display incoming transactions.

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

Display List

Use this task to display the list of incoming transactions.

To display the list of incoming transactions

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tran Type   | There are two types of transactions:  
  * TRN - Transaction coming through an exit point  
  * SOC - Transaction coming through a socket |
| User        | User who initiated the transaction |
| Server      | Type of server |
| Function    | Function being executed |
| SSL?        | Whether SSL is enabled:  
  * YES - SSL enabled  
  * NO - SSL disabled  
  * N/A - SSL Communication is not applicable |
| Client IP   | IP address of the server initiating the transaction |
| Tran. Count | Total number of transactions attempted |
| Note:       | The incoming transactions displayed in the interface are determined by the Collector Status. |
| Tip:        | See Manage Exit Points for information about editing the Collector Status. |
| Object Details | Object affected by the transaction |
| Timestamp   | Time at which the transaction was received |
Sort List

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

To sort the list

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

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

Move to Position in List

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

To move to a specific position within the list

1) Access the Incoming Transactions interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List

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

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

To filter the list using a subset

1) Access the Incoming Transactions interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter. The system filters the results based on the criteria you defined for the subset.
See also

Working with Transactions
Manage Incoming Transactions

Use this task to manage incoming transactions.

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

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

Access the Incoming Transactions Interface

To access the Incoming Transactions interface

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

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

3) Press **Enter**.

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

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

Display Incoming Transaction Details

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

To display the incoming transaction details

1) Access the **Incoming Transactions** interface.

2) In the **OPT** column for the desired transaction, enter 5 (Display).

3) Press **Enter**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Type</td>
<td>There are two types of transactions:</td>
</tr>
<tr>
<td></td>
<td><em>TRN</em> - Transaction coming through an exit point</td>
</tr>
<tr>
<td></td>
<td><em>SOC</em> - Transaction coming through a socket</td>
</tr>
<tr>
<td>User Name</td>
<td>User who initiated the transaction</td>
</tr>
</tbody>
</table>
Delete Incoming Transaction

Use this task to delete transactions.

Usage examples:

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

To delete an incoming transaction

1) Access the Incoming Transactions interface.

2) In the OPT column for the desired transaction, enter 4 (Delete).

3) Press Enter.

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

5) Press Enter.

Archive Incoming Transactions

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

Usage examples:
• You want to delete older transactions to see what new transactions are coming in.
• You want to perform a transaction count.

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

To archive incoming transactions

1) Access the **Incoming Transactions** interface.

2) Press the **F16** (Archive/Delete Transactions) function key.

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

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

   ![Note: For example, enter 1 to keep all transactions for today, but delete all transactions older than 1 day.]

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

Create a Rule-Based on a Transaction

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

To create a security rule based on a transaction

1) Access the **Incoming Transactions** interface.

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

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

3) Press **Enter**.

4) Enter the necessary parameters to define your rule.

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

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

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

**Tip:** If you decide to accept a suggestion, but then change your mind, in the OPT column for the desired rule, enter 6 (Undo Suggestion).

**Note:** The opportunity to undo a suggestion is only available during the current session. Once you exit the session (press F3 or F12), the option to undo the suggestion is lost. Any change after the point must be made manually by updating the group(s).

---

**Create an Exit Point Transaction Rule**

Use this task to create an exit point transaction rule.

**To create an exit point transaction rule**

1) Access the **Incoming Transactions** interface.

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

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

3) Press Enter.

4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>User/user group to which the rule applies</td>
</tr>
<tr>
<td>Operation/Port</td>
<td>Operation server or port to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address to which the rule applies</td>
</tr>
<tr>
<td>Calendar</td>
<td>Calendar that defines when the rule is applicable</td>
</tr>
<tr>
<td>Swap User</td>
<td>Swap user to which the rule applies</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether to send a notification when the rule is triggered</td>
</tr>
</tbody>
</table>
Create a Socket Transaction Rule

Use this task to create a socket transaction rule.

To create a socket transaction rule

1) Access the **Incoming Transactions** interface.

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

3) Press **Enter**.

4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>User/user group to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address to which the rule applies</td>
</tr>
</tbody>
</table>
Accept a Rule Suggestion

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

Perform these steps to accept a rule suggestion:

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

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

6) Press Enter.

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

**Tip:** If you decide to accept a suggestion, but then change your mind, in the OPT column for the desired rule, enter 6 (Undo Suggestion).

**Note:** The opportunity the undo a suggestion is only available during the current session. Once you exit the session (press F3 or F12), the option to undo the suggestion is lost. Any change after the point must be made manually by updating the group(s).
Note: You will only see the Rule Suggestion interface when the intelligence engine finds an opportunity to better utilize existing groups.

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

To accept a rule suggestion

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

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

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

See also

- Working with Transactions
- Rules Suggestion Engine
- Rules Decision Engine
Run Transactions (*TRN) Report

Use this task to generate the following incoming transaction reports:

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

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

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

Access the Network Reports Interface

To access the Access Escalation Reports interface

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

Run Incoming Transaction Details

Use this report to display incoming transaction details.

To run the Incoming Transactions Details Report

1) Access the Network Reports interface.
2) At the Selection or command prompt, enter 1 (Transaction Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 1 (Incoming Transactions Report).
5) Press Enter.
6) Modify the report run criteria as necessary. The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

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

**Run Transaction Summary by Server Report**

Use this report to display incoming transaction details by server.

**To run the Transaction Summary by Server Report**

1) Access the Network Reports interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **3** (Transaction Summary by Server).

5) Press **Enter**.

6) Modify the report run criteria as necessary. The criteria allow you to limit the data returned in the report when you generate it.

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

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

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

**Run Transaction Summary by User Report**

Use this report to display incoming transaction details by user.

**To run the Transaction Summary by User Report**

1) Access the Network Reports interface.

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

3) Press **Enter**.

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

5) Press **Enter**.

6) Modify the report run criteria as necessary. The criteria allow you to limit the data returned in the report when you generate it.

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

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

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.
Run Network Transaction Report

Use this report to display network transactions.

To run the Network Transaction Report

1) Access the Network Reports interface.

2) At the Selection or command prompt, enter 1 (Transaction Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 3 (Network Transaction Report).

5) Press Enter.

6) Modify the report run criteria as necessary. The criteria allow you to limit the data returned in the report when you generate it.

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

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

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

See also

Working with Transactions
Run Socket Transaction (*SOC) Reports

Use this task to generate the following socket transaction reports:

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

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

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

Access the Network Reports Interface

To access the Access Escalation Reports interface

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

Run Socket Transaction Report

Use this report to display the socket transaction details.

To run the Socket Transaction Report

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

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

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

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

**Run Socket Summary by Server Report**

Use this report to display socket transaction details by server.

**To run the Socket Summary by Server Report**

1) Access the Network Reports interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 1 (Socket Summary by Server).

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

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

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

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

**Run Transaction Summary by User Report**

Use this report to display socket transaction details by user.

**To run the Transaction Summary by User Report**

1) Access the Network Reports interface.

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

3) Press **Enter**.

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

5) Press **Enter**.

6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
7) Enter the desired output format in the **Report output type** field.

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

**See also**

*Working with Transactions*
Socket Rules

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

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

This section includes the following topics:

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

See also

Network Security
Working with Socket Rules

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

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

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

To access the Work with Socket Rules interface

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

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

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

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

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

**See also**

Socket Rules
Display List of Socket Rules

Use this task to display socket rules.

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of socket rules.

To display the list of socket rules

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User or user group to which the rule applies</td>
</tr>
<tr>
<td>Operation Port</td>
<td>Port to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address to which the rule applies</td>
</tr>
<tr>
<td>Calendar</td>
<td>Applicable calendar</td>
</tr>
<tr>
<td></td>
<td>Note: the calendar limits when the rule is applicable.</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>Action</td>
<td>The level at which action was taken:</td>
</tr>
<tr>
<td></td>
<td>*EXITLVL - Exit point level</td>
</tr>
<tr>
<td></td>
<td>Note: If the action failed, you will see *FAIL in this column.</td>
</tr>
</tbody>
</table>

Sort List

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

To sort the list

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

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

**Move to Position in List**

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

**To move to a specific position within the list**

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

**Filter List**

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

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

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

**See also**

*Working with Socket Rules*
Manage Socket Rules

Use this task to manage socket rules.

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

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

Access the Work with Socket Rules Interface

To access the Work with Socket Rules interface

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

Add Socket Rule

Use this task to add a socket rule.

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

To add a socket rule

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter the user or user group to which the rule applies</td>
</tr>
</tbody>
</table>
To copy a socket rule

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

To copy a socket rule

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

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

Edit Socket Rule

Use this task to edit an existing socket rule.

To edit a socket rule

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

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

Copy Socket Rule

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

To copy a socket rule

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

2) In the **OPT** column for the desired socket rule, enter 3 (Copy).

3) Press **Enter**.

4) Modify the parameters as necessary.

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

5) Press **Enter**.

### Delete Socket Rule

Use this task to delete a socket rule.

**To delete a socket rule**

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

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

3) Press **Enter**.

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

5) Press **Enter**.

### Display List of Users in a Group

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

   **Tip:** Group names always begin with a colon.

**To display the list of users**

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

2) In the **OPT** column for the desired socket rule, enter 6 (User Grp).

3) Press **Enter**.

4) Review the list of users.

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

### Display List of Clients in a Group

Use this task when **Client IP** field contains a network group. You can access the network group at this point to display its details or modify the group.
To display the list of clients
1) Access the Work with Socket Rules interface.
2) In the OPT column for the desired socket rule, enter 7 (Client Grp).
3) Press Enter.
4) Review the list of clients.

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

Display List of Servers in a Group

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

Tip: Group names always begin with a colon.

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

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

Display List of Operations in a Group

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

Tip: Group names always begin with a colon.

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

Working with Socket Rules
Run Socket Rule Reports

Use this task to generate the following socket rule reports:

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

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

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

Access the Network Reports Interface

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

Run Socket Rule Configuration Report

Use this report to display socket rule configuration details.

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

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

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
Run Socket Rule Configuration Changes Report

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

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

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

To run the Socket Rule Configuration Changes Report

1) Access the **Network Reports** interface.

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

3) Press **Enter**.

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

5) Press **Enter**.

6) Modify the report run criteria as necessary.

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

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

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

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

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

See also

Working with Socket Rules
Exit Rules

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

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

Client-Server Communication Process via transport layer:

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

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

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

This section includes the following topics:

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

See also

Network Security
Working with Exit Rules

Use the Exit Rule feature to do the following:

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

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

To access the Work with Exit Rules interface

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

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

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

4) At the Selection or command prompt, enter 3 (Remote Exit Rules).

5) Press Enter. The Work with Exit Rules interface is displayed.

See also

Exit Rules
Display List of Exit Rules

Use this task to display exit rules.

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

**Display List**

Use this task to display the list of exit rules.

**To display the list of exit rules**

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

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

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

4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User or user group to which the rule applies</td>
</tr>
<tr>
<td>Server</td>
<td>Server on which the rule applies</td>
</tr>
<tr>
<td>Function</td>
<td>Function to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address to which the rule applies</td>
</tr>
<tr>
<td>Calendar</td>
<td>Applicable calendar</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerting is enabled: <strong>YES</strong> - Alerts enabled <strong>NO</strong> - Alerts disabled</td>
</tr>
<tr>
<td>Action</td>
<td>The level at which action is taken: <strong>EXITLVL</strong> - Exit point level</td>
</tr>
<tr>
<td>Object Details</td>
<td>Short description of the object to which access was attempted</td>
</tr>
</tbody>
</table>

**Sort List**

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

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

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

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

Move to Position in List

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

To move to a specific position within the list

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

2) Sort the list based on the desired column heading.

3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

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

Filter List

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

   **Tip:** Use wildcard asterisk to help define your subset.

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

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

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

To filter the list using a subset

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

2) Press the **F8** (Subset) function key.

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

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

See also

*Working with Exit Rules*
Manage Exit Rules

Use this task to manage exit rules.

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

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

Access the Work with Exit Rules Interface

To access the Work with Exit Rules interface

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

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

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

4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).

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

Add Exit Rule

Use this task to add an exit rule.

To add an exit rule

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

2) Press the **F6** (Add) function key.

3) Complete the following fields:

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

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

4) Press **Enter**.

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

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

6) Press **Enter**.
Edit Exit Rule

Use this task to edit an existing exit rule.

To edit an exit rule

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

Copy Exit Rule

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

To copy an exit rule

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

Delete Exit Rule

Use this task to delete an exit rule.

To delete an exit rule

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

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

**Display List of Users**

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

> Tip: Group names always begin with a colon.

**To display the list of users**

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

**Display List of Clients**

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

> Tip: Group names always begin with a colon.

**To display the list of clients**

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

**Display List of Servers**

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

> Tip: Group names always begin with a colon.

**To display the list of servers**

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

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

Tip: Group names always begin with a colon.

To display the list of operations

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

Display List of Objects

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

Tip: Group names always begin with a colon.

To display the list of objects

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

See also

Working with Exit Rules
Run Exit Rule Reports

Use this task to generate the following exit rule reports:

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

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

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

Access the Network Reports Interface

To access the Access Escalation Reports interface

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

Run Exit Rule Configuration Report

Use this report to display exit rule configuration details.

To run the Exit Rule Configuration Report

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

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

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

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

**Run Exit Rule Configuration Changes Report**

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

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

**To run the Exit Point Configuration Changes Report**

1) Access the Network Reports interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 1 (Remote Exit Rules Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

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

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

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

See also

Working with Exit Rules
AI Rules

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

This section includes the following topics:

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

See also

Network Security
Working with AI Rules

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

- Display List of AI Rules
- Manage AI Rules

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

To access the **Work with AI Rules** interface

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

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

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

4) At the **Selection or command** prompt, enter 6 (AI Rules).

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

**See also**

- **AI Rules**

Display List of AI Rules

Use this task to display AI rules:

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

Display List

Use this task to display the list of exit rules.

To display the list of exit rules

1) Access the TGSecure Main menu.

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

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

4) At the Selection or command prompt, enter 6 (AI Rules).

5) Press Enter. The Work with AI Rules interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>Type of AI rule:</td>
</tr>
<tr>
<td></td>
<td>*PRE - Check AI rule before exit point rules</td>
</tr>
<tr>
<td></td>
<td>*POST - Check AI rule after regular exit point rules</td>
</tr>
<tr>
<td>User</td>
<td>User or user group to which the rule applies</td>
</tr>
<tr>
<td>Server</td>
<td>Server on which the rule applies</td>
</tr>
<tr>
<td>Function</td>
<td>Function to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address to which the rule applies</td>
</tr>
<tr>
<td>Calendar</td>
<td>Applicable calendar</td>
</tr>
<tr>
<td></td>
<td>Note: the calendar limits when the rule is applicable.</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>Action</td>
<td>The level at which action is taken:</td>
</tr>
<tr>
<td></td>
<td>*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>Object Details</td>
<td>Short description of the object to which access was attempted</td>
</tr>
</tbody>
</table>

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

**To sort the list**

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

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

**Move to Position in List**

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

**To move to a specific position within the list**

1) Access the **Work with AI Rules** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press Enter. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**Filter List**

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

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

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

**See also**
Working with AI Rules
Manage AI Rules

Use this task to manage AI rules.

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

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

Access the Work with AI Rules Interface

To access the Work with AI Rules interface

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

Add AI Rule

Use this task to add an AI rule.

**To add an AI rule**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>Enter the rule type:</td>
</tr>
<tr>
<td></td>
<td>*PRE - Check AI rule before exit point rules</td>
</tr>
<tr>
<td></td>
<td>*POST - Check AI rule after regular exit point rules</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user or user group to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>Enter the IP address to which the rule applies</td>
</tr>
<tr>
<td>Operation Server</td>
<td>Enter the operation server to which the rule applies</td>
</tr>
<tr>
<td>Calendar</td>
<td>Enter the applicable calendar</td>
</tr>
<tr>
<td>Note:</td>
<td>The calendar limits when the rule is applicable.</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Identify whether to enable alerting:</td>
</tr>
<tr>
<td><em>YES</em></td>
<td>Alerts enabled</td>
</tr>
<tr>
<td><em>NO</em></td>
<td>Alerts disabled</td>
</tr>
<tr>
<td>Action</td>
<td>Enter the level at which to execute the action:</td>
</tr>
<tr>
<td><em>EXITLVL</em></td>
<td>Exit point level</td>
</tr>
<tr>
<td>Note:</td>
<td>If the action failed, you will see <em>FAIL</em> in this column.</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>Enter the number of transactions required to trigger the rule</td>
</tr>
<tr>
<td>1-999999</td>
<td></td>
</tr>
<tr>
<td>Event Frequency</td>
<td>Enter the number of events required to trigger the rule</td>
</tr>
<tr>
<td>1-999999</td>
<td></td>
</tr>
<tr>
<td>Rule Description</td>
<td>Enter a short description that describes the purpose of the rule.</td>
</tr>
<tr>
<td>Type of object</td>
<td>Enter the object to which the rule applies</td>
</tr>
<tr>
<td><em>QSYS</em></td>
<td>Limit the rule to QSYS objects</td>
</tr>
<tr>
<td><em>IFS</em></td>
<td>Limit the rule to IFS objects</td>
</tr>
<tr>
<td><em>NONE</em></td>
<td>Include both QSYS and IFS objects</td>
</tr>
</tbody>
</table>

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

4) Press **Enter**.

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

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>you selected <em>QSYS</em></td>
<td>Complete the following additional fields:</td>
</tr>
<tr>
<td>as the object type</td>
<td><strong>Object Name</strong> - Name of QSYS object to which the rule applies</td>
</tr>
<tr>
<td></td>
<td><strong>Object Library</strong> - Name of the QSYS library to which the rule applies</td>
</tr>
<tr>
<td></td>
<td><strong>Object Type</strong> - Type of QSYS object to which the rule applies</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>You will receive a warning message if you enter a name/library/type combination that does not</td>
</tr>
<tr>
<td></td>
<td>currently exist on the server. If this is your intention (e.g., you are creating a rule for</td>
</tr>
<tr>
<td></td>
<td>future use or you are creating a generic rule that you plan to implement across multiple</td>
</tr>
<tr>
<td></td>
<td>servers), then ignore the warning by clicking <strong>Enter</strong>. If it was not your intention to create</td>
</tr>
<tr>
<td></td>
<td>a rule that cannot be applied on the current server, then make any necessary corrections at</td>
</tr>
<tr>
<td></td>
<td>this time.</td>
</tr>
</tbody>
</table>
you select `IFS` as the object type

If you select `IFS` as your object type, complete the following additional field:

**IFS Object** - Enter the file path to the IFS object

you select `ONE`

No additional fields are required

6) Press **Enter**:

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

**Edit AI Rule**

Use this task to edit an existing AI rule.

**To edit an AI rule**

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

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

3) Press **Enter**.

4) Modify the parameters as necessary:

5) Press **Enter**.

**Copy AI Rule**

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

**To copy an AI rule**

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

2) In the **OPT** column for the desired **AI** rule, enter **3** (Copy).

3) Press **Enter**.

4) Modify the parameters as necessary.

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

5) Press **Enter**.
Delete AI Rule

Use this task to delete an AI rule.

To delete an AI rule

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

Display List of Users

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

Tip: Group names always begin with a colon.

To display the list of users

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

Display List of Clients

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

Tip: Group names always begin with a colon.

To display the list of clients

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

Display List of Servers

Use this task when the AI rule definition includes a network group in the Server Name field. You can access the network group at this point to display its details or modify the group.
To display the list of servers

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

Display List of Operations

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

To display the list of operations

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

Display List of Objects

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

To display the list of objects

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

See also

Working with Al Rules
Access Escalation Management

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

To access the Access Escalation Management interface

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

Use the Access Escalation Management interface to do the following:

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

See also

Getting Started
Access Escalation Defaults

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

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

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

The section includes the following topics:

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

**See also**

Access Escalation Management
Working with Access Escalation Management Defaults

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

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

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

To access the Work with Access Escalation interface

1) Log into TGSecure. The Main menu appears.

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

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

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

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

See also

Access Escalation Management
Display Access Escalation Defaults

Use this task to display the Access Escalation default settings.

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

To display Access Escalation defaults

1) Access the TGSecure Main menu.

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

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Y - Enable tracking of changes</td>
<td></td>
</tr>
<tr>
<td>N - Disable tracking of changes</td>
<td></td>
</tr>
</tbody>
</table>

Tip: This flag must be set to Y if you plan to run access escalation change reports.

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

**See also**

*Working with Access Escalation Management Defaults*
Manage Access Escalation

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

- Access the Access Escalation Interface
- Modify Access Escalation Defaults
- Enable Access Escalation Change Auditing

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

Access the Access Escalation Interface

**To access the Work with Access Escalation interface**

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

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

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

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

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

Modify Access Escalation Defaults

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

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

**To modify access escalation defaults**

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

2) Modify the parameters as necessary.

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

3) Press **Enter** twice.

Enable Access Escalation Change Auditing

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

**Tip:** Tracking is required if you plan to **run access escalation change reports**.
To enable access escalation configuration change tracking

1) Access the Work with Access Escalation interface.

2) In the Audit Configuration Changes field, ensure the flag is set to Y (Yes).

3) Press Enter twice.

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

See also

Working with Access Escalation Management Defaults
Run Access Escalation Report

Use this task to generate the Access Escalation report.

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

To run the Access Escalation Reports

1) Access the TGSecure Main menu.

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

3) Press Enter.

4) At the Selection or command prompt, enter 20 (Access Escalation Reports).

5) Press Enter.

6) At the Selection or command prompt, enter the category of the report type you want to run.

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access Escalation Usage Report</td>
</tr>
<tr>
<td>2</td>
<td>Access Escalation Configuration Report</td>
</tr>
<tr>
<td>3</td>
<td>Access Escalation Change Report</td>
</tr>
</tbody>
</table>

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

7) Press Enter.

8) Choose the desired report from the list.

9) Press Enter.

See also

Working with Access Escalation Management Defaults
Entitlements

Use the Entitlements feature to allow users to borrow the access rights of a higher-privileged user (swap user) temporarily to execute an activity on an object.

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

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

This section contains the following topics:

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

See also

Access Escalation Management
Working with Entitlements

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

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

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

**To access the Work with Entitlements interface**

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

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

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

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

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

**To access the AEM interface**

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

2) Press **Enter**. The **AEM** interface is displayed.

**See also**

Entitlements
Display List of Entitlements

Use this task to display entitlements.

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

Display List

Use this task to display the list of entitlements.

To display the list of entitlements

1) Access the TGSecure Main menu.

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

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

4) At the Selection or command prompt, enter 1 (Work with Entitlements).

5) Press Enter. The Work with Entitlements interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Status</td>
<td>Whether the entitlement is enabled: Y - Enabled</td>
</tr>
<tr>
<td></td>
<td>N - Disabled</td>
</tr>
<tr>
<td>User</td>
<td>User or user group to which the entitlement applies</td>
</tr>
<tr>
<td>Object</td>
<td>Object or object group 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>Aut Req?</td>
<td>Whether the 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>Entitlement Description</td>
<td>Short description identifying the purpose of the entitlement</td>
</tr>
</tbody>
</table>
Sort List

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

To sort the list

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

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

Move to Position in List

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

To move to a specific position within the list

1) Access the Work with Entitlements interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.
– Add an asterisk after text (e.g., report*) to find list items that start with specific text.
– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

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

4) Press Enter. The system filters the results based on the criteria you defined for the subset.

See also

Working with Entitlements
Manage Entitlements

Use this task to manage entitlements.

- Access the Work with Entitlements Interface
- Add Entitlement
- Edit Entitlement
- Copy Entitlement
- Delete Entitlement

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

Access the Work with Entitlements Interface

To access the Work with Entitlements interface

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

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

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

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

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

Add Entitlement

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

To add entitlement

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

2) Press the **F6** (Add) function key.

3) Enter the parameters necessary to define the entitlement.

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>User or user group to which the entitlement applies</td>
</tr>
<tr>
<td>Object Name</td>
<td>Object or object group to which the entitlement applies</td>
</tr>
</tbody>
</table>
To copy entitlement

Copy Entitlement

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

To copy entitlement

<table>
<thead>
<tr>
<th>Object Library</th>
<th>Library in which the object resides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object 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>Server Name</td>
<td>Server or server group from which the user must be accessing the system</td>
</tr>
<tr>
<td>Calendar</td>
<td>Calendar to be applied</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>Authentication?</td>
<td>Whether the 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>Alerting?</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>Entitlement Description</td>
<td>Short description identifying the purpose of the entitlement</td>
</tr>
</tbody>
</table>

4) Press **Enter** twice.

**Edit Entitlement**

Use this task to edit an entitlement.

**To edit entitlement**

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

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

3) Press **Enter**.

4) Modify the parameters as necessary.

---

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

5) Press **Enter** twice.

**Copy Entitlement**

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

**To copy entitlement**
1) Access the **Work with Entitlement** interface.

2) In the OPT column for the desired entitlement, enter 3 (Copy).

3) Press **Enter**.

4) Modify the parameters as necessary.

5) Press **Enter**.

### Delete Entitlement

Use this task to delete an entitlement.

**To delete entitlement**

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

2) In the OPT column for the desired group, enter 4 (Delete).

3) Press **Enter**.

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

5) Press **Enter**.

**See also**

*Working with Entitlements*
Run Entitlement Reports

Use this task to generate the following entitlement reports:

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

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

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

Access the Access Escalation Reports Interface

To access the Access Escalation Reports interface

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

Run Entitlement Usage Report

Use this report to display entitlement usages details.

To run the Entitlement Usage Report

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

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

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

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

**Run Entitlement Configuration Report**

Use this report to display entitlement configuration details.

**To run the Entitlement Configuration Report**

1) Access the **Access Escalation Report** interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 3 (Entitlements).

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

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

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

**Run Entitlement Configuration Changes Report**

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

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

**To run the Entitlement Configuration Changes Report**

1) Access the **Access Escalation Report** interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 3 (Entitlements Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.
7) Enter the desired output format in the Report output type field.

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

See also

Working with Entitlements
Access Control

Use the **Access Control** feature to grant or revoke access to the **Access Escalation Management (AEM)** interface. The AEM interface is the tool from which a user can execute an entitlement.

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

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

This section contains the following topics:

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

**See also**

- Access Escalation Management
Working with Access Control

Use the Access Control feature to do the following:

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

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

To access the Work with Access Control interface

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

See also

Access Control
Display Who Has Access to the AEM Interface

Use this task to display access control options.

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

Display List

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

To display the list of users who have access control

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

Sort List

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

To sort the list

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

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

Move to Position in List

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

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

**Filter List**

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

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

**To filter the list using a subset**

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

**See also**

*Working with Access Control*
Manage Access Control

Use this task to manage access control options.

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

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

Access the Work with Access Control Interface

**To access the Work with Access Control interface**

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 4 (Access Escalation Management).

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

4) At the Selection or command prompt, enter 3 (Work with Access Control).

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

Add Access Control

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

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

1) Access the Work with Access Control interface.

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

3) Enter the parameters necessary to define the control.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</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>
</tbody>
</table>

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

Edit Access Control

Use this task to modify an exiting access control record.

To edit entitlement

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

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

5) Press Enter twice.

Copy Access Control

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

To copy access control

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

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

5) Press Enter.

Delete Access Control

Use this task to delete an access control record.

To delete entitlement

1) Access the Work with Entitlement interface.
2) In the OPT column for the desired group, enter 4 (Delete).
3) Press Enter.

4) Review the record to ensure you are deleting the right user.

5) Press Enter.

**See also**

*Working with Access Control*
Run Access Control Reports

Use this task to generate the following access control reports:

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

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

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

**Access the Escalation Reports interface**

To access the Access Escalation Reports interface

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

**Run Access Control Configuration Report**

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

To run the Access Control Configuration Report

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

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

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

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

### Run Access Control Change Report

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

- **Tip:** You must enable auditing to produce change reports. See [Enable AEM Change Auditing](#) for additional information.

### To run the Access Control Change Report

1) Access the **Access Escalation Report** interface.

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

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 4 (Access Control Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

- **Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see [Run TGSecure Reports](#).

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

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

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

### See also

- [Working with Access Control](#)
Execute an Entitlement Using the AEM Interface

Use this task to access the Access Escalation Management (AEM) interface and execute an entitlement (which allows the users to borrow the privileges of a swap profile).

The following requirements must be met for a user to access the AEM interface and execute a task (e.g., download a highly sensitive HR document) using a swap profile:

- **Requirement 1:** The user must have access to the AEM interface.
- **Requirement 2:** An entitlement must be defined for the user.
- **Requirement 3:** The criteria in the entitlement must be met.
- **Requirement 4:** A user with appropriate privileges to perform the task must be identified as the swap user within the entitlement.

To access the AEM interface

1) At the **Selection or command** prompt, enter **TGACCMGR**.
2) Press **Enter**.
3) Enter the program/command you want to execute.
4) Enter the appropriate swap profile. This is the user who has the privilege to perform the command/program you are attempting to execute.
5) Enter your user password (for some entitlements this is optional).
6) Enter a description of why you are performing this task.
7) Press **Enter**.

**See also**

Working with Access Control
File Editor

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

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

This section includes the following topics:

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

**See also**

Access Escalation Management
Working with File Editor

Use the File Editor feature to do the following:

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

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

To access the Work with File Editors interface

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

See also

File Editor
Display List of File Editors

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

To display the list of File Editors

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

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

3) Press **Enter**.

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

5) Press **Enter**. The **Work with File Editors** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**See also**

[Working with File Editor](#)
Manage File Editors

Use this task to manage the following file editors:

- Add File Editor
- Edit File Editor
- Copy File Editor
- Delete File Editor

To access the Work with File Editors interface

1) Access the TGSecure Main menu.

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

3) Press Enter.

4) At the Selection or command prompt, enter 11 (Work with File Editors).

5) Press Enter. The Work with File Editors interface is displayed.

Add File Editor

Use this task to add a file editor.

To add file editor

1) Access the Work with File Editors interface.

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

3) Enter the parameters necessary to define the file editor.

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

4) Enter a description for the file editor.

5) Press Enter twice.

Edit File Editor

Use this task to edit a file editor.

To edit file editor

1) Access the Work with File Editor interface.

2) In the OPT column for the desired file editor, enter 2 (Edit).

3) Press Enter.

4) Modify the parameters as necessary.
5) Press **Enter** twice.

**Copy File Editor**

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

**To copy file editor**

1) Access the **Work with File Editor** interface.

2) In the **OPT** column for the desired file editor, enter **3 (Copy)**.

3) Press **Enter**.

4) Modify the parameters as necessary.

5) Press **Enter**.

**Delete File Editor**

Use this task to delete a file editor.

**To delete file editor**

1) Access the **Work with File Editor** interface.

2) In the **OPT** column for the desired file editor, enter **4 (Delete)**.

3) Press **Enter**.

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

5) Press **Enter**.

**See also**

*Working with File Editor*
Run File Editor Reports

Use this task to generate the following file editor reports:

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

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

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

Access the Access Escalation Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure Main menu.

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

3) Press Enter.

4) At the Selection or command prompt, enter 20 (Access Escalation Reports).

5) Press Enter. The Access Escalation Reports interface is displayed.

Run File Editors Configuration Report

Use this task to display file editor configuration details.

To run File Editor Report

1) Access the Access Escalation Reports interface

2) At the Selection or command prompt, enter 2 (Access Escalation Configuration Reports).

3) Press Enter. The Access Escalation Configuration Reports interface is displayed

4) At the Selection or command prompt, enter 2 (File Editors).

5) Press Enter.

6) Modify the run criteria as necessary.

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

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

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

**Run File Editor Change Report**

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

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

**To run File Editor Change Report**

1) Access the Access Escalation Reports interface.

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

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

4) At the **Selection or command** prompt, enter 2 (File Editors Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

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

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

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

**See also**

[Working with File Editor](#)
**Inactive Session Lockdown**

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

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

**To access the Inactive Session Lockdown interface**

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

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

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

**See also**

Getting Started
Inactive Session Lockdown Defaults

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

Inactive session lockdown defaults allow you to define the following:

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

This section includes the following topics:

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

See also

Inactive Session Lockdown
Working with Inactive Session Lockdown Defaults

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

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

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

To access the Work with Inactive Session Lockdown Settings Interface

1) Access the TGSecure Main menu.

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

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

4) At the Selection or command prompt, enter 10 (ISL Defaults).

5) Press Enter. The Work with Inactive Session Lockdown Settings interface is displayed.

See also

Inactive Session Lockdown
Display Inactive Session Lockdown Defaults

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

To display the Interactive Session Lockdown defaults

1) Access the TGSecure Main menu.

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

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

4) At the Selection or command prompt, enter 10 (ISL Defaults).

5) Press Enter. The Work with Inactive Session Lockdown Settings interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Interval</td>
<td>How often the system checks for inactive sessions</td>
</tr>
<tr>
<td>Audit Status</td>
<td>Whether the system should track (audit) inactive sessions data</td>
</tr>
<tr>
<td></td>
<td>*YES - Enable auditing</td>
</tr>
<tr>
<td></td>
<td>*NO - Disable auditing</td>
</tr>
<tr>
<td></td>
<td>Tip: Set this flag to *YES if you plan to run ISL usage reports.</td>
</tr>
<tr>
<td>Audit Journal</td>
<td>Journal in which to store ISL usage data</td>
</tr>
<tr>
<td></td>
<td>Note: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
</tr>
<tr>
<td>Audit Journal Library</td>
<td>Library in which the journal resides</td>
</tr>
<tr>
<td>Audit Configuration Changes</td>
<td>Whether to collect data about ISL configuration 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>
<tr>
<td></td>
<td>Tip: Set this flag to Y if you plan to run ISL change reports.</td>
</tr>
<tr>
<td></td>
<td>Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL, this indicates that configuration changes are being tracked in all modules.</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerts are enabled (stored in the alert queue):</td>
</tr>
<tr>
<td></td>
<td>*YES - Enable alerts (create admin alert)</td>
</tr>
<tr>
<td></td>
<td>*NO - Disable alerts</td>
</tr>
<tr>
<td>Alert Message Queue</td>
<td>Queue in which to store alerts</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Alert Message Queue Library</td>
<td>Library in which to store the queue</td>
</tr>
<tr>
<td>Temporary Disconnect Message</td>
<td>Custom message defined by the administrator and used to inform the user that their session is about to be locked or ended</td>
</tr>
<tr>
<td>Temporary Sign on Screen Header</td>
<td>The title assigned to the message screen that notifies the user of an impending disconnect (e.g., company name)</td>
</tr>
<tr>
<td>Send Warning</td>
<td>Whether alerts are sent to warn the user of an impending disconnect</td>
</tr>
<tr>
<td><em>YES</em> - Warning alert enabled</td>
<td><em>NO</em> - Warning alert disabled</td>
</tr>
<tr>
<td>Warning Interval</td>
<td>When to send the user a warning message (seconds before disconnect)</td>
</tr>
<tr>
<td>Revoke Authority</td>
<td>Whether to revoke a user's authority when they are locked or their session is ended</td>
</tr>
<tr>
<td><em>YES</em> - The user's session is locked or ended, and the user's authority is revoked</td>
<td><em>NO</em> - The user's session is locked or ended, but the user's authority is maintained</td>
</tr>
</tbody>
</table>

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

**Warning:** Consider the workflow consequences thoroughly before enabling this feature.

**See also**

*Working with Inactive Session Lockdown*
Manage Inactive Session Lockdown

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

- Access the Work with Interactive Session Lockdown Settings Interface
- Enable ISL Auditing
- Enable ISL Change Auditing
- Enable ISL Alerts
- Set Check Interval
- Set Warning Interval
- Set Disconnect Message
- Set Revoke Authority
- Start Monitor
- End Monitor
- Check Monitor Status

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

### Access the Work with Interactive Session Lockdown Settings Interface

**To access the Work with Interactive Session Lockdown Settings interface**

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

### Enable ISL Auditing

Use this task to enable inactive session auditing.

**Tip:** Auditing is required if you plan to run [ISL usage reports](#).

**To enable the ISL auditing**

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

Enable ISL Change Auditing

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

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

To enable tracking of configuration changes in the ISL module

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

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

Enable ISL Alerts

Use this task to enable ISL alerts.

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

To enable ISL alerts

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

Set Check Interval

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

To set the check interval

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

**Set Warning Interval**

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

**To set the warning interval**

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

2) In the **Send Warning** field, enter one of the following:
   - {*YES*} - Enable the warning feature
   - {*NO*} - Disable the warning feature

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

   **Note:** This value must be greater or equal to the check interval.

4) Press Enter twice.

**Set Disconnect Message**

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

**To set the disconnect message**

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

2) In the **Temporary Disconnect Message** field, enter the desired message.

3) In the **Temporary Sign on Screen Header** field, enter the desired disconnect dialog box heading.

4) Press Enter twice.

**Set Revoke Authority**

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

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

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

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

2) In the **Revoke Authority** field, enter one of the following:
   - (*)YES - Enable the revoke feature
   - (*)NO - Disable the revoke feature

3) Press **Enter** twice.

**Start Monitor**

Use this task to start ISL monitoring.

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

**To monitor status**

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

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

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

3) Press **Enter**.

**End Monitor**

Use this task to end ISL monitoring.

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

**To monitor status**

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

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

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

3) Press **Enter**.

**Check Monitor Status**

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

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

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

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

3) Press **Enter**.

**See also**

*Working with Inactive Session Lockdown*
Run Inactive Session Lockdown Reports

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

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

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

To access the Inactivity Session Reports interface

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

Run Inactivity Disconnect Report

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

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

To run the Inactivity Disconnect report

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

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
7) Enter the desired output format in the Report output type field.
8) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Inactivity Session Configuration Settings Report

Use this report to view the ISL configuration settings.

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

To run the Inactivity Session Configuration Settings report

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

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

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

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

Run Inactivity Session Configuration Changes Report

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

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

To run the Inactivity Session Configuration Changes report

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

4) At the Selection or command prompt, enter 1 (Inactivity Session Configuration Changes).

5) Press Enter.

6) Modify the report run criteria as necessary.

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

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

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

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

**See also**

Working with Inactive Session Lockdown Defaults
Inactive Session Rules

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

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

This section includes the following topics:

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

See also

Inactive Session Lockdown
Working with Inactive Session Rules

Use the Inactive Session Rules feature to do the following:

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

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

To access the Work with Inactive Session Rules interface

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

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

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

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

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

See also

Inactive Session Rules
Display Inactive Session Rules

Use this task to display inactive session rules.

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

Display List

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

To display the list of inactive session rules

1) Access the TGSecure Main menu.

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

3) Press Enter.

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

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

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

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

To sort the list

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

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

Move to Position in List

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

To move to a specific position within the list

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

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

Filter List

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

Tip: Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.
– Add an asterisk after text (e.g., report*) to find list items that start with specific text.
– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

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

Working with Inactive Session Rules

Note: The system filters the results based on the criteria you defined for the subset.
Manage Inactive Session Rules

Use this task to manage inactive session rules.

- Access the Work with Inactive Session Interface
- Add Inactive Session Rule
- Edit Inactive Session Rule
- Copy Inactive Session Rule
- Delete Inactive Session Rule

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

Access the Work with Inactive Session Interface

**To access the Work with Inactive Session interface**

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

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

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

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

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

Add Inactive Session Rule

Use this task to add an inactive session rule.

**To add an inactive session rule**

1. Access the **Work with Inactive Session Rules** interface.

2. Press the **F6** (Add) function key.

3. Define the rule using the fields provided.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Rule Type  | Enter the type of rule:  
*PGM* - Rule that affects a program  
*WRKSTN* - Rule that affects a workstation  
*SBSD* - Rule that affects a subsystem (e.g., country, region, department)  
*CTL* - Rule that affects a controller  
*USER* - Rule that affects a user  
**Note:** If *USER* is specified, then enter user name or user group the **Object** field. |
| Object     | Enter the object name or object group to which the rule is applicable  
**Tip:** Enter **ALL** to apply the rule to all objects, except when **Rule Type** is defined as *USER*. |
4) Press Enter twice.

**Edit Inactive Session Rule**

Use this task to edit an existing ISL rule.

*To edit an inactive session rule*

1) Access the **Work with Inactive Session Rules** interface.

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

3) Press Enter.

4) Modify the parameters as necessary.

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

5) Press Enter twice.

**Copy Inactive Session Rule**

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

*To copy an inactive session rule*

1) Access the **Work with Inactive Session Rules** interface.

2) In the OPT column for the desired rule, enter 3 (Copy).

3) Press Enter.

4) Modify the parameters as necessary.
5) Press **Enter** twice.

**Delete Inactive Session Rule**

Use this task to delete an ISL k rule.

**To delete an inactive session rule**

1) Access the **Work with Inactive Session Rules** interface.

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

3) Press **Enter**.

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

5) Press **Enter** twice.

**See also**

*Working with Inactive Session Rules*
Run Inactive Session Rules Reports

Use this task to generate the following inactive session reports:

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

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

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

Access the Inactive Sessions Report Interface

**To access the Inactive Sessions Reports interface**

1) Access the TGSecure Main menu.

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

3) Press Enter.

4) At the Selection or command prompt, enter 20 (Inactive Session Reports).

5) Press Enter. The Inactivity Session Reports interface is displayed.

Run Inactivity Session Inclusion Exception Rules Report

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

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

**To run the Inactivity Session Inclusion Exception Rules report**

1) Access the Inactivity Session Reports interface.

2) At the Selection or command prompt, enter 2 (Inactive Session Configuration Reports).

3) Press Enter. The Inactivity Session Configuration Reports interface is displayed.

4) At the Selection or command prompt, enter 3 (Inactive Session Inclusion Exception Rules).

5) Press Enter.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
7) Enter the desired output format in the **Report output type** field.

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

### Run Inactivity Session Rules Change Report

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

**Tip**: You must enable auditing to produce change reports. See [Manage Inactive Session Rules](#) for additional information.

### To run the Inactivity Session Rules Change report

1) Access the **Inactivity Session Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Inactivity Session Changes Reports).

3) Press **Enter**. The **Inactivity Session Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 3 (Inactivity Session Rule Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

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

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

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

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

**See also**

[Working with Inactive Session Rules](#)
**Disconnection Options**

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

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

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

This section includes the following topics:

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

**See also**

Inactive Session Lockdown
Working with Disconnect Options

Use the Disconnect Options feature to do the following:

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

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

To access the Work with Disconnect Option interface

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

See also

Disconnection Options
Display Disconnect Options

Use this task to display disconnect options.

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

Display List

Use this task to display the list of disconnect options.

To display the list of disconnect options

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect Option</td>
<td>Name assigned to the disconnect option</td>
</tr>
<tr>
<td>Time Limit</td>
<td>Time the system must remain inactive to trigger the disconnect</td>
</tr>
</tbody>
</table>
| Disconnect Type  | The type of disconnect:  
| ENDJOB - End the job (user must restart their job)  
| DSCJOB - Disconnect (pause) the job and show the IBM standard disconnect message  
| TGDSCJOB - Disconnect (pause) the job and show a custom disconnect message  
| HLDJOB - Hold (freeze) the job (only an admin can unfreeze a job)  
| SIGNOFF - End the session (user must restart their session and job) |

Tip: If TGDSCJOB is defined as the disconnect type, ensure that program ISL80001P in library TGPROD is defined as the user's initial. To see which program is defined as the initial program for the user, at the Selection or command prompt, enter DSPUSRPRF. Enter the desired user in the User Profile field. Press Enter. Page down until you see Initial Program and Library entries. If ISL80001P is not defined as the initial program, you must either use a different disconnect type or change the user's initial program.

Sort List

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

To sort the list

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

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

Move to Position in List

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

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

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

Filter List

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

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

To filter the list using a subset
1) Access the Work with Disconnect Options interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter.

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

See also

Working with Disconnect Options
Manage Disconnect Options

Use this task to manage disconnect options.

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

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

To access the Work with Disconnect Options interface

1) Access the TGSecure Main menu.

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

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

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

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

Add Disconnect Option

Use this task to add a disconnect option.

To add a disconnect option

1) Access the Work with Disconnect Options interface.

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

3) Define the disconnect option using the fields provided.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect Option</td>
<td>Enter the name you want to assign the disconnect option</td>
</tr>
<tr>
<td>Time Limit</td>
<td>Enter the time the system must remain inactive to trigger the disconnect option</td>
</tr>
</tbody>
</table>
### Work with Disconnect Options

<table>
<thead>
<tr>
<th>Disconnect Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENDJOB</td>
<td>End the job (user must start the job over)</td>
</tr>
<tr>
<td>DSCJOB</td>
<td>Disconnect (pause) the job and show the IBM standard disconnect message</td>
</tr>
<tr>
<td>TGDSCJOB</td>
<td>Disconnect (pause) the job and show a custom disconnect message</td>
</tr>
<tr>
<td>HLDJOB</td>
<td>Hold (freeze) the job (only an admin can unfreeze a job)</td>
</tr>
<tr>
<td>SIGNOFF</td>
<td>Signoff from the server</td>
</tr>
</tbody>
</table>

**Warnings:** Do not select **HLDJOB** if a trained admin will not be available to unfreeze the job.

**Tip:** If you select **TGDSCJOB**, ensure that program **ISL80001P** in library **TGPROD** is defined as the user's initial program. To see which program is defined as the initial program for the user, at the **Selection or command** prompt, enter **DSPUSRPRF**. Enter the desired user in the **User Profile** field. Press **Enter**.

- Page down until you see **Initial Program** and **Library** entries. If **ISL80001P** is not defined as the initial program, you must either use a different disconnect type or change the user's initial program.

4) Press **Enter** twice.

## Edit Disconnect Option

Use this task to edit an existing disconnect option.

### To edit a disconnect option

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

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

5) Press **Enter** twice.

## Copy Disconnect Option

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

### To copy a disconnect option

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

Delete Disconnect Option

Use this task to delete a disconnect option.

To delete a disconnect option

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

See also

Working with Disconnect Options
Run Disconnect Option Reports

Use this task to generate the following disconnection option reports:

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

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

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

Access the Inactive Session Reports Interface

To access the Inactive Sessions Reports interface

1) Access the TGSecure Main menu.

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

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

4) At the Selection or command prompt, enter 20 (Inactive Session Reports).

5) Press Enter. The Inactivity Session Reports interface is displayed.

Run Inactivity Session Disconnect Option Report

Use this report to view the list of disconnect options.

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

To run the Inactivity Session Disconnect Option report

1) Access the Inactivity Session Reports interface.

2) At the Selection or command prompt, enter 2 (Inactivity Session Configuration Reports).

3) Press Enter. The Inactivity Session Configuration Reports interface is displayed.

4) At the Selection or command prompt, enter 2 (Inactivity Session Disconnect Options).

5) Press Enter.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

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

8) Press **Enter**.

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

---

**Run Inactivity Session Disconnect Option Change Report**

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

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

---

**To run the Inactivity Session Disconnect Option Change report**

1) Access the **Inactivity Session Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Inactivity Session Changes Reports).

3) Press **Enter**. The **Inactivity Session Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 2 (Inactivity Session Disconnect Option Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

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

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

9) Enter the desired output format in the **Report output type** field.

10) Press **Enter**.

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

---

**See also**

**Working with Disconnect Options**
Resource Manager

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

To access the Resource Manager interface

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

Use the Resource Manager interface to do the following:

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

See also

Getting Started
Resource Manager Defaults

This section describes working with Resource Manager defaults.

Resource Manager defaults allow you to define the following:

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

This section includes the following topics:

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

See also

Resource Manager
Working with Resource Manager Defaults

Use the Resource Manager Defaults settings to do the following:

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

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

**To access the Resource Manager interface**

1) Log into TGSecure. The Main menu appears.

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

3) Press Enter. The Resource Manager interface is displayed.

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

5) Press Enter. The Resource Manager Defaults interface is displayed.

**See also**

Resource Manager Defaults
## Display Resource Manager Defaults

Use this task to display the Resource Manager default settings.

### To display the Resource Manager defaults

1. Access the TGSecure Main menu.

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

3. Press **Enter**. The Resource Manager interface is displayed.

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

5. Press **Enter**. The Resource Manager Defaults interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Journal</td>
<td>Journal in which to store resource manager usage data</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: The Audit Journal and Library fields must be filled with a valid value if you plan to run <a href="#">Resource Manager usage reports</a>.</td>
</tr>
<tr>
<td>Audit Journal Library</td>
<td>Library in which the audit journal resides</td>
</tr>
<tr>
<td>Audit Configuration Changes</td>
<td>Whether to collect data about resource changes:</td>
</tr>
<tr>
<td></td>
<td><strong>Y</strong> - Enable tracking of changes</td>
</tr>
<tr>
<td></td>
<td><strong>N</strong> - Disable tracking of changes</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: Set this flag to <strong>Y</strong> if you plan to run the <a href="#">Resource Manager change reports</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see <strong>NONE</strong> 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 <strong>PARTIAL</strong>, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see <strong>ALL</strong>, this indicates that configuration changes are being tracked in all modules</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerts are enabled:</td>
</tr>
<tr>
<td></td>
<td><strong>YES</strong> - Enable alerts (create admin alert)</td>
</tr>
<tr>
<td></td>
<td><strong>NO</strong> - Disable alerts</td>
</tr>
<tr>
<td>Alert Message Queue</td>
<td>Queue in which to store alerts</td>
</tr>
<tr>
<td>Alert Message Queue Library</td>
<td>Library in which to store the queue</td>
</tr>
</tbody>
</table>
See also

Working with Resource Manager Defaults
Manage Resource Manager Defaults

Use this task to manage the Resource Manager default settings.

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

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

Access the Resource Manager Defaults Interface

To access the Resource Manager Defaults interface

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

Enable Resource Change Auditing

Use this task to enable resource change auditing.

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

To enable the resource auditing

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

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

Enable Resource Change Alerts
Use this task to enable inactive session alerts.

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

To enable resource alerts

1) Access the Resource Manager Defaults interface.

2) In the Alert Status field, enter ‘YES’.

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

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

5) Press Enter.

See also

Working with Resource Manager Defaults
Run Resource Manager Reports

Use this task to generate the following Resource Manager reports:

- Access the Resource Manager Reports Interface
- Run Resource Manager Configuration Report
- Run Resource Manager Configuration Change Report
- Run Resource Manager Out of Compliance Data
- Run Resource Manager Out of Compliance Data Changes Report

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

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

Access the Resource Manager Reports Interface

To access the Resource Manager Reports interface

1) Access the TGSecure Main menu.

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

3) Press Enter. The Resource Manager interface is displayed.

4) At the Selection or command prompt, enter 20 (Resource Manager Reports).

5) Press Enter. The Resource Manager Reports interface is displayed.

Run Resource Manager Configuration Report

Use this report to view the Resource Manager configuration details.

To run the Resource Manager Configuration Report

1) Access the Resource Manager Reports interface.

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

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

4) At the Selection or command prompt, enter 1 (Resource Manager Configuration).

5) Press Enter.

6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
7) Enter the desired output format in the **Report output type** field.

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

**Run Resource Manager Configuration Change Report**

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

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

**To run the Resource Manager Configuration Change Report**

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

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

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

4) At the **Selection or command** prompt, enter 1 (Resource Manager Configuration Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

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

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

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

**Run Resource Manager Out of Compliance Data**

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

**To run the Resource Manager Out of Compliance Report**

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

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

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

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

6) Modify the run criteria as necessary.

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

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

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

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

### Run Resource Manager Out of Compliance Data Changes Report

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

**To run the Resource Manager Out of Compliance Data Changes Report**

1) Access the Resource Manager Reports interface.

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

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

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

5) Press Enter.

6) Modify the run criteria as necessary.

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

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

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

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

**See also**

Working with Resource Manager Defaults
Authority Schemas

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

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

This section includes the following topics:

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

See also

Resource Manager
Working with Authority Schemas

Use the Authority Schemas feature to do the following:

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

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

To access the authority schemas interface

1) Log into TGSecure. The Main menu appears.

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

3) Press Enter. The Resource Manager interface is displayed.

4) At the Selection or command prompt, enter 1 (Authority Schema Configuration).

5) Press Enter. The Work with Authority Schemas interface is displayed.

See also

Authority Schemas
Display Authority Schemas

Use this task to display the authority schemas.

- **Sort List of Schemas**
- **Move to Position in List of Schemas**
- **Display List of Schemas Details**
- **Sort List of Schemas Details**
- **Move to Position in List of Schemas Details**
- **Filter List Schemas Details**

**Display List of Schemas**

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

**To display the list of authority schemas**

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

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

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

4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).

5) Press **Enter**. The **Work with Authority Schemas** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema ID</td>
<td>ID assigned to the schema</td>
</tr>
<tr>
<td>Compliances</td>
<td>Date and time at which the last check for authority schema compliance was performed</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Date and time at which user authorities were compared to the authority schema and compliance with the schema was enforced</td>
</tr>
</tbody>
</table>
| Alert Status     | Whether alerts are enabled:  
  *YES* - Enable alerts (create admin alerts)  
  *NO* - Disable alerts |
| Schema Description | Description of the authority schema                                          |
| Compliance Status | Whether the current authority levels comply with the schema  
  *PASS* - User authorities comply with the current authority scheme  
  *FAIL* - User authorities do not comply with the current authority scheme |

**Note**: See Manage Authority Scheme for instruction on enforcing an authority schema.

**Sort List of Schemas**

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

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

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

Move to Position in List of Schemas

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

**To move to a specific position within the list**

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

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

Filter List Schemas

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

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

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

Display List of Schemas Details

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

To display the list of authority schema details

1) Access the Work with Authority Schemas interface.

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

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

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

Sort List of Schemas Details

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

To sort the list

1) Access the Work with Authority Schemas interface.

2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key on your keyboard.

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

**Move to Position in List of Schemas Details**

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

**To move to a specific position within the list**

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

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

**Filter List Schemas Details**

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

**To filter the list using a subset**

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

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

**See also**

*Working with Authority Schemas*
Manage Authority Schemas

Use this task to manage authority schemas.

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

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

Access the Work with Authority Schema Interface

To access the Work with Authority Schemas interface

1) Access the TGSecure Main menu.

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

3) Press Enter. The Resource Manager interface is displayed.

4) At the Selection or command prompt, enter 1 (Authority Schema Configuration).

5) Press Enter. The Work with Authority Schemas interface is displayed.

Add Authority Schema

Use this task to add an authority schema.

To add an authority schema

1) Access the Work with Authority Schemas interface.

2) Press the F6 (Create) function key on your keyboard.
3) Complete the following fields.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema ID</td>
<td>ID you want to assign to the schema</td>
</tr>
<tr>
<td>Schema Description</td>
<td>Text describing the purpose of the schema</td>
</tr>
</tbody>
</table>
| Alert Status   | Whether alerts are enabled:  
*YES - Enable alerts (create admin alerts)  
*NO - Disable alerts |
| Include IFS or Library Object | Which structures to check:  
*SYS - Enable check only in system libraries  
*IFS - Enable check only in Integrated File System (IFS).  
Note: IFS is a newer file management structure that supports stream input/output and is similar to the structure used by personal computers and UNIX operating systems. For more information about IBM file systems, refer to the IBM Knowledge Center.  
*ALL - Enable check-in (both SYS and IFS)  
*NO - Disable check-in |
| Filter Details | Whether data is filtered:  
*NONE - Data is not filtered  
Filter name - Enter the filter name or press F4 to select from a list. |
| IFS Depth      | Depth of IFS Folder to include:  
00-99 - Depth level  
Tip: Enter 00 to include only the IFS Scope directory level. |

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Object Name    | Enter a specific object name or object group to which this schema applies  
You can also choose one of the following options:  
*NONE - No objects  
*ALL - All objects  
Tip: You can skip this field for IFS files. |
5) Define the authorities by completing the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Library</td>
<td>Enter the name of the library to which this authority schema applies or enter *ALL to include all libraries</td>
</tr>
<tr>
<td><strong>Tip:</strong> You can skip this field for IFS files.</td>
<td></td>
</tr>
<tr>
<td>Object Type</td>
<td>Enter the object type to which this authority schema applies or enter *ALL to include all object types</td>
</tr>
<tr>
<td><strong>Tip:</strong> You can skip this field for IFS files.</td>
<td></td>
</tr>
<tr>
<td>Path or ASP Name</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>– Enter the file path for the IFS</td>
</tr>
<tr>
<td></td>
<td>– Enter the ASP (Auxiliary Storage Pool) for the system libraries</td>
</tr>
<tr>
<td><strong>Note:</strong> If you enter *SYSBAS, the system ASP and all basic user ASPs are included.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter the user's name</td>
</tr>
</tbody>
</table>

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

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

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

To edit an authority schema

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

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter twice.

Edit Authority Schema

Use this task to edit an existing authority schema.

To edit an authority schema

1) Access the Work with Authority Schemas interface.
2) In the OPT column for the desired schema, enter 2 (Edit).
3) Press Enter.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

5) Press Enter twice.

Copy Authority Schema

Use this task to create a new authority schema by copying an existing authority schema.

To copy an authority schema

1) Access the Work with Authority Schemas interface.
2) In the OPT column for the desired schema, enter 3 (Copy).
3) Press Enter.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
5) Press Enter.

Delete Authority Schema

Use this task to delete an authority schema.

To delete an authority schema

1) Access the Work with Authority Schemas interface.
2) In the OPT column for the desired schema, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct schema.
5) Press Enter twice.

Enabling Authority Schema Alerting

Use this task to enable alerting.

To enable/disable authority schema alerting

1) Access the Work with Authority Schemas interface.
2) In the OPT column for the desired schema, enter 2 (Edit).
3) Press Enter.
4) In the Alert Status field, enter *YES to enable alerting.

Disable Authority Schema Alerting

Use this task to disable alerting.

To enable/disable authority schema alerting

1) Access the Work with Authority Schemas interface.
2) In the OPT column for the desired schema, enter 2 (Edit).
3) Press Enter.
4) In the Alert Status field, enter *NO to disable alerting.

Limit Scope of Authority Schema to System Libraries (SYS)

Use this task to limit the scope of an authority schema to only address system libraries (SYS).

To limit the scope of the schema

1) Access the Work with Authority Schemas interface.
2) In the OPT column for the desired schema, enter 2 (Edit).
3) Press Enter.

4) In the Include IFS or Library Object field, enter *SYS.

**Limit Scope of Authority Schema to Integrated File System (IFS)**

Use this task to limit the scope of an authority schema to only address the Integrated File System (IFS).

**To limit the scope of the schema**

1) Access the Work with Authority Schemas interface.

2) In the OPT column for the desired schema, enter 2 (Edit).

3) Press Enter.

4) In the Include IFS or Library Object field, enter *IFS.

**Change Scope of Authority Schema (Object or IFS)**

Use this task to change the scope of an authority schema.

**To change the scope of the schema**

1) Access the Work with Authority Schemas interface.

2) In the OPT column for the desired schema, enter 12 (Edit).

3) Press Enter. The Change Scope (Object or IFS) interface is displayed.

4) Updated the following fields as necessary:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Type</td>
<td>Enter the appropriate file type:</td>
</tr>
<tr>
<td>*SYS - QSYS.Lib (tradition) file types</td>
<td></td>
</tr>
<tr>
<td>*IFS - IFS (Integrated File System) file types</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> For more information about IBM file systems, refer to the IBM Knowledge Center.</td>
<td></td>
</tr>
<tr>
<td>Object Name</td>
<td>Enter a specific object name or object group to which this schema applies</td>
</tr>
<tr>
<td>*NONE - No objects</td>
<td>You can also choose one of the following options:</td>
</tr>
<tr>
<td>*ALL - All objects</td>
<td>Tip: You can skip this field for IFS files.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Enter the object type to which this authority schema applies, or enter *ALL to include all object types</td>
</tr>
<tr>
<td>Tip: You can skip this field for IFS files.</td>
<td></td>
</tr>
<tr>
<td>Object Library</td>
<td>Enter the name of the library to which this authority schema applies, or enter *ALL to include all libraries</td>
</tr>
<tr>
<td>Tip: You can skip this field for IFS files.</td>
<td></td>
</tr>
</tbody>
</table>
Add Schema Details

Use this task to add an authority schema details. The details are the exceptions that are allowed.

To add an authority schema details

1) Access the **Work with Authority Schemas** interface.

2) In the **OPT** column for the desired schema, enter 10 (Work with Authority Schema Details).

3) Press **Enter**. The **Work with Authority Schema Details** interface is displayed.

4) Press the **F6** (Create) function key on your keyboard.

5) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema ID</td>
<td>ID assigned to the schema (not editable)</td>
</tr>
<tr>
<td>Schema Description</td>
<td>Text describing the purpose of the schema (not editable)</td>
</tr>
<tr>
<td>File Type</td>
<td>Enter the appropriate file type:</td>
</tr>
<tr>
<td></td>
<td><em>SYS</em> - QSYS.Lib (tradition) file types</td>
</tr>
<tr>
<td></td>
<td><em>IFS</em> - IFS (Integrated File System) file types</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: For more information about IBM file systems, refer to the IBM Knowledge Center.</td>
</tr>
<tr>
<td>Object Owner</td>
<td>Enter the name of the object owner</td>
</tr>
<tr>
<td>Authorization List</td>
<td>Enter the name of the authority list to which this authority schema applies, or enter *NONE if not applicable</td>
</tr>
<tr>
<td>Object Primary Group</td>
<td>Enter the name of the object primary group to which this authority schema applies or enter *NONE if not applicable</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the name of the user (or group) to which the exception applies or enter *PUBLIC to apply to all users.</td>
</tr>
<tr>
<td>Object Authority</td>
<td>Enter the authority level:</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Grant public users all authorities (i.e., change, exclude, use, etc.)</td>
</tr>
<tr>
<td></td>
<td><em>CHANGE</em> - Grant public users change authority</td>
</tr>
<tr>
<td></td>
<td><em>EXCLUDE</em> - Prohibit public users from performing operations on the object</td>
</tr>
<tr>
<td></td>
<td><em>USE</em> - Grant access to the object attributes and allow public users to use of the object (changes to object not allowed)</td>
</tr>
<tr>
<td></td>
<td><em>AUTL</em> - Grant public users the public authority specified in the authority list</td>
</tr>
</tbody>
</table>
6) Press Enter twice.

**Edit Schema Details**

Use this task to edit schema details.

**To edit schema details**

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press Enter. The **Work with Authority Schema Details** interface is displayed.
4) In the **OPT** column for the desired schema, enter **2** (Edit).
5) Press Enter.
6) Modify the parameters as necessary.

7) Press Enter twice.

**Copy Schema Detail**

Use this task to create a new schema detail by copying an existing schema detail.

**To copy schema details**

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press Enter. The **Work with Authority Schema Details** interface is displayed.
4) In the **OPT** column for the desired schema, enter **3** (Copy).
5) Press Enter.
6) Modify the parameters as necessary.

7) Press Enter.

**Delete Schema Detail**
To delete a schema detail

1) Access the Work with Authority Schemas interface.

2) In the OPT column for the desired schema, enter 10 (Work with Authority Schema Details).

3) Press Enter. The Work with Authority Schema Details interface is displayed.

4) In the OPT column for the desired schema, enter 4 (Delete).

5) Press Enter.

6) Review the record to ensure you are deleting the correct schema.

7) Press Enter twice.

Display Authority Schema Compliance Issues

Use this task to display authority schema compliance issues.

Tip: Run this task before you attempt to enforce authority schema to determine if exceptions (details) are required (see Add Schema Details).

To display authority schema compliance issues

1) Access the Main menu.

2) At the Selection or command prompt, enter 4 (Resource Manager).

3) Press Enter.

4) At the Selection or command prompt, enter 10 (Enforcement based on Authority Schema).

5) Press Enter.

6) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme ID</td>
<td>ID assigned to the scheme you want to analyze for compliance</td>
</tr>
<tr>
<td>Audit report</td>
<td>Enter *YES to enable auditing (tracking)</td>
</tr>
<tr>
<td>Report output type</td>
<td>Enter the desired report output format (*HTML, *PRINT, etc.)</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Enter *NO to display only (not enforce) compliance issues</td>
</tr>
<tr>
<td></td>
<td>Tip: Always display and investigate before enforcing.</td>
</tr>
<tr>
<td>Run interactively</td>
<td>Whether to run interactively or add to batch:</td>
</tr>
<tr>
<td></td>
<td>*YES - Run the report immediately</td>
</tr>
<tr>
<td></td>
<td>*NO - Add the report to a batch job to be run when most efficient for the system</td>
</tr>
</tbody>
</table>
7) Press Enter.

**Enforce Authority Schema**

Use this task to enforce an authority schema.

- **Tip:** Before enforcing an authority schema, first identify where non-compliance is occurring (see Display Authority Schema Compliance Issues). In some cases, an issue of non-compliance might identify an exception (authority detail) that must be added. In other words, you might need to update the scheme.

**To enforce authority schemas**

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter 4 (Resource Manager).

3) Press Enter.

4) At the **Selection or command** prompt, enter 10 (Enforcement based on Authority Schema).

5) Press Enter.

6) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme ID</td>
<td>ID assigned to the scheme you want to analyze for compliance</td>
</tr>
<tr>
<td>Audit report</td>
<td>Enter *YES to enable auditing (tracking)</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Enter *YES to enforce the schema</td>
</tr>
</tbody>
</table>
| Run interactively | Whether to run interactively or add to batch:  
*YES - Run the report immediately
*NO - Add the report to a batch job to be run when most efficient for the system |

- **Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press Enter.

**See also**

Working with Authority Schemas
Run Authority Schema Reports

Use this task to generate the following authority schema reports:

- Access the Resource Manager Reports Interface
- Run Resource Manager Schema Details Report
- Run Resource Manager Schema Details Changes Report
- Run Resource Manager Schema Header Changes Report
- Run Authority Schema Compliance Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Resource Manager reports, access from the Resource Manager Reports interface.

Access the Resource Manager Reports Interface

To access the Inactive Sessions Reports interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 4 (Resource Manager).

3) Press Enter.

4) At the Selection or command prompt, enter 20 (Resource Manager Reports).

5) Press Enter. The Resource Manager Reports interface is displayed.

Run Resource Manager Schema Details Report

Use this report to view the list of details (exceptions) associated with each authority schema.

To run the Resource Manager Schema Details Report

1) Access the Resource Manager Reports interface.

2) At the Selection or command prompt, enter 2 (Resource Manager Configuration Reports).

3) Press Enter. The Resource Manager Configuration Reports interface is displayed.

4) At the Selection or command prompt, enter 2 (Resource Manager Schema Details).

5) Press Enter.

6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run Resource Manager Schema Details Changes Report

Use this report to view the list of changes made to the details (exceptions) associated with each authority schema.

**Tip:** You must enable auditing to produce change reports. See [Manage Resource Manager Defaults](#) for additional information.

### To run the Resource Manager Schema Details Changes Report

1) Access the **Resource Manager Reports** interface.

2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).

3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see [Run TGSecure Reports](#).

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run Resource Manager Schema Header Report

Use this report to display the list of schema headers.

### To run the Resource Manager Schema Header Report

1) Access the **Resource Manager Reports** interface.

2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).

3) Press **Enter**. The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header).
5) Press Enter.

6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the Report output type field.

8) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Resource Manager Schema Header Changes Report**

Use this report to display the list of changes to schema headers.

**To run the Resource Manager Schema Header Changes Report**

1) Access the Resource Manager Reports interface.

2) At the Selection or command prompt, enter 3 (Resource Manager Change Reports).

3) Press Enter. The Resource Manager Configuration Reports interface is displayed.

4) At the Selection or command prompt, enter 3 (Resource Manager Schema Header Changes).

5) Press Enter.

6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the Report output type field.

8) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Authority Schema Compliance Report**

Use this task to display authority schema compliance issues.

**Tip:** Run this task before you attempt to enforce an authority schema to determine if exceptions (details) are required (see Add Schema Details).

**To run the authority schema compliance report**
1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Resource Manager).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).

5) Press **Enter**.

6) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme ID</td>
<td>ID assigned to the scheme you want to analyze for compliance</td>
</tr>
<tr>
<td>Audit report</td>
<td>Enter <em>YES</em> to enable auditing (tracking)</td>
</tr>
<tr>
<td>Report output type</td>
<td>Enter the desired report output format (*HTML, *PRINT, etc.)</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Enter <em>NO</em> to display (not enforce) compliance issues. <strong>Tip</strong>: Always display and investigate before enforcing.</td>
</tr>
</tbody>
</table>

7) Press **Enter**.

**See also**

*Working with Authority Schemas*
Authority Collections

This section describes working with the authority collections to compare IBM's least-privileges model with your current authority state in order to help define an authority schema that best meets the security needs of your organization.

Tip: It's good practice is to compare IBM's least privilege model with your current authority state to determine if a user has been granted more authority than necessary. This helps you to eliminate unnecessary over-authorization.

This section includes the following topics:

- Working with Authority Collections
- Display Authority Collection Configuration
- Manage Authority Collection Configuration
- Run Authority Collection Reports

See also

Resource Manager
Working with Authority Collections

Use the **Authority Collection** feature to do the following:

- Display Authority Collection Configuration
- Manage Authority Collection Configuration
- Run Authority Collection Reports

**Note:** To work with authority collections, you must access the **Work with Authority Collection Configuration Users** interface.

To access the **Work with Authority Collection Configuration Users** interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Resource Manager).

3) Press **Enter**. The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).

5) Press **Enter**. The **Work with Authority Collection Configuration Users** interface is displayed.

**See also**

Authority Collections
Display Authority Collection Configuration

Use this task to display the authority collection configuration details.

- Display List of Authority Collections
- Display Authority Collection Details

Display List of Authority Collections

Use this task to display the list of authority collections.

⚠️ Important: Authority collection is only available with OS IBM i 7.3 or higher.

To display the list of authority collections

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 4 (Resource Manager).
3) Press Enter. The Resource Manager interface is displayed.
4) At the Selection or command prompt, enter 2 (Authority Collection Configuration).
5) Press Enter. The Work with Authority Collection Configuration Users interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Name of the user</td>
</tr>
<tr>
<td>Collection Active</td>
<td>Whether user authority data is collected:</td>
</tr>
<tr>
<td></td>
<td>YES - Collection enabled (started)</td>
</tr>
<tr>
<td></td>
<td>NO - Collection disabled (ended)</td>
</tr>
<tr>
<td>Repository Exists</td>
<td>Whether a repository exists for the storage of authority data:</td>
</tr>
<tr>
<td></td>
<td>YES - Repository exists</td>
</tr>
<tr>
<td></td>
<td>NO - Repository does not exist</td>
</tr>
</tbody>
</table>

Display Authority Collection Details

To display the authority collection configuration details

1) Access the Main menu.
2) At the Selection or command prompt, enter 4 (Resource Manager).
3) Press Enter.
4) At the Selection or command prompt, enter 1 (Authority Collection Configuration).
5) Press Enter. The Work with Authority Collection Configuration interface is displayed.
6) In the OPT column for the desired authority collection, enter 5 (Display Collection Details).
Press Enter. The **Display Collection Details** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User profile</td>
<td>Name of the user for which authority data is being collected</td>
</tr>
<tr>
<td>Library</td>
<td>Name of the library monitored, or one of the following:</td>
</tr>
<tr>
<td></td>
<td><em>NONE</em> - Exclude libraries</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all libraries</td>
</tr>
<tr>
<td>ASP Device</td>
<td>Name of the ASP device or <em>SYBAS</em></td>
</tr>
<tr>
<td>Object</td>
<td>Name of the object or one of the following:</td>
</tr>
<tr>
<td></td>
<td>generic* - First few letters of an object name followed by an asterisk (wildcard) This indicates that all object that begins with the letters identified are to be included.</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all objects</td>
</tr>
<tr>
<td>Object type</td>
<td>Name of the object type or one of the following:</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all object types</td>
</tr>
<tr>
<td>Include DLO</td>
<td>Identifies the document libraries to include:</td>
</tr>
<tr>
<td></td>
<td><em>NONE</em> - Exclude document library objects</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all document library objects (*DOC and *FLR)</td>
</tr>
<tr>
<td></td>
<td><em>DOC</em> - include only documents</td>
</tr>
<tr>
<td></td>
<td><em>FLR</em> - Include only folders</td>
</tr>
<tr>
<td>Include file system objects</td>
<td>Identifies the file system objects to include:</td>
</tr>
<tr>
<td></td>
<td><em>NONE</em> - Exclude file system objects</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all file system objects</td>
</tr>
<tr>
<td></td>
<td><em>BLKSF</em> - Include only block files</td>
</tr>
<tr>
<td></td>
<td><em>CHRSF</em> - Include only character files</td>
</tr>
<tr>
<td></td>
<td><em>DIR</em> - Include only directories</td>
</tr>
<tr>
<td></td>
<td><em>FIFO</em> - Include only first-in-first-out special files</td>
</tr>
<tr>
<td></td>
<td><em>SOCKET</em> - Include only socket files</td>
</tr>
<tr>
<td></td>
<td><em>STMF</em> - Include only steam files</td>
</tr>
<tr>
<td></td>
<td><em>SYMLNK</em> - Include only symbolic links</td>
</tr>
<tr>
<td>Delete collection</td>
<td>Whether to store or dispose of the collection</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Dispose</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Store</td>
</tr>
<tr>
<td>Detail</td>
<td>What level of detail should be collected</td>
</tr>
<tr>
<td></td>
<td><em>OBJINF</em> - Collect authority details for each unique instance of the object-level information <em>OBJJOB</em> - Collect authority details for each unique instance of the object-level information and each unique instance of the job</td>
</tr>
</tbody>
</table>

**See also**

*Working with Authority Collection*
Manage Authority Collection Configuration

Use this task to manage the authority collection configuration details.

- Access the Authority Collection Users Interface
- Start Authority Collection
- End Authority Collection
- Delete Authority Collection

**Note**: To manage authority collections, access the **Work with Authority Collection Users** interface.

### Access the Authority Collection Users Interface

**To access the Work with Authority Collection Users interface**

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter 4 (Resource Manager).

3) Press **Enter**. The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter 2 (Authority Collection Configuration).

5) Press **Enter**. The **Work with Authority Collection Users** interface is displayed.

### Start Authority Collection

Use this task to add an authority collection.

**To add an authority collection**

1) Access the **Work with Authority Collections Users** interface.

2) Press the **F6** (Start Collection) function key on your keyboard.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User profile</td>
<td>Name of the user for which you want to begin collecting authority data</td>
</tr>
<tr>
<td>Library</td>
<td>Name of the library you want to monitor or enter one of the following:</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all libraries</td>
</tr>
<tr>
<td></td>
<td><em>NONE</em> - Exclude all libraries</td>
</tr>
<tr>
<td>ASP Device</td>
<td>Name of the ASP device or *SYSBAS</td>
</tr>
<tr>
<td>Object</td>
<td>Name of the object or one of the following:</td>
</tr>
<tr>
<td></td>
<td>generic* - First few letters of an object name followed by an asterisk</td>
</tr>
<tr>
<td></td>
<td>(wildcard). This indicates that all objects that begin with the letters</td>
</tr>
<tr>
<td></td>
<td>identified are to be included.</td>
</tr>
<tr>
<td></td>
<td><em>ALL</em> - Include all objects</td>
</tr>
</tbody>
</table>
### Trinity Guard

#### End Authority Collection

Use this task to end an authority collection.

**To edit an authority collection**

1. Access the **Work with Authority Collections Users** interface.
2. In the **OPT** column for the desired schema, enter **3** (End Collection).
3. Press **Enter**.
4. Review the record to ensure you are ending the correct collection.

**Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5. Press **Enter** twice.

#### Delete Authority Collection
Use this task to delete an authority collection.

To delete an authority collection

1) Access the Work with Authority Collections Users interface.

2) In the OPT column for the desired schema, enter 4 (Delete).

3) Press Enter.

4) Review the record to ensure you are deleting the correct collection.

5) Press Enter twice.

See also

Working with Authority Collection
Run Authority Collection Reports

Use this task to generate the following authority configuration reports:

- Access the Resource Manager Reports Interface
- Run Authority Compliance Report (Single Schema)
- Run Authority Compliance Report (All Schemas)
- Run Authority Collection Report (QSYS)
- Run Authority Collection Report (IFS)

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with authority collection reports, access from the Resource Manager Reports interface.

Access the Resource Manager Reports Interface

To access the Resource Manager Reports interface
1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 4 (Resource Manager).
3) Press Enter. The Resource Manager interface is displayed.
4) At the Selection or command prompt, enter 20 (Resource Manager Reports).
5) Press Enter. The Resource Manager Reports interface is displayed.

Run Authority Compliance Report (Single Schema)

Use this report to identify compliance issues with your authority schema(s). You can use this report to identify two states:

- Instances in which your authority scheme is being enforced (i.e., in compliance with your schema)
- Instances in which your authority scheme is not being enforced (i.e., out of compliance with your schema)

To run the Authority Compliance report for all schemas
1) Access the Main menu.
2) At the Selection or command prompt, enter 4 (Resource Manager).
3) Press Enter. The Resource Manager interface is displayed.
4) At the Selection or command prompt, enter 1 (Authority Schema Configuration).
5) Press Enter. The Work with Authority Schemas interface is displayed.
6) In the OPT column for the desired schema, enter 22 (Run Compliance Report).
7) Press Enter.
8) In the **Audit report** field, enter ‘YES’.

9) Enter the desired output format in the **Report output type** field.

10) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Authority Compliance Report (All Schemas)**

---

**Note:** Running authority compliance for all reports might take a lot time and system resources.

Use this report to identify compliance issues with your authority schema(s). You can use this report to identify two states:

- Instances in which your authority scheme is being enforced (i.e., in compliance with your schema)
- Instances in which your authority scheme is not being enforced (i.e., out of compliance with your schema)

**To run the Authority Compliance report for all schemas**

1) Access the **Resource Manager Reports** interface.

2) At the **Selection or command** prompt, enter 1 (Resource Manager Usage Reports).

3) Press **Enter**. The **Resource Manager Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 1 (Authority Compliance Report).

5) Press **Enter**.

6) Modify the run criteria as necessary.

---

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Authority Collection Report (QSYS)**

Use this task to generate the authority collection report for QSYS.

---

**Note:** QSYS is the traditional file management structure used to control the storing and accessing of traditional file objects (*FILE objects in the QSYS.LIB library). For more information about IBM file systems, refer to the IBM Knowledge Center.

**To run the Authority Collection report (QSYS)**

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter 1 (Resource Manager Usage Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 3 (Authority Collection Report - QSYS).

5) Press **Enter**.

6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

---

**Run Authority Collection Report (IFS)**

Use this task to generate the authority collection report for the Integrated File System (IFS).

**Note:** IFS a newer file management structure that supports stream input/output and is similar to the structure used by personal computers and UNIX operating systems. For more information about IBM file systems, refer to the IBM Knowledge Center.

---

**To run the Authority Collection report (IFS)**

1) Access the **Resource Manager Reports** interface.

2) At the **Selection or command** prompt, enter 1 (Resource Manager Usage Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 2 (Authority Collection Report - IFS).

5) Press **Enter**.

6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.
See also

Working with Authority Collection
User Profile Management

Use the User Profile Management feature to manage user profiles using blueprints. Think of a blueprint as a template that defines user profile best practices. Once you create a blueprint, you can use it to evaluate, create, or modify user profiles.

To access the User Profile Manager interface

1) Access the Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Manager).
3) Press Enter.

Use the User Profile Management interface to do the following:

- Work with profile manager defaults
- Work with blueprints
- Work with user exclusions
- Work with archived profiles
- Work with inactive profiles
- Work with user profiles
- Work with password rules

See also

Getting Started
Profile Management Defaults

This section describes how to work with **User Profile Management Defaults**.

User Profile Manager defaults allow you to define the following:

- Whether to send profile change alerts
- Whether to track profile changes (required if you plan to run reports)
- Journal in which to store profile changes
- Library in which to store profile changes
- Queue in which to store profile alerts
- Queue library in which to store profile alerts

This section includes the following topics:

- Working with User Profile Management Defaults
- Display User Profile Management Defaults
- Manage User Profile Management Defaults
- Run User Profile Management Reports

**See also**

User Profile Management
Working with User Profile Management Defaults

Use the **Profile Manager Defaults** interface to do the following:

- Display User Profile Management Defaults
- Manage User Profile Management Defaults
- Run User Profile Management Reports

**Note:** To work with profile manager defaults, you must access the **Profile Management Defaults** interface.

**To access the User Profile Management Defaults interface**

1) Log into to TGSecure. The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).

3) Press **Enter**. The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (User Profile Management Defaults).

5) Press **Enter**. The **User Profile Manager Defaults** interface is displayed.

**See also**

User Profile Management
Display User Profile Management Defaults

Use this task to display the User Profile Management default settings.

To display the User Profile Manager defaults

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 7 (Profile Manager Defaults).

5) Press Enter. The User Profile Management Defaults interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Journal Library</td>
<td>Library in which to store profile manager usage data</td>
</tr>
<tr>
<td>Audit Journal Library</td>
<td>Note: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
</tr>
<tr>
<td>Audit Configuration Changes</td>
<td>Indicates whether to track profile 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>
<tr>
<td></td>
<td>Tip: Set this flag to Y if you plan to run usage reports.</td>
</tr>
<tr>
<td></td>
<td>Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL, this indicates that configuration changes are being tracked in all modules.</td>
</tr>
<tr>
<td>Alerting Status</td>
<td>Indicates whether alerts are enabled:</td>
</tr>
<tr>
<td></td>
<td>*YES - Enable alerts (create admin alert)</td>
</tr>
<tr>
<td></td>
<td>*NO - Disable alerts</td>
</tr>
<tr>
<td>Alert Message Queue</td>
<td>Queue in which to store alerts</td>
</tr>
<tr>
<td>Alert Message Queue Library</td>
<td>Library in which to store the queue</td>
</tr>
</tbody>
</table>
| Archive User Profile | Indicates whether to archive inactive profiles:  
*YES - Create an archive  
*NO - Do not create an archive |
|----------------------|---------------------------------------------------------------|
| **Tip:** For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met:  
a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.)  
b. The user profile is associated with a blueprint  
c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion |

<table>
<thead>
<tr>
<th>Archive Profiles Retention (Days)</th>
<th>Number of days an archived profile is retained by the system</th>
</tr>
</thead>
</table>

| Exit Programs Installed | Indicates whether the exit programs necessary for profile management (including archiving) are installed:  
*YES - The exit programs that support user profile management are installed  
*NO - The exit programs that support user profile management are uninstalled |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> See Manage Profile Manager Defaults for instruction on adding exit programs.</td>
<td></td>
</tr>
</tbody>
</table>

**See also**

*Working with User Profile Management Defaults*
Manage User Profile Management Defaults

Use this task to manage the User Profile Management default settings.

- Accessing the User Profile Management Defaults Interface
- Edit User Profile Manager Settings
- Enable Profile Auditing
- Enable Profile Alerts
- Enable Profile Archiving
- Add Profile Exit Programs
- Remove Profile Exit Programs

Note: To manage Profile Manager defaults, access the User Profile Management Defaults interface.

Accessing the User Profile Management Defaults Interface

To access the User Profile Management Defaults interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 7 (User Profile Management Defaults).

5) Press Enter. The User Profile Management Defaults interface is displayed.

Edit User Profile Manager Settings

Use this task to edit profile auditing settings

To edit profile manager settings

1) Access the User Profile Management Defaults interface.

2) Modify the following fields as necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Journal</td>
<td>Journal in which to store profile manager usage data</td>
</tr>
<tr>
<td>Note: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
<td></td>
</tr>
<tr>
<td>Audit Journal Library</td>
<td>Library in which the journal resides</td>
</tr>
</tbody>
</table>
| Audit Configuration Changes | Indicates whether to track profile changes:  
|                           | **Y** - Enable tracking of changes  
|                           | **N** - Disable tracking of changes  
|                           | **Tip:** Set this flag to **Y** if you plan to run usage reports.  
|                           | **Note:** There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see **NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see **PARTIAL**, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see **ALL**, this indicates that configuration changes are being tracked in all modules.  
| Alerting Status | Indicates whether alerts are enabled:  
|                | **YES** - Enable alerts (create admin alert)  
|                | **NO** - Disable alerts  
| Alert Message Queue | Queue in which to store alerts  
| Alert Message Queue Library | Library in which to store the queue  
| Archive User Profile | Indicates whether to archive inactive profiles:  
|                       | **YES** - Create an archive  
|                       | **NO** - Do not create an archive  
|                       | **Tip:** For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met:  
|                       | a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.)  
|                       | b. The user profile is associated with a blueprint  
|                       | c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion  
| Archive Profiles Retention (Days) | Number of days an archived profile is retained by the system  
| Archive Method | Indicates the method used to archive inactive profiles:  
|               | **SAVSEC** - Save user profile data using SAVSECDTA command  
|               | **SAVPRF** - Save user profile data to a database file  
|               | **Tip:** Using **SAVSEC** option is slower, restore from archive option will run **RSTUSRPRF** command, whereas using **SAVPRF** is faster, restore option will run **CRTUSRPRF** command.  

Enable Profile Auditing

Use this task to enable profile change auditing.

Tip: Auditing is required if you plan to run profile change reports.

To enable profile auditing

1) Access the User Profile Management Defaults interface.

2) In the Audit Journal field, enter the name of the journal in which to store changes.

3) In the Audit Journal Library field, enter the name of the library in which the journal resides.

4) In the Audit Configuration Change field, enter Y.

5) Press Enter.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL, this indicates that configuration changes are being tracked in all modules.

Enable Profile Alerts

Use this task to enable profile change alerts.

Tip: Alerting is required if you plan to send alert notifications.

To enable profile alerts

1) Access the User Profile Management Defaults interface.

2) In the Alerting Status field, enter *YES.

3) In the Alert Message Queue field, enter the name of the queue in which to store the alerts.

4) In the Alert Message Queue Library field, enter the name of the library in which the queue resides.

5) Press Enter.
Enable Profile Archiving
Use this task to enable archiving of inactive user profiles.

Tip: The exit programs are required (must be installed) if you plan to use the Program Manager feature.

To enable profile archiving
1) Access the User Profile Management Defaults interface.
2) In the Archive User Profile field, enter *YES.
3) In the Archive Profiles Retention field, enter the number of days the archived should be retained.
4) Press Enter.

Add Profile Exit Programs
Use this task to add (install) the User Profile Management exit program.

Tip: This exit program is required to enable Program Manager features.

To add Profile Manager exit programs
1) Access the User Profile Management Defaults interface.
2) Press the F20 (Add Exit Program) function key on your keyboard.

Remove Profile Exit Programs
Use this task to remove (uninstall) the User Profile Management exit program.

Tip: The exit program is required to enable Program Manager features.

To remove profile exit programs
1) Access the User Profile Management Defaults interface.
2) Press the F21 (Remove Exit Program) function key on your keyboard.

See also
- Working with User Profile Management Defaults
- Display User Profile Management Defaults
Run User Profile Management Reports

Use this task to generate the following User Profile Manager reports:

- Access the User Profile Reports Interface
- Run User Profile Management Defaults Report
- Run User Profile Management Defaults Changes Report

Tip: You can schedule the Profile Manager Default reports (like all other reports) to run when most convenient.

Note: To work with Profile Manager Default reports, access from the User Profile Reports interface.

Access the User Profile Reports Interface

To access the User Profile Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (User Profile Reports).
5) Press Enter. The User Profile Reports interface is displayed.

Run User Profile Management Defaults Report

To run the User Profile Manager Default Report

1) Access the User Profile Reports interface.
2) At the Selection or command prompt, enter 2 (User Profile Configuration Reports).
3) Press Enter. The User Profile Configuration Reports interface is displayed.
4) At the Selection or command prompt, enter 11 (Profile Manager Defaults).
5) Press Enter.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.
Run User Profile Management Defaults Changes Report

Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

To run the Profile Manager Default Changes Report

1) Access the User Profile Reports interface.

2) At the Selection or command prompt, enter 3 (User Profile Change Reports).

3) Press Enter. The User Profile Change Reports interface is displayed.

4) At the Selection or command prompt, enter 11 (Profile Manager Defaults Changes).

5) Press Enter.

6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

See also

Working with User Profile Management Defaults
Blueprints

This section describes how to work with **Blueprints**. Blueprints allow you to design a 'template' by which to create new user profiles. In addition, you can use a blueprint to perform a mass update to all profiles assigned to a specific user group. To determine if the profiles within a user group conform to a blueprint, run the blueprint compliance report. The report identifies any discrepancies. You can then enforce a blueprint to eliminate the discrepancies (modify the user profiles within a group to 'match' the blueprint).

The following is the process used to define and implement blueprints:

This section includes the following topics:

- Working with Blueprints
- Display Blueprints
- Manage Blueprints
- Run Blueprint Reports

See also

User Profile Management
Working with Blueprints

Use the Blueprint feature to do the following:

- Display Blueprints
- Manage Blueprints
- Run Blueprint Reports

Note: To work with blueprints, you must access the Work with Blueprints interface.

To access the Work with Blueprint interface

1) Log into TGSecure. The Main menu appears.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 1 (Work with Blueprints).

5) Press Enter. The Work with Blueprints interface is displayed.

See also

Blueprints
Display Blueprints

Use this task to display blueprints.

- Display List of Blueprints
- Sort List of Blueprint
- Move to Position in List of Blueprints
- Filter List Blueprint

Display List of Blueprints

Use this task to display the list of available blueprints.

To display the list of blueprints

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 1 (Work with Blueprints).

5) Press Enter. The Work with Blueprints interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint ID</td>
<td>ID assigned to the blueprint</td>
</tr>
<tr>
<td>User Group</td>
<td>Name of user group to which the blueprint applies</td>
</tr>
<tr>
<td>Prf Parm</td>
<td>Whether parameters are defined:</td>
</tr>
<tr>
<td></td>
<td>*YES - One or more profile parameters are defined for the blueprint</td>
</tr>
<tr>
<td></td>
<td>*NO - No profile parameters are defined</td>
</tr>
<tr>
<td>Prf Auth</td>
<td>Whether object authorities are defined:</td>
</tr>
<tr>
<td></td>
<td>*YES - One or more object authorities are defined for the blueprint</td>
</tr>
<tr>
<td></td>
<td>*NO - No object authorities are defined</td>
</tr>
<tr>
<td>Auth List</td>
<td>Whether authority lists are defined:</td>
</tr>
<tr>
<td></td>
<td>*YES - One or more authority lists are defined for the blueprint</td>
</tr>
<tr>
<td></td>
<td>*NO - No object authorities are defined</td>
</tr>
<tr>
<td>3rd Party</td>
<td>Whether 3rd party scripts are defined:</td>
</tr>
<tr>
<td></td>
<td>*YES - One or more 3rd party scripts are defined for the blueprint</td>
</tr>
<tr>
<td></td>
<td>*NO - No 3rd party scripts are defined</td>
</tr>
<tr>
<td>Alt Sts</td>
<td>Whether alerts are enabled:</td>
</tr>
<tr>
<td></td>
<td>*YES - Alerts enabled (create admin alerts)</td>
</tr>
<tr>
<td></td>
<td>*NO - Alerts disabled</td>
</tr>
<tr>
<td>Compliance Date</td>
<td>Date on which blueprint compliance and profile inactivity check was last performed</td>
</tr>
<tr>
<td>Compliance Time</td>
<td>Time at which blueprint compliance and profile inactivity check was last performed</td>
</tr>
</tbody>
</table>
### Sort List of Blueprint

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

**To sort the list**

1) Access the **Work with Blueprint** interface.

2) Place your cursor on the desired column heading.

3) Press the F10 (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

### Move to Position in List of Blueprints

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

**To move to a specific position within the list**

1) Access the **Work with Blueprint** interface.

2) Sort the list based on the desired column heading.

3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

### Filter List Blueprint

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

| Inact Ovr          | Whether inactivity overrides are enabled:  
|--------------------|-----------------------------------------------|
|                    | *YES* - Overrides are enabled  
|                    | *NO* - Overrides disabled                    |
| Inact Prf?         | Whether inactive profiles exist (according to last report run):  
|                    | *Y* - Inactive profile were found (consider running enforcement)  
|                    | *N* - Inactive profiles were not found        |
| Comp Status        | Whether the current authority levels comply with the blueprint  
|                    | **PASS** - User authorities comply with the current blueprint  
|                    | **FAIL** - User authorities do not comply with the current blueprint |
| Blueprint Description | Description of the blueprint                  |
To filter the list using a subset

1) Access the **Work with Blueprint** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

*Working with Blueprints*
Manage Blueprints

Use this task to generate the following blueprint reports:

- Access the Work with Blueprints Interface
- Add Blueprint
- Copy Blueprint
- Delete Blueprint
- Display Blueprint Details
- Display Inactivity Overrides
- Edit Blueprint Details
- Edit Blueprint Profile Parameters
- Edit Blueprint Profile Authorities
- Edit Blueprint Authority Lists
- Edit Blueprint 3rd Party Scripts
- Edit Blueprint Permissions
- Add Blueprint User
- Edit Blueprint User
- Delete Blueprint User
- Display Blueprint Compliance Issues
- Display List of Non-Compliant Profiles
- Enforce Blueprint

Note: To manage blueprints, access the Work with Blueprints interface.

Access the Work with Blueprints Interface

To access the Work with Blueprints interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 1 (Work with Blueprints).

5) Press Enter. The Work with Blueprints interface is displayed.

Add Blueprint

Use this task to add a blueprint. There a number of details that need to be included in each blueprint, so a wizard has been designed to help you complete this multi-step process.

- Step 1: Add Blueprint Details
Step 1: Add Blueprint Details

To add blueprint details

1) Access the Work with Blueprints interface.

2) Press the F6 (Add Wizard) function key on your keyboard. The Blueprint - Add interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint ID</td>
<td>ID you want to assign to the blueprint</td>
</tr>
<tr>
<td>Blueprint Description</td>
<td>Text describing the purpose of the blueprint</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Indicates whether alerts are enabled:</td>
</tr>
<tr>
<td></td>
<td>*YES - Enable alerts (create admin alerts)</td>
</tr>
<tr>
<td></td>
<td>*NO - Disable alerts</td>
</tr>
<tr>
<td>User Scope</td>
<td>Enter the user group you want to associate with the blueprint.</td>
</tr>
<tr>
<td></td>
<td>Note: If you create a new profile based on this blueprint, the group you</td>
</tr>
<tr>
<td></td>
<td>enter in this field will be the user group to which you can add new</td>
</tr>
<tr>
<td></td>
<td>profiles. This is also the user group whose members are updated when a</td>
</tr>
<tr>
<td></td>
<td>blueprint is enforced. (See Manage User Profiles, for information about</td>
</tr>
<tr>
<td></td>
<td>adding a user profile based on an existing blueprint.)</td>
</tr>
<tr>
<td>Inactivity until User Profile is disabled</td>
<td>Number of days a profile must remain inactive profile before it is</td>
</tr>
<tr>
<td>(days)</td>
<td>disabled</td>
</tr>
<tr>
<td></td>
<td>Note: *DFT (Default) indicates that the standard number of days defined</td>
</tr>
<tr>
<td></td>
<td>by IBM should be applied</td>
</tr>
<tr>
<td>Inactivity until User Profile is deleted</td>
<td>Number of days a profile must remain inactive profile before it is</td>
</tr>
<tr>
<td>(days)</td>
<td>deleted</td>
</tr>
<tr>
<td></td>
<td>Note: *DFT (Default) indicates that the standard number of days defined</td>
</tr>
<tr>
<td></td>
<td>by IBM should be applied</td>
</tr>
<tr>
<td>Object owner for objects owned by deleted</td>
<td>Name of the user who should take over ownership of objects when/if a</td>
</tr>
<tr>
<td>profiles</td>
<td>profile is disabled or deleted</td>
</tr>
<tr>
<td></td>
<td>Note: *DFT (Default) indicates that the standard owner defined by IBM</td>
</tr>
<tr>
<td></td>
<td>should be applied</td>
</tr>
</tbody>
</table>

4) Press Enter. The User Profile Parameter Settings interface is displayed.

Tip: Press the F12 (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.
Step 2: Add Profile Parameters to a Blueprint

Tip: You can skip this step by pressing Enter.

To add profile parameters to your blueprint

1) Do one of the following:

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
</table>
| If you want to see all available parameters | Press the F6 (Add All) function key, go to Step 2  
  Note: This option adds all available profile parameters (and their associated default values). You can edit the default value if necessary.  
  Tip: *ANY is not a valid parameter value. If *ANY is the default value, you will be required to enter a specific value before you can save the blueprint.  |
| If you want to see only the system-suggested parameters | Press the F7 (Add Suggested) function key, skip to Step 4  
  Note: This option adds only the profile parameters suggested by the intelligence engine.  |
| If you want to add all default parameters | Press the F8 (Add All Default) function key, skip to Step 4  |

Note: The Parameter Selection dialog appears.

2) In the Sel column, enter 1 beside the parameter(s) you want to add.

Tip: To make no selections, press the F12 (Cancel) function key to return to the previous screen.

3) Press Enter to add the selected parameters and return to the User Profile Parameter Settings interface.

4) Press Enter. The User Profile Object Authority interface is displayed.

Tip: Press the F12 (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 3: Add Object Authorities to a Blueprint

Tip: You can skip this step by pressing Enter.

To add object authorities to your blueprint

1) In the *USRPRF Object area, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>

Trinity Guard
### Step 4: Add Authority List Settings to a Blueprint

2) In the **MSGQ Object** area, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object Owner</strong></td>
<td>Enter one the following:</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the user name you want to assign as the owner of message queue objects</td>
</tr>
<tr>
<td>*DFT</td>
<td>Assign message queue object ownership to the default (IBM) user</td>
</tr>
<tr>
<td>*USRPRF</td>
<td>Assign message queue object ownership to the user running the program</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If *DFT appears in this column, the two fields below should be left blank.</td>
</tr>
<tr>
<td><strong>Owner Authority</strong></td>
<td>Enter the authority level you want to assign the object owner:</td>
</tr>
<tr>
<td>*ALL</td>
<td>Grant owner all authorities (i.e., change, exclude, use, etc.)</td>
</tr>
<tr>
<td>*CHANGE</td>
<td>Grant owner change authority</td>
</tr>
<tr>
<td>*EXCLUDE</td>
<td>Prohibit owner from performing operations on the object</td>
</tr>
<tr>
<td>*USE</td>
<td>Grant access to the object attributes and allow the owner to use of the object (but not change the object)</td>
</tr>
<tr>
<td><strong>PUBLIC Authority</strong></td>
<td>Enter the authority level you want to assign to public users (*Public):</td>
</tr>
<tr>
<td>*ALL</td>
<td>Grant public users all authorities (i.e., change, exclude, use, etc.)</td>
</tr>
<tr>
<td>*AUTL</td>
<td>Grant public users the default level of authority specified by the authority list</td>
</tr>
<tr>
<td>*CHANGE</td>
<td>Grant public users change authority</td>
</tr>
<tr>
<td>*EXCLUDE</td>
<td>Prohibit public users from performing operations on the object</td>
</tr>
<tr>
<td>*USE</td>
<td>Grant access to the object attributes and allow public users to use of the object (but not change the object)</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter the user name you want to assign as the owner of user profile objects</td>
</tr>
<tr>
<td>*DFT</td>
<td>Assign user profile object ownership to the default (IBM) user</td>
</tr>
<tr>
<td>*USRPRF</td>
<td>Assign user profile object ownership to the user running the program</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If *DFT appears in this column, the two fields below should be left blank.</td>
</tr>
</tbody>
</table>

3) Press Enter. The **Authority List Settings** interface is displayed.

- **Tip:** Press the F12 (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

### Step 4: Add Authority List Settings to a Blueprint

- **Tip:** You can skip this step by pressing Enter.
To add authority list settings to your blueprint

1) Press the F6 (Add) function key on your keyboard. The Authority List Settings interface is displayed.

2) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority List</td>
<td>Enter the name of the authority list to which this blueprint applies. <strong>Note:</strong> An authority list displays the users who have the authority to access a specific object.</td>
</tr>
</tbody>
</table>
| Authority Value| Enter the authority level you want to assign users who are members of the authority list:  
*ALL* - Grant users all authorities (i.e., change, exclude, use, etc.)  
*CHANGE* - Grant users change authority  
*EXCLUDE* - Prohibit uses from performing operations on the object  
*USE* - Grant access to the object attributes and allow users to use the object (but not change the object) |

3) Press **Enter** to add the authority list and return to the User Authority List Settings interface.

4) Press **Enter**. The 3rd Party Integration interface is displayed.

**Tip:** Press the F12 (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 5: Add 3rd Party Scripts to a Blueprint

**Tip:** You can skip this step by pressing **Enter**.

To add 3rd party scripts to your blueprint

1) Press the F6 (Add) function key on your keyboard. The 3rd Party Integration interface is displayed.

2) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script Type</td>
<td>Type of the third-party script</td>
</tr>
<tr>
<td>Script Statement</td>
<td>3rd party script text</td>
</tr>
</tbody>
</table>

4) Press **Enter**.

**Tip:** Press the F12 (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 6: Add Permissions to a Blueprint
To add permissions to a blueprint

1) Press the **F6** (Add) function key on your keyboard. The **Blueprint Permissions** interface is displayed.

2) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Group</td>
<td>User or user group that has permission to use the blueprint to create and change user profiles. <strong>Tip:</strong> Press the F4 (List) function key to see a list of available options.</td>
</tr>
<tr>
<td>Create Permission</td>
<td>Whether the user/user group has permission to create new user profiles based on the blueprint. <strong>YES</strong> - Enable create, <strong>NO</strong> - Disable create.</td>
</tr>
<tr>
<td>Change Permission</td>
<td>Whether the user/user group has permission to change user profiles based on blueprint. <strong>YES</strong> - Enable change, <strong>NO</strong> - Disable change.</td>
</tr>
</tbody>
</table>

3) Press **Enter**.

**Tip:** You can skip this step by pressing **Enter**.

**Tip:** Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Copy Blueprint

Use this task to create a new blueprint by copying an existing blueprint.

To copy a blueprint

1) Access the **Work with Blueprint** interface.

2) In the **OPT** column for the desired blueprint, enter **3** (Copy).

3) Press **Enter**.

4) Modify the parameters as necessary.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

Delete Blueprint

Use this task to delete a blueprint.
To delete a blueprint

1) Access the **Work with Blueprint** interface.

2) In the **OPT** column for the desired blueprint, enter 4 (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct blueprint.

5) Press **Enter** twice.

**Display Blueprint Details**

Use this task to display blueprint details.

**To display blueprint details**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter 5 (Display).

3) Press **Enter**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint ID</td>
<td>ID assign to the blueprint</td>
</tr>
<tr>
<td>Blueprint Description</td>
<td>Text describing the purpose of the blueprint</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerts are enabled</td>
</tr>
<tr>
<td></td>
<td>*YES - Enable alerts (create admin alerts)</td>
</tr>
<tr>
<td></td>
<td>*NO - Disable alerts</td>
</tr>
<tr>
<td>User Scope</td>
<td>User group to which the blueprint applies</td>
</tr>
<tr>
<td>Inactivity until User Profile is disabled</td>
<td>Number of days a profile must remain inactive before it is disabled</td>
</tr>
<tr>
<td>(days)</td>
<td><strong>Note:</strong> <em>DFT (Default)</em> indicates that the standard number of days defined by IBM should be applied</td>
</tr>
<tr>
<td>Inactivity until User Profile is deleted</td>
<td>Number of days a profile must remain inactive before it is deleted</td>
</tr>
<tr>
<td>(days)</td>
<td><strong>Note:</strong> <em>DFT (Default)</em> indicates that the standard number of days defined by IBM should be applied</td>
</tr>
<tr>
<td>Object owner for objects owned by deleted</td>
<td>Name of the user who should take over ownership of objects when a profile is disabled or deleted</td>
</tr>
<tr>
<td>profiles</td>
<td><strong>Note:</strong> All objects must be assigned an owner.</td>
</tr>
</tbody>
</table>

**Display Inactivity Overrides**

Use this task to display inactivity overrides. When you create a blueprint, you have the option to use the default (*DFT) IBM policy to determine when an inactive user profile is disabled or deleted (and to whom object ownership should be transferred in such a case).

**To display inactive overrides**

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter 14 (Inactivity Overrides).

3) Press **Enter**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity until User Profile is disabled (days)</td>
<td>Number of days a profile must remain inactive profile before it is <strong>disabled</strong></td>
</tr>
<tr>
<td><strong>Note</strong>: <em>DFT (Default) indicates that the standard number of days defined by IBM should be applied</em></td>
<td></td>
</tr>
<tr>
<td>Inactivity until User Profile is deleted (days)</td>
<td>Number of days a profile must remain inactive profile before it is <strong>deleted</strong></td>
</tr>
<tr>
<td><strong>Note</strong>: <em>DFT (Default) indicates that the standard number of days defined by IBM should be applied</em></td>
<td></td>
</tr>
<tr>
<td>Object owner for objects owned by deleted profiles</td>
<td>Name of the user who should take over ownership of objects when a profile is disabled or deleted</td>
</tr>
</tbody>
</table>

**Edit Blueprint Details**

Use this task to edit the details of an existing blueprint.

**To edit blueprint details**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter 2 (Edit).

3) Press **Enter**.

4) Modify the parameters as necessary.

5) Press **Enter** twice.

**Edit Blueprint Profile Parameters**

Use this task to edit the profile parameters for an existing blueprint.

**To edit blueprint profile parameters**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter 10 (Profile Parameters).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete parameters.

5) Press **Enter** twice.

**Edit Blueprint Profile Authorities**

Use this task to edit the profile authorities for an existing blueprint.

**To edit blueprint profile authorities**
1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter **11** (Profile Authorities).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete profile authorities.

5) Press **Enter** twice.

**Edit Blueprint Authority Lists**

Use this task to edit the authority list for an existing blueprint.

**To edit blueprint authority list**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter **12** (Authority Lists).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete authority lists.

5) Press **Enter** twice.

**Edit Blueprint 3rd Party Scripts**

Use this task to edit 3rd party scripts associated with an existing blueprint.

**To edit blueprint 3rd party scripts**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter **13** (3rd Party).

3) Press **Enter**.

4) Modify the parameters as necessary. You also have the ability to add and delete 3rd party scripts.

5) Press **Enter** twice.

**Edit Blueprint Permissions**

Use this task to manage who can use a blueprint (as a template) to create and change user profiles.

**To edit blueprint permissions**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter **30** (Blueprint Permissions).

3) Press **Enter**.

4) Modify the following fields as necessary.
1) Access the interface.

To add blueprint user
Use this task to add a user (member) to a blueprint user group.

Add Blueprint User

5) Press Enter twice.

2) In the OPT column for the desired blueprint, enter 15 (Work with Users).

3) Press Enter. The Work with Users interface is displayed.

4) Press the F6 (Add) function key on your keyboard. The Work with Users - Add Record interface is displayed.

5) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of user</td>
</tr>
<tr>
<td>User Description</td>
<td>Description of user</td>
</tr>
</tbody>
</table>

6) Press Enter.

Note: If the system locates the user on the server, then a *YES appears in the Exists on Server field.

Edit Blueprint User

Use this task to edit the user details of a user (member) assigned to a blueprint group.

To edit a blueprint user

1) Access the Work with Blueprints interface.

2) In the OPT column for the desired blueprint, enter 15 (Work with Users).

3) Press Enter. The Work with Users interface is displayed.

4) In the OPT column for the desired user, enter 2 (Edit).
5) Press **Enter**.

6) Modify the parameters as necessary.

7) Press **Enter** twice.

### Delete Blueprint User

Use this task to delete a user (member) from a blueprint group.

**To delete a blueprint user**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).

3) Press **Enter**. The **Work with Users** interface is displayed.

4) In the **OPT** column for the desired user, enter **4** (Delete).

5) Press **Enter**.

6) Review the record to ensure you are deleting the correct blueprint.

7) Press **Enter** twice

### Display Blueprint Compliance Issues

Use this task to display blueprint compliance issues. This is another way of running the blueprint compliance report.

**To display blueprint compliance issues**

1) Access the **Work with Blueprints** interface.

2) In the **OPT** column for the desired blueprint, enter **22** (Run Compliance Report).

3) Press **Enter**.

4) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Name of blueprint</td>
</tr>
<tr>
<td>Audit report</td>
<td>Enter <strong>YES</strong> to enable auditing (tracking)</td>
</tr>
<tr>
<td>Report output type</td>
<td>Enter the desired report output format (<strong>HTML</strong>, <strong>PRINT</strong>, etc.)</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Enter <strong>NO</strong> to display only (not enforce them) compliance issues</td>
</tr>
</tbody>
</table>

**Tip:** Always display and investigate before enforcing.
1) Access the Work with Blueprints interface.

2) In the OPT column for the desired blueprint, enter 20 (Non-Compliant).

3) Press Enter.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of the user</td>
</tr>
<tr>
<td>Violation</td>
<td>How the user's profile is in violation of the blueprint: Category - Category of violation Keyword - Parameter that is in violation Description - Description of object in violation</td>
</tr>
<tr>
<td>Blueprint Value</td>
<td>Parameter value defined in the blueprint</td>
</tr>
<tr>
<td>Actual Value</td>
<td>Parameter value defined in the user profile</td>
</tr>
</tbody>
</table>

**Enforce Blueprint**

Use this task to enforce a blueprint.

**Tip:** Before enforcing a blueprint, first display the blueprint compliance issues to identify where non-compliance is occurring. In some cases, an issue of non-compliance might identify the need for an exclusion to be added. In other words, you might need to update the blueprint.

1) Access the Work with Blueprints interface.

2) In the OPT column for the desired blueprint, enter 24 (Run Enforcement).

3) Press Enter.

**To enforce authority blueprint**
4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Name of blueprint</td>
</tr>
<tr>
<td>Audit report</td>
<td>Enter *YES to enable auditing (tracking)</td>
</tr>
<tr>
<td>Report output type</td>
<td>Enter the desired report output format (*HTML, *PRINT, etc.)</td>
</tr>
</tbody>
</table>
| Enforcement        | Enter *YES to enforce the blueprint  
**Tip:** Always display and investigate before enforcing. |
| Run interactively  | Whether to run interactively or add to batch:  
*YES* - Run the report immediately  
*NO* - Add the report to a batch job to be run when most efficient for the system |

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

5) Press Enter.

See also

Working with Blueprints
Run Blueprint Reports

Use this task to generate the following blueprint reports:

- Access the User Profile Interface
- Run Blueprint Compliance Report (TGPRFCMP)
- Run Blueprint Master Report
- Run Blueprint Permission File Report
- Run Blueprint Parameter File Report
- Run Blueprint Object Authority File Report
- Run Blueprint Authority List Settings Report
- Run Blueprint Non-Compliance User Profiles Report
- Run Blueprint 3rd Party Integration File Report
- Run Blueprint Master Change Report
- Run Blueprint Permission File Change Report
- Run Blueprint Parameter File Change Report
- Run Blueprint Object Authority File Change Report
- Run Blueprint Authority List Settings Change Report
- Run Blueprint Non-Compliance User Profiles Change Report
- Run Blueprint 3rd Party Integration File Change Report

Tip: You can schedule the blueprint reports (like all other reports) to run when most convenient.

Note: To work with blueprint reports, access from the User Profile Reports interface.

Access the User Profile Interface

To access the User Profile Reports interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter.

4) At the Selection or command prompt, enter 20 (User Profile Reports).

5) Press Enter. The User Profile Reports interface is displayed.

Run Blueprint Compliance Report (TGPRFCMP)

Use this task to run the blueprint compliance issues report. This report lists the users whose profile authorities do not meet blueprint requirements.
To run the Blueprint Compliance Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).

3) Press **Enter**. The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Blueprint Compliance Report).

5) Press **Enter**.

6) Complete the following fields.

---

**Tip:** To see the complete list of available parameters, press the **F9** function key.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
<td>Enter <strong>“BLUEPRINT”</strong></td>
</tr>
<tr>
<td><strong>Audit report</strong></td>
<td>Enter <strong>“YES”</strong> to enable auditing (tracking)</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>User profile to include in the report</td>
</tr>
<tr>
<td><strong>Days for disable user profile</strong></td>
<td>Number of days a profile must remain inactive before it is <strong>disabled</strong></td>
</tr>
<tr>
<td><strong>Days for delete user profile</strong></td>
<td>Number of days a profile must remain inactive before it is <strong>deleted</strong></td>
</tr>
<tr>
<td><strong>Report output type</strong></td>
<td>Enter the desired report output format (<strong>“HTML</strong>,** “PRINT”, etc.)</td>
</tr>
<tr>
<td><strong>File to receive output</strong></td>
<td>Name of file to receive report output</td>
</tr>
<tr>
<td><strong>Library</strong></td>
<td>Library in which the file resides</td>
</tr>
<tr>
<td><strong>Replace or add records</strong></td>
<td>Whether to replace or append records to the file</td>
</tr>
<tr>
<td><strong>Enforcement</strong></td>
<td>Enter <strong>“NO”</strong> to display only (not enforce) compliance issues</td>
</tr>
<tr>
<td><strong>Run interactively</strong></td>
<td>Whether to run interactively or add to batch: <strong>YES</strong> - Run the report immediately, <strong>NO</strong> - Add the report to a batch job to run when most efficient for the system.</td>
</tr>
<tr>
<td><strong>Job queue</strong></td>
<td>If you want to include the report in a batch, enter job queue</td>
</tr>
</tbody>
</table>

---

**Tip:** Run this task before you attempt to enforce a blueprint to determine if exclusions are required (see **Manage User Exclusions**).
7) Press **Enter**.

**Run Blueprint Master Report**

Use this task to display the list of blueprints.

**To run the Blueprint Master Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).

3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Blueprint Master).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

**Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Permission File Report**

Use this task to display permissions associated with blueprints. Permissions determine who can use a blueprint to create or modify user profiles.

**To run the Blueprint Permission File Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).

3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Blueprint Permission File).

5) Press **Enter**.

6) Modify the report run criteria as necessary.
6) Modify the report run criteria as necessary.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Parameter File Report**

Use this task to display parameters associated with blueprints. For a user profile to be in compliance with a blueprint, the parameter values in the blueprint must match the parameter values in the associated user profile.

**To run the Blueprint Parameter File Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter 2 (User Profile Configuration Reports).

3) Press Enter. The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 3 (Blueprint Parameter File).

5) Press Enter.

6) Modify the report run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip**: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Object Authority File Report**

Use this task to display object authorities associated with blueprints.

**To run the Blueprint Object Authority File Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter 2 (User Profile Configuration Reports).

3) Press Enter. The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 4 (Blueprint Object Authority File).

5) Press Enter.

6) Modify the report run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip**: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
To run the Blueprint Non-Compliance User Profiles Report

1) Access the User Profile Reports interface.

2) At the Selection or command prompt, enter 2 (User Profile Configuration Reports).

3) Press Enter. The User Profile Configuration Reports interface is displayed.

4) At the Selection or command prompt, enter 6 (Blueprint Non-Compliance User Profiles).

5) Press Enter.
6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint 3rd Party Integration File Report**

Use this task to display 3rd party scripts associated with blueprints.

**To run the Blueprint 3rd Party Integration File Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).

3) Press **Enter**. The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Master Change Report**

Use this task to display changes made to the blueprint master.

**Tip:** You must enable auditing to produce change reports. See **Manage User Profile Management Defaults** for additional information.

**To run the Blueprint Master Change Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Blueprint Master Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

[Note] The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

[Tip] Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Permission File Change Report**

Use this task to display changes made to blueprint permissions. Permissions determine who can use a blueprint to create or modify user profiles.

**To run the Blueprint Permission File Change Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Blueprint Permission File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

[Note] The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

[Tip] Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Parameter File Change Report**

Use this task to display changes made to blueprint parameters.

**To run the Blueprint Parameter File Change Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.
4) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Object Authority File Change Report**

Use this task to display changes made to blueprint object authorities.

**To run the Blueprint Object Authority File Change Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Authority List Settings Change Report**

Use this task to display changes made to blueprint authority lists.

**To run the Blueprint Authority List Settings Change Report**

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter 3 (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 5 (Blueprint Authority List Settings Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint Non-Compliance User Profiles Change Report**

Use this task to display changes made to non-compliant user profiles.

**To run the Blueprint Non-Compliance User Profiles Change Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter 3 (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 6 (Blueprint Non-Compliance User Profiles Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Blueprint 3rd Party Integration File Change Report**

Use this task to display changes made to 3rd party scripts.

**To run the 3rd Party Integration File Change Report**

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

   **Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

   **Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

*Working with Blueprints*
User Exclusions

This section describes how to work with **User Exclusions**.

This section includes the following topics:

- Working with User Exclusions
- Display User Exclusions
- Manage User Exclusions
- Run User Exclusion Reports

See also

User Profile Management
Working with User Exclusions

Use the User Exclusion feature to do the following:

- Display User Exclusions
- Manage User Exclusions
- Run User Exclusion Reports

**Note:** To work with user exclusions, you must access the **Work with User Exclusions** interface.

**To access the Work with User Exclusions interface**

1) Log into to TGSecure. The **Main** menu appears.

2) At the **Selection or command** prompt, enter 5 (User Profile Management).

3) Press **Enter.** The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter 2 (Work with User Exclusions).

5) Press **Enter.** The **Work with User Exclusions** interface is displayed.

See also

[User Exclusions](#)
Display User Exclusions

Use this task to display user exclusions.

- Display List of User Exclusions
- Sort List of User Exclusions
- Move to Position in List of User Exclusions

Display List of User Exclusions

Use this task to display the list of available user exclusions.

To display the list of user exclusions

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter. The User Profile Management interface is displayed.
4) At the Selection or command prompt, enter 2 (Work with User Exclusions).
5) Press Enter. The Work with User Exclusions interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Group</td>
<td>Name of the user group to which exclusions apply</td>
</tr>
<tr>
<td>Exclusion Type</td>
<td>Type of exclusion</td>
</tr>
<tr>
<td></td>
<td>*ALL - All types</td>
</tr>
<tr>
<td></td>
<td>*ACTIVITY - Exclude the user group from inactivity check</td>
</tr>
<tr>
<td></td>
<td>*SYNC - Exclude the user group from synchronization with other iSeries systems</td>
</tr>
</tbody>
</table>

Sort List of User Exclusions

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the Work with User Exclusion interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List of User Exclusions

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.
To move to a specific position within the list

1) Access the Work with User Exclusion interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List User Exclusions

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the Work with User Exclusion interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter.

**Note:** The system filters the results based on the criteria you defined for the subset.

See also

Working with User Exclusions
Manage User Exclusions

Use this task to manage user exclusions.

- Access the Working with User Exclusions Interface
- Add Exclusion
- Edit Exclusion
- Copy Exclusion
- Delete Exclusion

**Note:** To manage user exclusions, access the Work with User Exclusions interface.

**Access the Working with User Exclusions Interface**

**To access the Work with User Exclusions interface**

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter 5 (User Profile Management).

3) Press **Enter**. The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter 2 (Work with User Exclusions).

5) Press **Enter**. The **Work with User Exclusions** interface is displayed

**Add Exclusion**

Use this task to create a new user exclusion.

**To copy an exclusion**

1) Access the **Work with User Exclusions** interface.

2) Press the **F6** (Add) function key on your keyboard.

3) Press **Enter**. The **Work with User Exclusion - Add** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Group</td>
<td>Name of the user group to which exclusions apply</td>
</tr>
<tr>
<td>Exclusion Type</td>
<td>Type of exclusion</td>
</tr>
<tr>
<td></td>
<td>*ALL - All types</td>
</tr>
<tr>
<td></td>
<td>*ACTIVITY - Exclude the user group from being checked for inactivity</td>
</tr>
<tr>
<td></td>
<td>*SYNC - Exclude the user group from being synchronized with other systems (e.g., TGCentral)</td>
</tr>
</tbody>
</table>

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.
5) Press Enter twice.

**Edit Exclusion**

Use this task to edit an existing user exclusion.

**To edit an exclusion**

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, enter 2 (Edit).
3) Press Enter.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

5) Press Enter twice.

**Copy Exclusion**

Use this task to create a new user exclusion by copying an existing user exclusion.

**To copy an exclusion**

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, enter 3 (Copy).
3) Press Enter.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

5) Press Enter twice.

**Delete Exclusion**

Use this task to delete an exclusion.

**To delete an exclusion**

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, enter 4 (Delete).
3) Press Enter.

4) Review the record to ensure you are deleting the correct exclusion.

5) Press Enter twice.

See also

Working with User Exclusions
Run User Exclusion Reports

Use this task to generate the following user exclusion reports:

- Access the User Profile Report Interface
- Run User Profile Exclusions Report
- Run User Profile Exclusions Changes Report

Tip: You can schedule the user exclusion reports (like all other reports) to run when most convenient.

Note: To work with user exclusion reports, access from the User Profile Reports interface.

Access the User Profile Report Interface

To access the User Profile Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (User Profile Reports).
5) Press Enter. The User Profile Reports interface is displayed.

Run User Profile Exclusions Report

Use this report to view the list of user profile exclusions.

To run the User Profile Exclusions Report

1) Access the User Profile Reports interface.
2) At the Selection or command prompt, enter 2 (User Profile Configuration Reports).
3) Press Enter. The User Profile Configuration Reports interface is displayed.
4) At the Selection or command prompt, enter 8 (User Profile Exclusions).
5) Press Enter.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.
7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run User Profile Exclusions Changes Report

Use this report to view the changes made to user profile exclusions.

- **Tip**: You must enable auditing to produce change reports. See [Manage User Profile Management Defaults](#) for additional information.

### To run the User Profile Exclusions Changes Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **8** (User Profile Exclusions Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

- **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see [Run TGSecure Reports](#).

- **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### See also

* [Working with User Exclusions](#)*
Archived Profiles

This section describes how to work with Archived Profiles.

This section includes the following topics:

- Working with Archived Profiles
- Display Archived Profiles
- Manage Archived Profiles
- Run Archived Profile Reports

See also

User Profile Management
Working with Archived Profiles

Use the Archived Profiles feature to do the following:

- Display Archived Profiles
- Manage Archived Profiles
- Run Archived Profile Reports

**Note:** To work with archived profiles, you must access the Work with Archived Profiles interface.

To access the Work with Archived Profiles interface

1) Log into TGSecure. The Main menu appears.

2) At the **Selection or command** prompt, enter 5 (User Profile Management).

3) Press **Enter**. The User Profile Management interface is displayed.

4) At the **Selection or command** prompt, enter 3 (Work with Archived Profiles).

5) Press **Enter**. The Work User Archived Profiles is displayed.

See also

Archived Profiles
Display Archived Profiles

Use this task to display archived profiles.

- Display List of Archived Profiles
- Clean up Profile Archive Data
- Sort List of Archived Profiles
- Move to Position in List of Archived Profiles
- Filter List Archived Profiles

Display List of Archived Profiles

Use this task to display the list of available archived profiles.

To display the list of archived profiles

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter. The User Profile Management interface is displayed.
4) At the Selection or command prompt, enter 3 (Work with Archived Profiles).
5) Press Enter. The Work with Archived Profiles is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of the user whose profile has met inactivity limits and should, therefore, be disabled or deleted</td>
</tr>
<tr>
<td>Archived Date</td>
<td>Date on which the user profile was archived</td>
</tr>
<tr>
<td>User Description</td>
<td>Description of the user</td>
</tr>
<tr>
<td>Arch Available</td>
<td>Where archive is available</td>
</tr>
<tr>
<td>Archived Library</td>
<td>Name of the archive library</td>
</tr>
<tr>
<td>Archived File</td>
<td>Name of the archive file</td>
</tr>
</tbody>
</table>

Clean up Profile Archive Data

Use this task to delete previously archived profile data.

To clean up profile data

1) Access the Profile Archive Cleanup interface.
2) Press the F16 (Profile Archive Cleanup) function key on your keyboard.
Sort List of Archived Profiles

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the Work with Archived Profiles interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key on your keyboard.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List of Archived Profiles

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Archived Profiles interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List Archived Profiles

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use a wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after the text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset
1) Access the **Work with Archived Profiles** interface.

2) Press the **F8** (Subset) function key on your keyboard.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**.

**Note:** The system filters the results based on the criteria you defined for the subset.

**See also**

*Working with Archived Profiles*
Manage Archived Profiles

Use this task to manage archived profiles.

- Access the Work with Archived Profiles Interface
- Reactivate Profile
- Delete Archived File

Note: To manage archived profiles, access the Work with Archived Profiles interface.

Access the Work with Archived Profiles Interface

To access the Work with Archived Profiles interface
1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter. The User Profile Management interface is displayed.
4) At the Selection or command prompt, enter 3 (Work with Archived Profiles).
5) Press Enter. The Work with Archived Profiles is displayed.

Reactivate Profile

Use this task to reactivate a profile.

Note: Profiles are archived (retired from the system and stored in an archive file) once they meet the inactivity requirements set in the Manage Inactive Profiles.

To reactivate a profile
1) Access the Work with Archived Profiles interface.
2) In the OPT column for the desired profile, enter 6 (Reactivate Profile).
3) Press Enter.

Delete Archived File

Warning: Before deleting an archive file, ensure you have a back-up of the file.

Use this task to delete an archive file, which contains multiple archived user profiles.

To delete an archive file
1) Access the Work with Archived Profiles interface.
2) In the OPT column for the desired archive file, enter 9 (Delete Archive File).
3) Press **Enter** twice.

**See also**

*Working with Archived Profiles*
Run Archived Profile Reports

Use this task to generate the following archived profile reports:

- Run User Profile Archive Report
- Run User Profile Archive Changes Report

**Tip:** You can schedule the archived profile reports (like all other reports) to run when most convenient.

**Note:** To work with archived profile reports, access from the User Profile Reports interface.

To access the User Profile Reports interface

1) Access the TGSecure Main menu.
2) At the **Selection or command** prompt, enter 5 (User Profile Management).
3) Press Enter.
4) At the **Selection or command** prompt, enter 20 (User Profile Reports).
5) Press Enter. The User Profile Reports interface is displayed.

Run User Profile Archive Report

Use this report to view the list of archived profiles.

To run the User Profile Archive Report

1) Access the User Profile Reports interface.
2) At the **Selection or command** prompt, enter 2 (User Profile Configuration Reports).
3) Press Enter. The User Profile Configuration Reports interface is displayed.
4) At the **Selection or command** prompt, enter 9 (User Profile Archive).
5) Press Enter.
6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run User Profile Archive Changes Report
To run the User Profile Archive Changes Report

1) Access the User Profile Reports interface.

2) At the Selection or command prompt, enter 3 (User Profile Change Reports).

3) Press Enter. The User Profile Change Reports interface is displayed.

4) At the Selection or command prompt, enter 9 (User Profile Archive Changes).

5) Press Enter.

6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

See also

Working with Archived Profiles
Inactive Profiles

This section describes how to work with **Inactive Profiles**.

This section includes the following topics:

- Working with Inactive Profiles
- Display Inactive Profile Settings
- Manage Inactive Profiles
- Run Inactive Profile Reports

**See also**

User Profile Management
Working with Inactive Profiles

Use the Inactive Profile feature to do the following:

- Display Inactive Profile Settings
- Manage Inactive Profiles
- Run Inactive Profile Reports

Note: To work with inactive profiles, you must access the Profile Inactivity Settings interface.

To access the Profile Inactivity Settings interface

1) Log into TGSecure. The Main menu appears.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter. The User Profile Management interface is displayed.
4) At the Selection or command prompt, enter 5 (Profile Inactivity Settings).
5) Press Enter. The Profile Inactivity Settings interface is displayed.

See also

Inactive Profiles
Display Inactive Profile Settings

Use this task to display the inactive profile settings.

To display Inactive profile settings

1) From the TGSecure Main menu appears.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 5 (Profile Inactivity Settings).

5) Press Enter. The Profile Inactivity Settings interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity until user profile is disabled</td>
<td>Number of days before an inactive user profile is disabled</td>
</tr>
<tr>
<td>Inactivity until user profile is deleted</td>
<td>Number of days before an inactive user profile is deleted</td>
</tr>
<tr>
<td>Delete profiles with password of *NONE</td>
<td>Whether to delete profiles that do not have an assigned password</td>
</tr>
<tr>
<td></td>
<td>*YES - Delete the profiles</td>
</tr>
<tr>
<td></td>
<td>*NO - Keep the profiles</td>
</tr>
<tr>
<td>Object owner for objects owned by deleted</td>
<td>The name of the user who will inherit ownership of objects for deleted user profiles</td>
</tr>
<tr>
<td>profiles</td>
<td></td>
</tr>
<tr>
<td>Remove deleted profiles from TG user group</td>
<td>Whether to remove deleted profiles from TG user groups</td>
</tr>
<tr>
<td></td>
<td>*YES - Delete the user profile from TG groups</td>
</tr>
<tr>
<td></td>
<td>*NO - Keep the user profile as a member of TG groups</td>
</tr>
<tr>
<td>Remove deleted profiles from TG rules</td>
<td>Whether to remove deleted profiles from TG rules.</td>
</tr>
<tr>
<td></td>
<td>*YES - Delete the user profile from rule definition</td>
</tr>
<tr>
<td></td>
<td>*NO - Keep the user profile as part of rule definition</td>
</tr>
<tr>
<td>Alert when inactivity found</td>
<td>Whether to send an alert to the admin when inactive profiles are detected</td>
</tr>
<tr>
<td></td>
<td>*YES - Enable alerts</td>
</tr>
<tr>
<td></td>
<td>*NO - Disable alerts</td>
</tr>
</tbody>
</table>

See also

Working with Inactive Profiles
Manage Inactive Profiles

Use this task to manage inactive profiles.

- Access the Profile Inactivity Settings Interface
- Edit Inactive Profile Settings
- Display the List of Inactive Profiles
- Enforce Inactive Profile Rules

**Note:** To manage Profile Manager defaults, access the Profile Inactivity Settings interface.

Access the Profile Inactivity Settings Interface

To access the Profile Inactivity Settings interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter. The User Profile Management interface is displayed.
4) At the Selection or command prompt, enter 5 (Profile Inactivity Settings).
5) Press Enter. The Profile Inactivity Settings interface is displayed.

Edit Inactive Profile Settings

To display Inactive profile settings

1) Access the Profile Inactivity Settings interface.
2) Modify the necessary parameters:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity until user profile is disabled</td>
<td>Number of days before an inactive user profile is flagged as needing to be disabled</td>
</tr>
<tr>
<td>Inactivity until user profile is deleted</td>
<td>Number of days before an inactive user profile is flagged as needing to be deleted</td>
</tr>
<tr>
<td>Delete profiles with password of *NONE</td>
<td>Whether to delete profiles with the password value of *NONE</td>
</tr>
<tr>
<td></td>
<td>*YES - Delete the profiles</td>
</tr>
<tr>
<td></td>
<td>*NO - Keep the profiles</td>
</tr>
<tr>
<td>Object owner for objects owned by deleted profiles</td>
<td>The name of the user who will inherit ownership of objects from deleted or disabled user profiles</td>
</tr>
<tr>
<td></td>
<td>Note: All objects must be assigned an owner.</td>
</tr>
<tr>
<td>Remove deleted profiles from TG user group</td>
<td>Whether to remove deleted profiles from TG user groups</td>
</tr>
<tr>
<td></td>
<td>*YES - Delete the user profile from TG groups</td>
</tr>
<tr>
<td></td>
<td>*NO - Keep the user profile as a member of TG groups</td>
</tr>
</tbody>
</table>
Remove deleted profiles from TG rules | Whether to remove rules that are no longer associated with a user because the user profile for which the rule was defined is no longer present in the system  
*YES* - Delete the rule  
*NO* - Keep the rule  

Alert when inactivity found | Whether to send an alert to the admin when inactive profiles are detected  
*YES* - Enable alerts  
*NO* - Disable alerts  

3) Press **Enter** twice.

**Display the List of Inactive Profiles**

Use this task to display the list of user profiles that the system (based on the inactive profile settings) has deemed as inactive.

**To display the list of inactive user profiles**

1) Access the **Profile Inactivity Settings** interface.
2) Press the **F22** (Run Inactive Report) function key on your keyboard.

- **Tip**: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F24**, you must hold down the **Shift** key and **F12**.

3) Modify the report run criteria as necessary.

- **Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see **Run TGSecure Reports**.

- **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Enforce Inactive Profile Rules**

Use this task to enforce the inactive profile rules.

- **Note**: Whether a profile is disabled or deleted during enforcement is based on the inactive profile settings.

**To enforce profile inactivity rules**

1) Access the **Profile Inactivity Settings** interface.
2) Press the **F23** (Run Inactivity Enforcement) function key on your keyboard.

- **Tip**: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F23**, you must hold down the **Shift** key and **F11**.

3) Modify the report run criteria as necessary.
4) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

*Working with Inactive Profiles*
Run Inactive Profile Reports

Use this task to generate the following inactive profile reports:

- Run Inactivity Compliance Report (TGPRFCMP)
- Run Profile Inactivity Settings Report
- Run Profile Inactivity Settings Changes Report

Tip: You can schedule the Archived Profile reports (like all other reports) to run when most convenient.

Note: To work with Archived Profile reports, access from the User Profile Reports interface.

To access the User Profile Reports interface
1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (User Profile Reports).
5) Press Enter. The User Profile Reports interface is displayed.

Run Inactivity Compliance Report (TGPRFCMP)

Use this report to display the list of inactive profiles.

To run the Inactivity Compliance Report
1) Access the User Profile Reports interface.
2) At the Selection or command prompt, enter 1 (User Profile Usage Reports).
3) Press Enter. The User Profile Usage Reports interface is displayed.
4) At the Selection or command prompt, enter 2 (Inactivity Compliance Report).
5) Press Enter.
6) Complete the following fields:

Tip: To see the complete list of available parameters, press the F9 function key.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Enter *INACTIVITY</td>
</tr>
<tr>
<td>Audit report</td>
<td>Enter *YES to enable auditing (tracking)</td>
</tr>
</tbody>
</table>
To run the Profile Inactivity Settings Report

1) Access the User Profile Reports interface.

2) At the Selection or command prompt, enter 10 (Profile Inactivity Settings).

3) Press Enter. The User Profile Configuration Reports interface is displayed.

4) At the Selection or command prompt, enter 10 (Profile Inactivity Settings).

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
5) Press **Enter**.

6) Modify the report run criteria as necessary.

   **Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run Profile Inactivity Settings Changes Report

Use this report to view the list of changes made to the profile inactivity settings.

#### Tip: You must enable auditing to produce change reports. See Manage User Profile Management Defaults for additional information.

### To run the Profile Inactivity Settings Changes Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter 3 (User Profile Change Reports).

3) Press **Enter**. The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 10 (Profile Inactivity Settings Changes).

5) Press **Enter**.

6) Modify the report run criteria as necessary.

   **Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

   **Tip:** Place your cursor in a field and press **F1 (Help)** to access a field description. Press **F4 (Prompt)** for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### See also

**Working with Inactive Profiles**
User Profiles

This section describes how to work with User Profiles.

This section includes the following topics:

- Working with User Profiles
- Manage User Profiles
- Run User Profile Reports

See also

User Profile Management
Working with User Profiles

Use the User Profile feature to do the following:

- Manage User Profiles
- Run User Profile Reports

**Note:** To work with user profiles, you must access the TG User Profile Manager interface.

To access the TG User Profile Manager interface

1) Log into TGSecure. The Main menu appears.

2) At the Selection or command prompt, enter 5 (User Profile Management).

3) Press Enter. The User Profile Management interface is displayed.

4) At the Selection or command prompt, enter 4 (Create/Change User Profile - TGUSRMGR).

5) Press Enter. The TG User Profile Manager interface is displayed.

See also

User Profiles
Manage User Profiles

Use this task to manage user profiles.

- Access the TG User Profile Manager Interface
- Create User Profile Based on a Blueprint
- Change User Profile Based on a Blueprint

Note: To manage user profiles using blueprints, access the TG User Profile Manager interface.

Access the TG User Profile Manager Interface

To access the TG User Profile Manager interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter. The User Profile Management interface is displayed.
4) At the Selection or command prompt, enter 4 (Create/Change User Profile - TGPRFMGR).
5) Press Enter. The TG User Profile Manager interface is displayed.

Create User Profile Based on a Blueprint

Use this task to create a user profile based on a blueprint.

Tip: Ensure you have permission to use the blueprint to create profiles before attempting this task.

To create a user profile based on a blueprint

1) Access the TG User Profile Manager interface.
2) In the Action type field, enter *CRT.
3) Press Enter.
4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint ID</td>
<td>Name of the blueprint on which to base the user profile</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of the user or user group</td>
</tr>
<tr>
<td>User Description</td>
<td>Description of the user</td>
</tr>
<tr>
<td>Add to Blueprint user group</td>
<td>Whether to add the user to the user group associated with the named blueprint</td>
</tr>
<tr>
<td></td>
<td>*YES - Add the user to the blueprint user group</td>
</tr>
<tr>
<td></td>
<td>*NO - Base the user profile on the blueprint only, but do not add the user to the blueprint user group</td>
</tr>
</tbody>
</table>
5) Press Enter.

**Change User Profile Based on a Blueprint**

Use this task to change a user profile based on a blueprint.

![Tip: Ensure you have permission to use the blueprint to change profiles before attempting this task.]

**To change a user profile based on a blueprint**

1) Access the TG User Profile Manager interface.

2) In the Action type field, enter *CHG*.

3) Press Enter.

4) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint ID</td>
<td>Name of the blueprint on which to base the user profile</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of the user</td>
</tr>
<tr>
<td>User Description</td>
<td>Description of the user</td>
</tr>
<tr>
<td>Add to Blueprint user group</td>
<td>Whether to add the user to the user group associated with the named blueprint</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Add the user to the blueprint user group</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Based the user profile on the blueprint only, but do not add the user to the blueprint user group</td>
</tr>
</tbody>
</table>

5) Press Enter.

**See also**

Working with User Profiles
Run User Profile Reports

Use this task to run the following user profile reports:

- Run User Profile Create/Change via Blueprint
- Run User Profile Activity Report
- Run User Profile Changes Report
- Run Invalid Sign-on Attempts Report
- Run Authority Failures For User Report

Tip: You can schedule the user profile reports (like all other reports) to run when most convenient.

Note: To work with user profile reports, access from the User Profile Reports interface.

To access the User Profile Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 5 (User Profile Management).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (User Profile Reports).
5) Press Enter. The User Profile Reports interface is displayed.

Run User Profile Create/Change via Blueprint

Use this report to view the profiles either created or changed using the profile manager feature.

To run the User Profile Create/Change via Blueprint Report

1) Access the User Profile Reports interface.
2) At the Selection or command prompt, enter 1 (User Profile Usage Reports).
3) Press Enter. The User Profile Usage Reports interface is displayed.
4) At the Selection or command prompt, enter 3 (User Profile Create/Change via Blueprint).
5) Press Enter.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run User Profile Activity Report**

Use this report to view modifications made to user profiles. The information is presented in two-row partners. The first row shows the previous state and the second row shows the change state.

**Tip:** This report has numerous columns. If you are interested in only a subset of user profile parameters, consider creating a custom report based on this built-in report.

**To run the User Profile Activity Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter 1 (User Profile Usage Reports).

3) Press Enter. The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 4 (User Profile Activity).

5) Press Enter.

6) Modify the report run criteria as necessary.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

7) Press Enter.

**Note:** The status of the report is displayed at the bottom of the screen.

**Run User Profile Changes Report**

Use this report to view who has modified user profiles and what they have changed.

**Tip:** You must enable auditing to produce change reports. See **Manage User Profile Management Defaults** for additional information.

**To run the User Profile Change Report**

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter 1 (User Profile Usage Reports).

3) Press Enter. The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter 6 (User Profile Changes).

5) Press Enter.
6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Invalid Sign-on Attempts Report**

Use this report to view the list of unsuccessful sign-on attempts.

**To run the Invalid Sign-on Attempts Report**

1) Access the User Profile Reports interface.

2) At the **Selection or command** prompt, enter 1 (User Profile Usage Reports).

3) Press Enter. The User Profile Usage Reports interface is displayed.

4) At the **Selection or command** prompt, enter 5 (Invalid Sign-on Attempts).

5) Press Enter.

6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Authority Failures For User Report**

Use this report to view job failures due to inadequate user authorities.

**To run the Invalid Sign-on Attempts Report**

1) Access the User Profile Reports interface.

2) At the **Selection or command** prompt, enter 1 (User Profile Usage Reports).

3) Press Enter. The User Profile Usage Reports interface is displayed.

4) At the **Selection or command** prompt, enter 7 (Authority Failures For User).

5) Press Enter.
6) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**See also**

Working with User Profiles
Password Rules

This section describes how to work with Password Rules.

This section includes the following topics:

- Working with Password Rules
- Manage Password Rules

See also

User Profile Management
Working with Password Rules

Use the **Password Rules** feature to do the following:

> **Note:** To work with inactive profiles, you must access the **Password Rule Settings** interface.

**To access the Password Rules Settings interface**

1) Log into TGSecure. The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).

3) Press **Enter**. The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **6** (Password Rule Settings).

5) Press **Enter**. The **Password Rules Settings** interface is displayed.

**See also**

*Password Rules*
Manage Password Rules

Use this task to manage password rules.

- Access the Work with Password Rules Setting Interface
- Add Password Exit Program
- Remove Password Exit Program
- Edit Password Rules

**Note:** To manage password rules, access the Password Rules Setting interface.

Access the Work with Password Rules Setting Interface

To access the Work with Password Rules Setting interface

1) Access the TGSecure Main menu.

2) At the **Selection or command** prompt, enter 5 (User Profile Management).

3) Press **Enter**. The User Profile Management interface is displayed.

4) At the **Selection or command** prompt, enter 6 (Password Rules Settings).

5) Press **Enter**. The Password Rules Setting is displayed.

Add Password Exit Program

Use this task to add (install) the password exit program.

**Note:** Before using the Profile Manager to modify password rules, you must install the password exit program.

To add password exit programs

1) Access the Password Rule Settings interface.

2) Press the **F20** (Add Password Exits) function key on your keyboard.

**Tip:** For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F20**, you must hold down the **Shift** key and **F8**.

Remove Password Exit Program

Use this task to remove the password exit program.

To remove password exit programs

1) Access the Password Rule Settings interface.

2) Press the **F21** (Remove Password Exits) function key on your keyboard.
Edit Password Rules

Use this task to edit password rules.

Tip: Changes made in this interface will not impact password rules unless the password exit program is installed.

Note: IBM provides documentation for all password rule parameters. To access the IBM documentation, enter the following at the **Selection or command** prompt: `WRKSYSVAL SYSVAL(QPWDRULES)` and then press F1 (Help).

To edit password rules

1) Access the **Password Rules Setting** interface.

2) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current password level (QPWDLVL)</td>
<td>Enter the desired password level</td>
</tr>
<tr>
<td>Password rule value set to *PWDSYSVAL</td>
<td>Whether to use default system values or custom rules</td>
</tr>
<tr>
<td></td>
<td>*YES - Use default password system values</td>
</tr>
<tr>
<td></td>
<td>*NO - Allow the admin to customize password rules</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: This value must be set to *NO if you want to use the profile manager feature to update password rules.</td>
</tr>
<tr>
<td>Number of mixed case letters (*MIXCASEn)</td>
<td>[0-9] - Number of mix-case letters required in the password</td>
</tr>
<tr>
<td>Limit repeat characters (*CHRLMTREP)</td>
<td>Whether a password to contain characters that repeat (appears next to each other)</td>
</tr>
<tr>
<td></td>
<td><strong>Y</strong> - Disallow consecutive use of characters</td>
</tr>
<tr>
<td></td>
<td><strong>N</strong> - Allow consecutive use of characters</td>
</tr>
<tr>
<td>Limit same character (*LMTSAMPOS)</td>
<td>Whether characters can be used in the same position as the previous password</td>
</tr>
<tr>
<td></td>
<td><strong>Y</strong> - Disallow characters in the same position</td>
</tr>
<tr>
<td></td>
<td><strong>N</strong> - Allow characters in the same position</td>
</tr>
<tr>
<td>Require upper/lower/digits/special char (*REQANY3)</td>
<td>Whether a password is required to contain the following types of characters: uppercase, lowercase, special characters or digits</td>
</tr>
<tr>
<td></td>
<td><strong>Y</strong> - Require character variation</td>
</tr>
<tr>
<td></td>
<td><strong>N</strong> - Do not require character variation</td>
</tr>
</tbody>
</table>
| Limit profile name (*LMTPRFNAME) | Whether a password can contain the user’s profile name.  
Y - Disallow user’s profile name in password  
N - Allow user’s profile name in password |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password cannot be same as last</td>
<td>[0-32] - Number of times before a password can be repeated</td>
</tr>
</tbody>
</table>
| Block password change (Hours)   | [1-99] - Number of hours allowed between password changes  
**Note:** Enter *NONE* to ignore this rule. |
| Password expiration interval (Days) | [1-366] - Number of days a password is valid  
**Note:** Enter *NOMAX* to ignore this rule. |
| Password expiration warning (Days) | [1-99] - Number of days before a password expiration warning is issued to the user |
| Limit Adjacent                   | Whether to allow adjacent elements:  
Y - Disallow adjacent characters, digits, or special characters  
N - Allow adjacent characters, digits, or special characters |
| Limit First Char                 | Whether to place limits on the first character  
Y - Disallow password to start with a character, digit, or special character  
N - Allow password to start with a character, digit, or special character |
| Limit Last Char                  | Whether to place limits on the last character  
Y - Disallow password to end with a character, digit, or special character  
N - Allow password to end with a character, digit, or special character |
| Maximum                          | [0-9] - Maximum number of characters, digits, or special characters allowed in the password |
| Minimum                          | [0-9] - Minimum number of characters, digits, or special characters allowed in the password (0-9) |

3) Press the **F8** (Save Settings) function key on your keyboard.

**See also**

*Working with Password Rules*
Command Security

Use the **Command Security** feature to add an additional layer of security at the command level. IBM security is based on object-level authorities, which is one level above commands. If a user has access to an object, then they can perform all authorized commands on that object. The **Command Security** feature allows you to limit which commands can be executed, even though the user has permission via Object authority.

**Tip:** The error message given to the end-user who is blocked from executing a command might be difficult for the user to decode (last request at level [N] ended), but the administrator can see full, clear details about why a user/user group was blocked from executing a command in the job log (dspjoblog).

### To access the Command Security interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter 6 (Command Security).

3) Press **Enter**.

This section contains the following topics:

- Command Security Defaults
- Command Security Rules
- Command Security Reports

**See also**

Getting Started
Command Security Defaults

Use the Command Security Defaults to define the following:

This section includes the following topics:

- Working with Command Security Defaults
- Display Command Security Defaults
- Manage Command Security Defaults

Note: To manage network defaults, access the Command Security Defaults interface.

To access the Command Security Defaults interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 6 (Command Security).
3) Press Enter. The Command Security interface is displayed.
4) At the Selection or command prompt, enter 10 (Command Security Defaults).

See also

Command Security
Working with Command Security Defaults

Use the **Command Security Defaults** feature to do the following:

- Display Command Security Defaults
- Manage Command Security Defaults
- Run Command Security Reports

**Note**: To manage network defaults, access the **Command Security Defaults** interface.

To access the Command Security Defaults interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter 6 (Command Security).

3) Press **Enter**. The **Command Security** interface is displayed.

4) At the **Selection or command** prompt, enter 10 (Command Security Defaults).

5) Press **Enter**. The **Command Security Defaults** interface is displayed.

**See also**

Command Security
Display Command Security Defaults

Use this task to display network security default settings.

To display the Command Security defaults

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter 6 (Command Security).

3) Press **Enter**. The **Command Security** interface is displayed.

4) At the **Selection or command** prompt, enter 10 (Command Security Defaults).

5) Press **Enter**. The **Command Security Defaults** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit Status</strong></td>
<td>Whether auditing is enabled globally (for all command security rules).</td>
</tr>
<tr>
<td><strong>YES</strong> - Record</td>
<td>command security changes in the audit journal</td>
</tr>
<tr>
<td><strong>NO</strong> - Do not</td>
<td>command security changes in the audit journal</td>
</tr>
<tr>
<td><strong>Tip</strong>: Auditing is required if you plan to run command security reports.</td>
<td></td>
</tr>
<tr>
<td><strong>Audit Journal</strong></td>
<td>Journal in which to store command security data</td>
</tr>
<tr>
<td><strong>Note</strong>: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
<td></td>
</tr>
<tr>
<td><strong>Audit Journal Library</strong></td>
<td>Library in which the journal resides</td>
</tr>
<tr>
<td><strong>Audit Configuration Changes</strong></td>
<td>Whether to collect data about command security changes</td>
</tr>
<tr>
<td><strong>Y</strong> - Enable tracking of changes</td>
<td><strong>N</strong> - Disable tracking of changes</td>
</tr>
<tr>
<td><strong>Tip</strong>: Set this flag to <strong>Y</strong> if you plan to run command security change reports.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: There are multiple TGSecure modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see <strong>NONE</strong> 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 <strong>PARTIAL</strong>, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see <strong>ALL</strong>, this indicates that configuration changes are being tracked in all modules.</td>
<td></td>
</tr>
<tr>
<td><strong>Alert Status</strong></td>
<td>Whether alerting is enabled globally (for all command rules). Alerting is required if you plan to send alert notifications.</td>
</tr>
<tr>
<td><strong>YES</strong> - Enable alerts</td>
<td><strong>NO</strong> - Disable alerts</td>
</tr>
<tr>
<td><strong>Tip</strong>: If alerts are disabled at the command security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the command rule (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific command rule. See <strong>Manage Command Security Rules</strong> for information about setting the alert status for an individual exit point.</td>
<td></td>
</tr>
<tr>
<td>Alert Message Queue</td>
<td>Queue in which to store alerts</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> You can change the queue if you are using a third-party application for message monitoring.</td>
<td></td>
</tr>
<tr>
<td>Alert Message Queue Library</td>
<td>Library in which the queue is located</td>
</tr>
<tr>
<td>Primary Group Inheritance</td>
<td>Whether to allow primary group inheritance</td>
</tr>
<tr>
<td><em>YES</em> - Enable profile inheritance for the primary group</td>
<td></td>
</tr>
<tr>
<td><em>NO</em> - Disable profile inheritance for the primary group</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The primary group is the user ID entered in the Group profile field when using command <strong>CHGUSRPRF</strong>. The primary group is the first ID from which a user inherits privileges.</td>
<td></td>
</tr>
<tr>
<td>Supplemental Group Inheritance</td>
<td>Whether to allow supplemental group inheritance</td>
</tr>
<tr>
<td><em>YES</em> - Enable profile inheritance for supplemental groups</td>
<td></td>
</tr>
<tr>
<td><em>NO</em> - Disable profile inheritance for supplemental groups</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The supplemental groups are user IDs entered in the Supplemental group field when using command <strong>CHGUSRPRF</strong>. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.</td>
<td></td>
</tr>
<tr>
<td>Command Security</td>
<td>Whether to enable the <strong>Command Security</strong> feature</td>
</tr>
<tr>
<td><em>YES</em> - Enable the Command Security feature</td>
<td></td>
</tr>
<tr>
<td><em>NO</em> - Disable the Command Security feature</td>
<td></td>
</tr>
</tbody>
</table>

**See also**

*Working with Command Security Defaults*
Manage Command Security Defaults

Use this task to manage Command Security default settings.

- Access the Command Security Defaults Interface
- Enable Command Security (Globally)
- Enable Command Security Auditing
- Enable Command Security Change Auditing
- Enable Command Security Alerts
- Enable Group Profile Inheritance

Note: To manage network defaults, access the Command Security Defaults interface.

Access the Command Security Defaults Interface

To access the Command Security Defaults interface
1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 6 (Command Security).
3) Press Enter. The Command Security interface is displayed.
4) At the Selection or command prompt, enter 10 (Command Security Defaults).

Enable Command Security (Globally)

Use this task to enable/disable command security globally (TGCMSEC).

Alternatively, this same action can be executed by entering *YES/*NO in the Command Security (Enable/Disable) field in the Command Security Defaults interface.

To enable/disable command security globally
1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 6 (Command Security).
3) Press Enter. The Command Security interface is displayed.
4) At the Selection or command prompt, enter 2 (Enable/Disable Command Security).
5) Press Enter. The TG Command Security (TGCMSEC) interface is displayed.
6) In the Enable Command Security field, enter the desired option:
   - *YES - Enable the Command Security feature
   - *NO - Disable the Command Security feature (disregard all command security rules)
Enable Command Security Auditing

Use this task to enable command security auditing.

Tip: Auditing is required if you plan to run network security reports.

Note: If auditing is disabled at the command security (module) level, then auditing will not occur. The module-level setting takes precedence. However, if auditing is enabled at the module level, you must also enable it at the secondary level (each command rule) if you want to record auditing data for a specific command rule.

To enable command security auditing

1) Access the Command Security Defaults interface.
2) In the Auditing Status field, enter *YES.
3) In the Audit Journal field, enter the name of the journal in which to store the auditing data.
4) In the Audit Journal Library field, enter the name of the library in which the journal resides.
5) Press Enter. The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Enable Command Security Change Auditing

Use this task to enable tracking of command security configuration changes.

Tip: Tracking is required if you plan to run command security change reports.

To enable command security configuration change tracking

1) Access the Command Security Defaults interface.
2) In the Audit Configuration Changes field, enter Y.
3) Press Enter.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL, this indicates that configuration changes are being tracked in all modules.

Enable Command Security Alerts

Use this task to enable command security alerts.

Tip: Alerting is required if you plan to send alert notifications.
To enable command security alerts

1) Access the Command Security Defaults interface.

2) In the Alert Status field, enter “YES.”

3) In the Alert Message Queue field, enter the name of the queue in which to store the alerts.

4) In the Alert Message Queue Library field, enter the name of the library in which the queue resides.

5) Press Enter.

Enable Group Profile Inheritance

Use this task to enable users to inherit privileges as defined in their IBM profile. In other words, if an IBM user profile is a member of a group (as defined by the Group profile and/or Supplemental group profile parameters), then you can use the following instruction to ensure that rules created in TGSecure consider the privileges inherited by users when the system is enforcing rules.

Here is a usage example. There are two IBM users: User AAA (higher privilege user) and user BBB (lower privilege user). An IBM user administrator decides to allow user BBB to inherit the privileges from user AAA. To do this, the IBM user administrator uses the command CHGUSRPRF, and then enters AAA in the Group profile or Supplemental group parameter. By taking this action, the user administrator is allowing user BBB to inherit the privileges as user AAA. Now if you want the inherited privileges granted by the IBM user administrator to be considered in TGSecure when evaluating rules, then you must enable group profile inheritance in TGSecure.

To enable group profile inheritance

1) Access the Command Security Defaults interface.

2) In the Primary Group Inheritance field, enter “YES.”

3) In some cases, a user might inherit privileges from multiple users. In such a case, enter “YES in Supplemental Group Inheritance field.

4) Press Enter.

Note: The primary group is the user ID entered in the Group profile field when using command CHGUSRPRF. The primary group is the first ID from which a user inherits privileges.

Note: Supplemental groups are user IDs entered in the Supplemental group field when using command CHGUSRPRF. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.

Note: If alerts are disabled at the command security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the rule (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific rule.

Tip: Refer to the IBM knowledge base for additional information regarding primary and secondary group inheritance.
See also

Working with Command Security Defaults
Command Security Rules

Use Command Security rules to implement restrictions on commands.

This section contains the following topics:

- Working with Command Security Rules
- Display List of Command Security Rules
- Manage Command Security Rules

Note: To work with command security rules, access the Work with Command Security interface.

To access the Work with Command Security interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 6 (Command Security).

3) Press Enter. The Command Security interface is displayed.

4) At the Selection or command prompt, enter 1 (Work with Command Security Rules).

5) Press Enter. The Work with Command Security interface is displayed.

See also

Command Security
Working with Command Security Rules

Use **Command Security** rules to do the following:

- Display List of Command Security Rules
- Manage Command Security Rules
- Run Command Security Reports

**Note:** To work with command security rules, access the **Work with Command Security** interface.

To access the Work with Command Security interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter 6 (Command Security).
3) Press **Enter**. The **Command Security** interface is displayed.
4) At the **Selection or command** prompt, enter 1 (Work with Command Security Rules).
5) Press **Enter**. The **Work with Command Security** interface is displayed.

See also

**Command Security Rules**
Display List of Command Security Rules

Use this task to display Command Security rules.

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of command security rules.

To display the list of command security rules

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 6 (Command Security).
3) Press Enter. The Command Security interface is displayed.
4) At the Selection or command prompt, enter 1 (Work with Command Security Rules).
5) Press Enter. The Work with Command Security interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Name of command</td>
</tr>
<tr>
<td>Library</td>
<td>Library in which command resides</td>
</tr>
<tr>
<td>User</td>
<td>User or user group to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address to which the rule applies</td>
</tr>
<tr>
<td>Calendar</td>
<td>Applicable calendar</td>
</tr>
<tr>
<td></td>
<td>Note: the calendar limits when the rule is applicable.</td>
</tr>
<tr>
<td>Parm Rest</td>
<td>Whether parameter restrictions are enabled:</td>
</tr>
<tr>
<td></td>
<td>*YES - Parameter restrictions are enabled</td>
</tr>
<tr>
<td></td>
<td>*NO - Parameter restrictions are disabled</td>
</tr>
<tr>
<td></td>
<td>Note: Parameter restrictions limit which parameters a user can enter for a command.</td>
</tr>
<tr>
<td>Alert Sts</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>Exit Inst</td>
<td>Whether the associated exit point is installed:</td>
</tr>
<tr>
<td></td>
<td>*YES - Exit point installed</td>
</tr>
<tr>
<td></td>
<td>*NO - Exit point not installed</td>
</tr>
<tr>
<td>Action</td>
<td>The level at which action was taken:</td>
</tr>
<tr>
<td></td>
<td>*EXITLVL - Exit point level</td>
</tr>
<tr>
<td></td>
<td>Note: If the action failed, you will see *FAIL in this column.</td>
</tr>
</tbody>
</table>
Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the User column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Command Security interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Command Security interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk to help define your subset.
- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the Work with Command Security interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter. The system filters the results based on the criteria you defined for the subset.
See also

Working with Command Security Rules
Manage Command Security Rules

Use this task to manage Command Security rules.

- Access the Work with Command Security Interface
- Add Command Security Rule
- Edit Command Security Rule
- Copy Command Security Rule
- Delete Command Security Rule
- Create Parameter Restriction

Note: To manage command security rules, access the Work with Command Security interface.

Access the Work with Command Security Interface

To access the Work with Command Security Interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 6 (Command Security).

3) Press Enter. The Command Security interface is displayed.

4) At the Selection or command prompt, enter 1 (Work with Command Security Rules).

5) Press Enter. The Work with Command Security interface is displayed.

Add Command Security Rule

Use this task to add a command security rule.

Tip: You can define a command security rule for groups of users, networks, or operations.

To add a command security rule

1) Access the Work with Command Security interface.

2) Press the F6 (Add) function key.

3) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Name</td>
<td>Enter the name you want to assign the command rule</td>
</tr>
<tr>
<td>Command Library</td>
<td>Enter the library in which the command rule resides</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user or user group to which the rule applies</td>
</tr>
<tr>
<td>Client IP</td>
<td>Enter the IP address to which the rule applies</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Status</td>
<td>Identify whether to enable the rule</td>
</tr>
<tr>
<td>*YES - Rule enabled</td>
<td>*NO - Rule disabled</td>
</tr>
<tr>
<td>Audit Status</td>
<td>Identify whether to enable auditing</td>
</tr>
<tr>
<td>*YES - Auditing enabled</td>
<td>*NO - Auditing disabled</td>
</tr>
<tr>
<td>Note: Auditing must be enabled to generate reports.</td>
<td></td>
</tr>
<tr>
<td>Alert Status</td>
<td>Identify whether to enable alerting:</td>
</tr>
<tr>
<td>*YES - Alerts enabled</td>
<td>*NO - Alerts disabled</td>
</tr>
<tr>
<td>Calendar</td>
<td>Enter the applicable calendar</td>
</tr>
<tr>
<td>Note: the calendar limits when the rule is applicable.</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Enter the level at which to execute the action:</td>
</tr>
<tr>
<td>*EXITLVL - Exit point level</td>
<td>*FAIL - If the action failed, you will see *FAIL in this column.</td>
</tr>
<tr>
<td>Note: If the action failed, you will see *FAIL in this column.</td>
<td></td>
</tr>
<tr>
<td>Parameter Restriction</td>
<td>Identify whether to enable parameter restrictions:</td>
</tr>
<tr>
<td>*YES - Parameter restrictions are enabled</td>
<td>*NO - Parameter restrictions are disabled</td>
</tr>
<tr>
<td>Note: Parameter restrictions limit which parameters a user can enter for a command.</td>
<td></td>
</tr>
<tr>
<td>Exit Installed</td>
<td>Identify whether to install the associated exit point:</td>
</tr>
<tr>
<td>*YES - Exit point installed</td>
<td>*NO - Exit point not installed</td>
</tr>
</tbody>
</table>

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**.

**Note:** At this point, you might receive suggestions from the system. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server) as well.

**Edit Command Security Rule**

Use this task to edit an existing command security rule.

**To edit a command security rule**


2) In the OPT column for the desired command security rule, enter 2 (Edit).

3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

5) Press Enter twice.

Copy Command Security Rule

Use this task to create a new rule by copying a command security rule.

To copy a command security rule

2) In the OPT column for the desired command security rule, enter 3 (Copy).
3) Press Enter.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

5) Press Enter.

Delete Command Security Rule

Use this task to delete a command security rule.

To delete a command security rule

2) In the OPT column for the desired command security rule, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct rule.
5) Press Enter.

Create Parameter Restriction

Use this task to create restrictions based on command parameters.

To create a parameter restriction

2) In the OPT column for the desired command security rule, enter 2 (Edit).
3) Press Enter.
4) In the Action field, enter one of the following options:
   - **PASS** - If the parameter restriction is met, allow the action.
   - **FAIL** - If the parameter restriction is met, disallow the action.

5) Select **YES** for the Parameter Restrictions field to enable parameter restrictions.

6) Press Enter twice.

7) In the OPT column for the desired rule, enter 10 (Work with Parameters). The Work with Command Security - Parameter interface is displayed.

8) In the Command Parm. Restriction field, enter the parameter and the parameter value (in parenthesis) that you want to restrict (pass or fail).
   For example, enter SBS (TGCMN) to restrict the parameter SBS to the parameter value of TGCMN.

9) Press Enter twice.

See also

Working with Command Security Rules
Command Security Reports

This section includes the following topics:

- Working with Command Security Reports
- Run Command Security Reports

**Note:** To work with command security reports, access from the Command Security Reports interface.

To access the Command Security Reports interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 6 (Command Security).

3) Press Enter. The Command Security interface is displayed.

4) At the Selection or command prompt, enter 20 (Command Security Reports).

5) Press Enter. The Command Security Reports interface is displayed.

See also

Command Security
Working with Command Security Reports

Use the Command Security Reports interface to do the following:
- **Run Command Security Reports**

**Note:** To work with command security reports, access from the Command Security Reports interface.

To access the Command Security Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter **6** (Command Security).
3) Press Enter. The Command Security interface is displayed.
4) At the Selection or command prompt, enter **20** (Command Security Reports).
5) Press Enter. The Command Security Reports interface is displayed.

See also

Command Security Reports
Run Command Security Reports

Use this task to generate the following Command Security reports:

- Access the Command Security Reports Interface
- Run Command Security Activity Reports
- Run Command Security Configuration Reports
- Run Command Security Change Reports

**Tip:** Refer to the TGSecure Report Reference for a complete list of report definitions.

**Note:** To work with command security rule reports, access from the Command Security Reports interface.

Access the Command Security Reports Interface

To access the Command Security Reports interface:

1) Access the TGSecure Main menu.

2) At the **Selection or command** prompt, enter 6 (Command Security).

3) Press **Enter**. The Command Security interface is displayed.

4) At the **Selection or command** prompt, enter 20 (Command Security Reports).

5) Press **Enter**. The Command Security Reports interface is displayed.

Run Command Security Activity Reports

Use this task to run the reports classified as activity reports.

To run the Command Security Activity Reports:

1) Access the Command Security Reports interface.

2) At the **Selection or command** prompt, enter 1 (Command Security Activity Reports).

3) Press **Enter**. The Command Security Activity Reports interface is displayed.

4) Select the desired activity report.

5) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.
6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run Command Security Configuration Reports

Use this task to run the reports classified as configuration reports.

**Tip**: You must enable auditing to produce change reports. See [Manage Command Security Defaults](#) for additional information.

To run the Command Security Configuration Reports

1) Access the **Command Security Reports** interface.

2) At the **Selection or command** prompt, enter 2 (Command Security Configuration Reports).

3) Press **Enter**. The **Command Security Configuration Reports** interface is displayed.

4) Select the desired configuration report.

5) Modify the report run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see [Run TGSecure Reports](#).

**Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run Command Security Change Reports

Use this task to run the reports classified as change reports.

**Tip**: You must enable auditing to produce change reports. See [Manage Command Security Defaults](#) for additional information.

To run the Command Security Change Reports

1) Access the **Command Security Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Command Security Change Reports).

3) Press **Enter**. The **Command Security Change Reports** interface is displayed.

4) Select the desired change report.

5) Modify the report run criteria as necessary.
**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see [Run TGSecure Reports](#).

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

[Working with Command Security Reports](#)
System Value Management

Use the System Value Management feature to manage...

To access the System Value Management interface

1) Log into TGSecure. The Main menu appears.

2) At the Selection or command prompt, enter 7 (System Value Management).

3) Press Enter.

This section contains the following topics:

- System Value Defaults
- System Values Rules
- System Value Reports

See also

Getting Started
System Value Defaults

Use the System Value Management Defaults to define the following:

This section includes the following topics:

- Working with System Value Management Defaults
- Display System Value Defaults
- Manage System Value Defaults

![Note: To manage system value defaults, access the System Value Default interface.]

To access the System Value Default interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 7 (System Value Management).

3) Press Enter. The System Value Management interface is displayed.

4) At the Selection or command prompt, enter 10 (System Value Management Defaults).

5) Press Enter. The System Value Default interface is displayed.

See also

System Value Management
Working with System Value Management Defaults

Use the Command Security Defaults feature to do the following:

- Display System Value Defaults
- Manage System Value Defaults
- Run System Value Management Reports

**Note:** To manage network defaults, access the System Default Default interface.

To access the System Value Default interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 7 (System Value Management).

3) Press Enter. The System Value Management interface is displayed.

4) At the Selection or command prompt, enter 10 (System Value Management Defaults).

5) Press Enter. The System Value Default interface is displayed.

See also

System Value Management
# Display System Value Defaults

Use this task to display **System Value** default settings.

**To display the System Value defaults**

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter 7 (System Value Defaults).

3) Press **Enter**. The **System Value Management** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (System Value Defaults).

5) Press **Enter**. The **System Value Default** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Journal</td>
<td>Journal in which to store command security data</td>
</tr>
<tr>
<td><strong>Note:</strong> The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
<td></td>
</tr>
<tr>
<td>Audit Journal Library</td>
<td>Library in which the journal resides</td>
</tr>
<tr>
<td>Audit Configuration Changes</td>
<td>Whether to collect data about command security changes</td>
</tr>
<tr>
<td><strong>Y</strong> - Enable tracking of changes</td>
<td><strong>N</strong> - Disable tracking of changes</td>
</tr>
<tr>
<td><strong>Tip:</strong> Set this flag to <strong>Y</strong> if you plan to run command security change reports.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> There are multiple TGSecure modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see <strong>NONE</strong> 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 <strong>PARTIAL</strong>, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see <strong>ALL</strong>, this indicates that configuration changes are being tracked in all modules.</td>
<td></td>
</tr>
<tr>
<td>Alert Status</td>
<td>Whether alerting is enabled globally (for all command rules). Alerting is required if you plan to send alert notifications.</td>
</tr>
<tr>
<td><strong>YES</strong> - Enable alerts</td>
<td><strong>NO</strong> - Disable alerts</td>
</tr>
<tr>
<td><strong>Tip:</strong> If alerts are disabled at the command security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the command rule (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific command rule. See <a href="#">Manage Command Security Rules</a> for information about setting the alert status for an individual exit point.</td>
<td></td>
</tr>
<tr>
<td>Alert Message Queue</td>
<td>Queue in which to store alerts</td>
</tr>
<tr>
<td><strong>Tip:</strong> You can change the queue if you are using a third-party application for message monitoring.</td>
<td></td>
</tr>
</tbody>
</table>
### Alert Message Queue Library

Library in which the queue is located

<table>
<thead>
<tr>
<th>Enforcement Enable</th>
<th>Whether to enforce system value rules.</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>Enable enforcement of system value rules</td>
</tr>
<tr>
<td>NO</td>
<td>Disable enforcement of system value rules</td>
</tr>
</tbody>
</table>

**See also**

*Working with System Value Management Defaults*
Manage System Value Defaults

Use this task to manage System Value default settings.

- Access the System Value Defaults Interface
- Enable System Value Enforcement
- Enable System Value Auditing
- Enable System Value Change Auditing
- Enable System Value Alerts

**Note:** To manage network defaults, access the System Value Defaults interface.

Access the System Value Defaults Interface

To access the System Value Management Defaults interface

1) Access the TGSecure Main menu.
2) At the **Selection or command** prompt, enter 7 (System Value Management).
3) Press **Enter**. The System Value Management interface is displayed.
4) At the **Selection or command** prompt, enter 10 (System Value Defaults).
5) Press **Enter**. The System Value Defaults interface is displayed.

Enable System Value Enforcement

Use this task to enable/disable system value enforcement.

Alternatively, this same action can be executed by entering *YES*/NO in the Enforcement Enable field in the System Value Default interface.

To enable/disable system value enforcement

1) Access the TGSecure Main menu.
2) At the **Selection or command** prompt, enter 7 (System Value Management).
3) Press **Enter**. The System Value Management interface is displayed.
4) At the **Selection or command** prompt, enter 10 (System Value Defaults).
5) Press **Enter**. The System Value Default interface is displayed.
6) In the Enforcement Enable field, enter the desired option:
   - *YES* - Enable the enforcement of system values
   - *NO* - Disable the enforcement of system values

Enable System Value Auditing
Use this task to enable system value auditing.

Tip: Auditing is required if you plan to run system value reports.

To enable system value auditing

1) Access the System Value Default interface.
2) In the Audit Status field, enter *YES*.
3) In the Audit Journal field, enter the name of the journal in which to store the auditing data.
4) In the Audit Journal Library field, enter the name of the library in which the journal resides.
5) Press Enter. The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Enable System Value Change Auditing

Use this task to enable tracking of system value configuration changes.

Tip: Tracking is required if you plan to run system value change reports.

To enable system value configuration change tracking

1) Access the System Value Default interface.
2) In the Audit Configuration Changes field, enter Y.
3) Press Enter.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE* in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL*, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL*, this indicates that configuration changes are being tracked in all modules.

Enable System Value Alerts

Use this task to enable system value alerts.

Tip: Alerting is required if you plan to send alert notifications.

Note: If alerts are disabled at the system value management (module) level, then alerts are not stored in the message queue even if alerts are enabled at the rule (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific rule.

To enable system value security alerts
1) Access the **System Value Default** interface.

2) In the **Alerting Status** field, enter *YES*.

3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.

4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.

5) Press **Enter**.

**See also**

*Working with System Value Management Defaults*
System Values Rules

Use **System Values** rules to establish recommendations for what is expected as the current value.

This section contains the following topics:

- Working with System Values Rules
- Display List of System Value Rules
- Manage System Value Rules

**Note:** To work with command security rules, access the **Work with System Values** interface.

To access the **Work with System Values** interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter 7 (System Values Management).

3) Press **Enter**. The **System Values** interface is displayed.

4) At the **Selection or command** prompt, enter 1 (Work with System Values).

5) Press **Enter**. The **Work with System Values** interface is displayed.

**See also**

System Value Management
Working with System Values Rules

Use **System Values** to do the following:

- Display List of System Value Rules
- Manage System Value Rules
- Run System Value Management Reports

**Note:** To work with system values, access the **Work with System Values** interface.

To access the Work with System Values interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **7** (System Value Management).
3) Press **Enter**. The **System Values** interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with System Values).
5) Press **Enter**. The **Work with System Values** interface is displayed.

**See also**

System Values Rules
Display List of System Value Rules

Use this task to display the list of System Values.

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of system value rules.

To display the list of system values rules

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 7 (System Value Management).
3) Press Enter. The System Value interface is displayed.
4) At the Selection or command prompt, enter 1 (Work with System Values).
5) Press Enter. The Work with System Values interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Value</td>
<td>Name assigned to the system value</td>
</tr>
<tr>
<td>Category</td>
<td>System value category</td>
</tr>
<tr>
<td>System Value Description</td>
<td>Description of the system value</td>
</tr>
<tr>
<td>Alt Sts</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>Expected Value</td>
<td>The parameter value expected (recommended)</td>
</tr>
<tr>
<td>Current Value</td>
<td>The parameter value currently defined</td>
</tr>
<tr>
<td>Compl Sts</td>
<td>Compliance status:</td>
</tr>
<tr>
<td></td>
<td>*PASS - Expected value and current value match</td>
</tr>
<tr>
<td></td>
<td>*FAIL - Expected value and current value differ</td>
</tr>
</tbody>
</table>

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the User column so that column heading initially appears in white text.

To sort the list

1) Access the Work with System Value interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

### Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

**To move to a specific position within the list**

1) Access the **Work with System Values** interface.

2) Sort the list based on the desired column heading.

3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

### Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with System Values** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

### See also

*Working with System Values Rules*
Manage System Value Rules

Use this task to manage System Values rules.

- Access the Work with System Values Interface
- Edit System Value Rule
- Change System Value
- Set System Value to Expected Value

Note: To manage system value rules, access the Work with System Values interface.

Access the Work with System Values Interface

To access the Work with System Values interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 7 (System Value Management).
3) Press Enter. The System Values interface is displayed.
4) At the Selection or command prompt, enter 1 (Work with System Values).
5) Press Enter. The Work with System Values interface is displayed.

Edit System Value Rule

Use this task to edit an existing system value rule.

To edit a system value rule

1) Access the Work with System Values interface.
2) In the OPT column for the desired command security rule, enter 1 (Edit).
3) Press Enter.
4) Modify the following fields as necessary:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Value</td>
<td>Name assigned to the system value</td>
</tr>
<tr>
<td>Compliance Status</td>
<td>Flag indicating whether current authority levels defined in the system align with the rule&lt;br&gt;*FAIL - There are discrepancies&lt;br&gt;*PASS - There are no discrepancies (authority levels and schema align)</td>
</tr>
<tr>
<td>Category</td>
<td>System value category</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the system value</td>
</tr>
</tbody>
</table>
To change a system value

Use this task to change a system value.

To change a system value

1) Access the **Work with System Values** interface.

2) In the **OPT** column for the desired system value, enter 2 (Change System Value).

3) Press Enter.

4) In the **Option** column for the desired system value rule, enter 2 (Change).

---

<table>
<thead>
<tr>
<th>Shipped Value</th>
<th>Parameter defined for the system value at the time the product was shipped (distributed) to the client</th>
</tr>
</thead>
<tbody>
<tr>
<td>TG Recommended</td>
<td>Parameter recommended by Trinity Guard for the system value</td>
</tr>
<tr>
<td>Current Value</td>
<td>Current parameter set for the system value</td>
</tr>
</tbody>
</table>
| Compliance Cond | The condition/range of parameters acceptable for the current value (in relation to the expected value) to be in compliance (*PASS).  
  
  **INFO** -  
  = - Current value complies if it is equal to the expected value  
  LIKE - Current value complies if it is similar to the expected value  
  NLIKE - Current value complies if it is not similar to the expected value  
  <> - Current value complies if it is not equal to the expected value  
  < - Current value complies if it is less than the expected value  
  > - Current value complies if it is greater than the expected value  
  <= - Current value complies if it is less than or equal to the expected value  
  >= - Current value complies if it is greater than or equal to the expected value |
| Alert Status   | Whether alerting is enabled:  
  *YES* - Alerts enabled  
  *NO* - Alerts disabled |
| Expected Value | The expected parameters for system value.  
  **Note**: If the current value does not match the expected value, then compliance status displays as *FAIL.** |

---

**Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.
5) Press Enter.

6) Modify the parameters as necessary.

7) Press Enter.

**Set System Value to Expected Value**

Use this task to set a system value to the expected value.

**To set a system value to the expected value**

1) Access the **Work with System Values** interface.

2) In the **OPT** column for the desired command security rule, enter 6 (Set to Expected Value).

3) Press Enter. You should receive a confirmation or information message at the bottom of the screen.

**See also**

*Working with System Values Rules*
System Value Reports

This section includes the following topics:

- Working with System Value Management Reports
- Run System Value Management Reports

Note: To work with command security reports, access from the System Value Reports interface.

To access the System Value Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 7 (System Value Management).
3) Press Enter. The System Value Management interface is displayed.
4) At the Selection or command prompt, enter 20 (System Value Reports).
5) Press Enter. The System Value Reports interface is displayed.

See also

System Value Management
Working with System Value Management Reports

Use the **Command Security Reports** interface to do the following:

- Run System Value Management Reports

| Note: | To work with command security reports, access from the **Command Security Reports** interface. |

**To access the Command Security Reports interface**

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **6** (Command Security).

3) Press **Enter**. The **Command Security** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Command Security Reports).

5) Press **Enter**. The **Command Security Reports** interface is displayed.

**See also**

System Value Reports
Run System Value Management Reports

Use this task to generate the following System Value Management reports:

- Access the System Value Reports Interface
- Run System Value Activity Reports
- Run System Value Configuration Reports
- Run System Value Change Reports

**Tip:** Refer to the TGSecure Report Reference for a complete list of report definitions.

**Note:** To work with command security rule reports, access from the System Value Management interface.

Access the System Value Reports Interface

To access the System Value Reports interface

1) Access the TGSecure Main menu.

2) At the Selection or command prompt, enter 7 (System Value Management).

3) Press Enter. The System Value Management interface is displayed.

4) At the Selection or command prompt, enter 20 (System Value Reports).

5) Press Enter. The System Value Reports interface is displayed.

Run System Value Activity Reports

Use this task to run the reports classified as activity reports.

To run the System Value Activity Reports

1) Access the System Value Reports interface.

2) At the Selection or command prompt, enter 1 (System Value Activity Reports).

3) Press Enter. The System Value Activity Reports interface is displayed.

4) Select the desired activity report.

5) Modify the report run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
6) Enter the desired output format in the Report output type field.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run System Value Configuration Reports**

Use this task to run the reports classified as configuration reports.

Tip: You must enable auditing to produce change reports. See Manage System Value Defaults for additional information.

To run the System Value Configuration Reports

1) Access the System Value Management Reports interface.

2) At the Selection or command prompt, enter 2 (System Value Configuration reports).

3) Press Enter. The System Value Configuration Reports interface is displayed.

4) Select the desired configuration report.

5) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run TGSecure Reports.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

6) Enter the desired output format in the Report output type field.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run System Value Change Reports**

Use this task to run the reports classified as change reports.

Tip: You must enable auditing to produce change reports. See Manage System Value Defaults for additional information.

To run the System Value Change Reports

1) Access the System Value Change Reports interface.

2) At the Selection or command prompt, enter 3 (System Value Change Reports).

3) Press Enter. The System Value Change Reports interface is displayed.

4) Select the desired change report.

5) Modify the report run criteria as necessary.
6) Enter the desired output format in the **Report output type** field.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

*Working with System Value Reports*
Reports

This section describes how to work with TGSecure reports. Reports allow you to display and analyze system transactions.

This section includes the following topics:

- Working with TGSecure Reports
- Display List of TGSecure Reports
- Run TGSecure Reports
- Create TGSecure Reports
- Manage TGSecure Reports

To access the Reports interface

1) Access the Main menu.

2) At the Selection or command prompt, enter 30 (Work with Reports).

3) Press Enter.

See also

Getting Started
Working with TGSecure Reports

Use the Reports feature to do the following:

- Display List of TGSecure Reports
- Run TGSecure Reports
- Create TGSecure Reports
- Manage TGSecure Reports

**Tip:** See the TGSecure Report Reference for details about a specific report.

**Note:** To work with built-in reports, access the Work with Reports interface.

To access the Work with Reports interface

1) Access the Main menu.
2) At the Selection or command prompt, enter 30 (Work with Reports).
3) Press Enter.

See also

Reports
Display List of TGSecure Reports

Use this task to do the following:

- Display list
- Sort List
- Move to Location in List
- Filter List

Display list

Use this task to display the list of available reports.

To display the list of reports

1) Access the Main menu.
2) At the Selection or command prompt, enter 30 (Work with Reports).
3) Press Enter. The Work with Reports interface is displayed.

Sort List

Use this task to sort the list of available reports. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Collector ID column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Reports interface.
2) Place your cursor on a column heading (e.g., Collector ID, Report Name, or Category).
3) Press the F10 (Sort) function key.

Tip: The system sorts the list of reports in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Location in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a report.

To move to a specific position within the list

1) Access the Work with Reports interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter.
Filter List

Use this task to limit the reports displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the Work with Reports interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter. The system filters the results based on the criteria you defined for the subset.

See also

Working with TGSecure Reports
Run TGSecure Reports

Use this task to run a built-in or custom report using the Work with Reports interface:

- Run Reports with Start and End Time Requirements
- Run Reports without Start and End Time Requirements

Tip: You can schedule reports to run when most convenient.

Run Reports with Start and End Time Requirements

Use these instructions when the report requires the start and end time entries.

Identifying a start and end time helps you filter the data reported and is required for some types of reports that have the potential to contain a huge amount of data.

To run a report with start and end time requirements

1) Access the Main menu.
2) At the Selection or command prompt, enter 30 (Work with Reports).
3) Press Enter.
4) Enter 7 in the Opt column for the report you want to run.
5) Press Enter.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector ID</td>
<td>ID identifying the collector from which report data is obtained (not an editable field)</td>
</tr>
<tr>
<td>Collector Name</td>
<td>Name assigned to the collector (not an editable field)</td>
</tr>
<tr>
<td>Report ID</td>
<td>ID assigned to the report you want to run (not an editable field)</td>
</tr>
<tr>
<td>User profile</td>
<td>Name of the user or group for which you want to report data</td>
</tr>
</tbody>
</table>

Tip: Enter "ALL" to include all users
Run Reports without Start and End Time Requirements

Use these instructions when the report does not require a start and end time.

**To run a report without start and end time requirements**

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**.

4) Enter **7** in the **Opt** column for the report you want to run.

5) Press **Enter**.

6) Modify the run criteria as necessary.

---

**Note:** The criteria allow you to limit the data returned in the report when you generate it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector ID</td>
<td>ID identifying the collector (not an editable field)</td>
</tr>
</tbody>
</table>
### Working with TGSecure Reports

#### Note:
Multiple reports can be produced from a single collector, so at this point, you could change the report ID to any of the reports linked to the identified collector.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collector</strong></td>
<td>Name assigned to the collector (not an editable field)</td>
</tr>
<tr>
<td><strong>Report ID</strong></td>
<td>ID assigned to the report you want to run (must be a report associated with the collector)</td>
</tr>
</tbody>
</table>

**Note:** Multiple reports can be produced from a single collector, so at this point, you could change the report ID to any of the reports linked to the identified collector.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Override report defaults</strong></td>
<td>Whether to override report defaults:</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Ignore run-time collector defaults</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Apply Run-time collector defaults</td>
</tr>
</tbody>
</table>

**Tip:** Run-time collector defaults maximize report efficiency. Collector defaults allow you to filter collector data before attempting to generate your report. See Create Reports for additional information about setting up run-time collector defaults.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reload collector data</strong></td>
<td>Whether to reload the collector data:</td>
</tr>
<tr>
<td></td>
<td><em>AI</em> - Allow the artificial intelligence engine to determine if data source collection should be re-run</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Re-run data source collection before producing the report output</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Used cached version of the data source collection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report output type</strong></td>
<td>Enter the desired report output format (*HTML, *PRINT, etc.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Run interactively?</strong></td>
<td>Whether to run interactively or add to batch:</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Run the report immediately</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Add the report to a batch job to be run when most efficient for the system.</td>
</tr>
</tbody>
</table>

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### See also

*Working with TGSecure Reports*
Create TGSecure Reports

Use this task to create a custom report. Creating a report is a multi-step process:

- Access the Work with Reports Interface
- Step 1: Add Report
- Step 2: Select Data Source Collector
- Step 3: Name the Report
- Step 4: Select Report Fields
- Step 5: Change Order of Fields
- Step 6: Define Report Filter Criteria
- Step 7: Define Run-time Collector Defaults
- Step 8: Confirm Report Creation

Note: To create reports, access the Work with Reports interface.

Access the Work with Reports Interface

To access the Work with Reports interface

1) Access the Main menu.
2) At the Selection or command prompt, enter 30 (Work with Reports).
3) Press Enter.

Step 1: Add Report

To add a Report

1) Access the Work with Reports interface.
2) Press the F6 (Add Report) function key on your keyboard.
3) Follow the steps in the report wizard.

Step 2: Select Data Source Collector

Use this task to select the data source collector for your custom report. Each report must have a least one source (collector) from which to pull data.

To select the data source collector

1) In the Opt column for the collector that you want to use as the data source for your report, enter 1 (Select).
2) Press Enter.

Step 3: Name the Report
Use this task to assign a name, ID, and category to your custom report.

**To identify the report**

1) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report ID</td>
<td>ID you want to assign to the report</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> The name cannot contain spaces.</td>
</tr>
<tr>
<td>Report Name</td>
<td>Name you want to assign the report</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Use a name that describes the data that will appear in the report.</td>
</tr>
<tr>
<td>Category</td>
<td>The report category under which you want to group the report</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> There are four standard categories: Configuration, Resources, Profiles, Network.</td>
</tr>
</tbody>
</table>

2) Press **Enter**.

**Note:** The report should now be linked to the collector and appear in your list of available reports under the identified category.

**Step 4: Select Report Fields**

Use this task to select the collector fields that you want to appear as columns in your report.

**Note:** By default, all collector fields are selected when you create a custom report.

**Tip:** To customize which collector fields to include, press the F4 (Select Fields) function key on your keyboard.

**To select report fields**

1) Press the **F4** (Select Fields) function key on your keyboard.

2) Enter **1** in the **Sel** column for each field you want to include as a column in your custom report.

3) Press **Enter**.
Step 5: Change Order of Fields

To change the order of the selected fields

Use this task to define the order in which fields should appear in the report.

**Tip:** The column with the lowest sequence number appears as the first column. The column with the highest sequence number appears as the last column.

1) Adjust the sequence numbers in the **Seq** column.
2) Press **Enter**.

Step 6: Define Report Filter Criteria

Use this task to define the filter criteria for your custom report.

**Note:** Filters are not necessary but might improve the performance of your report.

To build report filter criteria

1) Press the **F4** (Select Fields) function key on your keyboard.
2) Enter 1 in the **Sel** column for each field to which you want to apply a filter.
3) Press **Enter**.

To add filter criteria

1) Add operators and comparison values as necessary.
2) Press **Enter**.

![Tip: An SQL-like format is used to create report filters. For a list of supported operators, press **F10**.](image)

![Note: You can use up to five levels of nesting. To begin a nested condition, enter an open parenthesis "(" in the **Nest Str** column. Likewise, to end a nested condition, enter a closing parenthesis ")" in the **Nest End** column.](image)

![Figure: Build Report Filter Criteria](image)

**To delete filter criteria**

1) Enter **4** (Delete) in the **Opt** column for the filter criteria you want to delete.

2) Press **Enter**.

**Step 7: Define Run-time Collector Defaults**

Use this task to customize the defaults for the data source collection. This enables you to maximize how efficiently the report runs. Report defaults provide options specific to the data source collector on which the report is based, so you can filter the actual data source before the report filter is even applied.

An example of when report defaults are very useful is in the case of reports based on QAUDJRN journal data or database file journal data, where very large amounts of data can potentially accumulate and take a long time to process in a typical reporting scheme. With report defaults, you can specify particular date ranges so that any report filters are only run across a subset of data instead of the entire range of available data.

Report defaults are processed before any report run-time options, except when a user selects **YES** in the **Override report defaults** field at the time they run a report.

(See **Run TGSecure Reports** for additional information about the **Override report defaults** field.)

![Tip: Collector defaults are highly recommended, but they are not required. Click the **F2** function key to skip this step.](image)

**To define report defaults**

1) Enter the desired run-time collector default values.

2) Press **Enter**.
Step 8: Confirm Report Creation

Use this task to confirm that you want to create the report that you have just defined.

Tip: Click the F12 function key to go back one step at a time if you want to make changes or verify that you entered the correct information.

To confirm report creation

1) Review the information.

2) Press Enter.

See also

Working with TGSecure Reports
Manage TGSecure Reports

Use this task to do the following:

- Access the Work with Reports Interface
- Edit Report
- Copy Report
- Delete Report
- Enabling Report Alerting

**Note:** To manage reports, access the Work with Reports interface.

### Access the Work with Reports Interface

To access the Work with Reports interface

1) Access the Main menu.
2) At the Selection or command prompt, enter 30 (Work with Reports).
3) Press Enter. The Work with Reports Interface is displayed.

Alternatively, at the IBM i command line, enter TGWRKRPT, and press Enter.

### Edit Report

Use this task to edit a custom report.

**Tip:** You cannot edit built-in reports, but you can create a copy of a built-in report and then edit the copy.

**Important:** The Report ID cannot be edited after the report is created.

### To edit a report

1) Access the Work with Reports interface.
2) Enter the appropriate option in the Opt column for the report you want to modify:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (Edit)</td>
<td>Modify the report name, category, and regulation details</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Only available for custom reports, not built-in reports (those shipped with the product)</td>
</tr>
<tr>
<td>5 (Alerts)</td>
<td>Modify the condition (number of rows returned) that trigger the generation of an alert</td>
</tr>
<tr>
<td>6 (Defaults)</td>
<td>Modify the run-time collector defaults, which help to filter collector data</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See Create Reports for additional information about run-time collector defaults.</td>
</tr>
</tbody>
</table>
Copy Report

Use this task to copy a report. This is useful when an existing report provides results that are close to what you need, but still do not quite meet your requirements. You can save time by copying the report and customizing it instead of beginning from scratch.

To copy a report

1) Access the Work with Reports interface.
2) In the Opt column for the report you want to copy, enter 3 (Copy).
3) Enter a unique Report ID and continue customization as desired. Please refer to "Creating Reports" for details.

Delete Report

Use this task to delete a report.

Tip: You can delete only customer reports, not built-in reports.

To delete a report

1) Access the Work with Reports interface.
2) In the Opt column for the report you want to delete, enter 4 (Delete).

Enabling Report Alerting

Use this task to enable alerting based on the results (number of rows) produced in a given report. This is useful if you want the system to send a notification when the number of rows in a report exceeds a threshold.

Tip: You can set up alerts for both built-in and custom reports.

To enable report alerting

1) Access the Work with Reports interface.
2) In the Opt column for the desired report, enter 5 (Alerts).
3) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Status</td>
<td>Enter *YES to enable alerts for this specific report (local setting)</td>
</tr>
<tr>
<td>Alert Criteria (Condition)</td>
<td>Enter the desired mathematical symbol (&lt;, &gt;, =, etc.)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Alert Criteria (No. of Rows)</td>
<td>Enter the number of rows used in conjunction with a mathematical symbol to determine the threshold used to trigger an alert (e.g., if the number of rows is &gt; 10, then trigger an alert). <strong>Note:</strong> See Set Up Alert Defaults for instructions on defining the action taken when a report triggers an alert.</td>
</tr>
</tbody>
</table>

**See also**

*Working with TGSecure Reports*
Groups

This section describes how to work with Groups. There are several types of groups that you can create.

This section includes the following topics:

- Working with Groups
- User Groups
- Network Groups
- Operation Groups
- Object Groups

See also

Getting Started
Working with Groups

This section includes the following topics:

- Working with User Groups
- Working with Network/Server Groups
- Working with Object Groups
- Working with Operation Groups

**Note**: To work with groups, access the **Work with Groups** interface.

**To access the Work with Groups interface**

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Groups).

3) Press **Enter**. The **Work with Groups** interface is displayed.

**See also**

Groups
User Groups

This section describes how to work with Users and User Groups.

This section includes the following topics:

- Working with User Groups
- Display List of User Groups
- Display List of Users in a Group
- Manage User Groups
- Manage Users in a Group
- Run User Groups Report

See also

Groups
Working with User Groups

1. Access the **Main** menu.

2. Do one of the following:

   - **TGAudit**
     - At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).
     - Press **Enter**.
     - At the **Selection or command prompt**, enter the **11** (Work with User Groups).

   - **TGDetect**
     - At the **Selection or command** prompt, enter **10** (Work with User Groups).

   - **TGEncrypt**
     - At the **Selection or command** prompt, enter **4** (Work with Groups).
     - Press **Enter**.
     - At the **Selection or command prompt**, enter the **1** (Work with User Groups).

   - **TGSecure**
     - At the **Selection or command** prompt, enter **31** (Work with Groups).
     - Press **Enter**.
     - At the **Selection or command prompt**, enter the **1** (Work with User Groups).

See also

**User Groups**
Display List of User Groups

Use this task to do the following with user groups:

- Display Lists of User Groups
- Sort List
- Move to Position in List
- Filter List

**Note:** To work with user groups, you must access the **Work with User Groups** interface.

Display Lists of User Groups

Use this task to display the list of user groups.

**To display the list of user groups**

1) Access the **Main** menu.

2) Do one of the following:

**Note:** Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGAudit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. At the <strong>Selection or command</strong> prompt, enter the 3 (Job Activity Monitor).</td>
</tr>
<tr>
<td></td>
<td>2. Press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. At the <strong>Selection or command prompt</strong>, enter the 11 (Work with User Groups).</td>
</tr>
<tr>
<td>TGDetect</td>
<td>At the <strong>Selection or command</strong> prompt, enter 10 (Work with User Groups).</td>
</tr>
<tr>
<td>TGEncrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. At the <strong>Selection or command</strong> prompt, enter 4 (Work with Groups).</td>
</tr>
<tr>
<td></td>
<td>2. Press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. At the <strong>Selection or command prompt</strong>, enter the 1 (Work with User Groups).</td>
</tr>
<tr>
<td>TGSecure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. At the <strong>Selection or command</strong> prompt, enter 31 (Work with Groups).</td>
</tr>
<tr>
<td></td>
<td>2. Press <strong>Enter</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. At the <strong>Selection or command prompt</strong>, enter the 1 (Work with User Groups).</td>
</tr>
</tbody>
</table>

Sort List
Use this task to sort the list of available networks. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

**To sort the list**

1) Access the **Work with User Groups** interface.

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

   **Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

**Move to Position in List**

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

**To move to a specific position within the list**

1) Access the **Work with User Groups** interface.

2) Sort the list based on the desired column heading.

3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**.

   **Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**Filter List**

Use this task to limit the user groups displayed in the list by defining a subset for filtering purposes.

   **Tip:** Use wildcard asterisk to help define your subset.
   
   – Add an asterisk before text (e.g., *report) to find list items that end with specific text.
   – Add an asterisk after text (e.g., report*) to find list items that start with specific text.
   – Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with User Groups** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.
4) Press Enter. The system filters the results based on the criteria you defined for the subset.

See also

Working with User Groups
Display List of Users in a Group

Use this task to do the following with user groups:

- Display Lists of User Groups
- Sort List
- Move to Position in List

**Note:** To work with user groups, you must access the Work with User Groups interface.

Display Lists of User Groups

Use this task to display the list of user groups.

**To display the list of user groups**

1) Access the Main menu.
2) Do one of the following:

**Note:** Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit   | 1. At the Selection or command prompt, enter the 3 (Job Activity Monitor).  
            2. Press Enter.  
            3. At the Selection or command prompt, enter the 11 (Work with User Groups).                                                   |
| TGDetect  | At the Selection or command prompt, enter 10 (Work with User Groups).                                                             |
| TGEncrypt | 1. At the Selection or command prompt, enter 4 (Work with Groups).  
            2. Press Enter.  
            3. At the Selection or command prompt, enter the 1 (Work with User Groups).                                                   |
| TGSecure  | 1. At the Selection or command prompt, enter 31 (Work with Groups).  
            2. Press Enter.  
            3. At the Selection or command prompt, enter the 1 (Work with User Groups).                                                   |

Sort List

Use this task to sort the list of available users.
To sort the list

1) Access the **Work with Users** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

![Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.]

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Users** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

![Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.]

See also

*Working with User Groups*
Manage User Groups

Use this task to do the following with user groups:

- Access the Work with User Group Interface
- Add User Group
- Edit User Group
- Copy User Group
- Delete User Group

**Note:** To manage user groups, access the **Work with User Groups** interface.

Access the Work with User Group Interface

**To access the Work with User Groups interface**

1) Access the **Main** menu.

2) Do one of the following:

**Note:** Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit | 1. At the **Selection or command** prompt, enter the 3 (Job Activity Monitor).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 11 (Work with User Groups). |
| TGDetect | At the **Selection or command** prompt, enter 10 (Work with User Groups). |
| TGEncrypt | 1. At the **Selection or command** prompt, enter 4 (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |
| TGSecure | 1. At the **Selection or command** prompt, enter 31 (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |

Add User Group

Use this task to add a user group.
To add user group

1) Access the **Work with User Groups** interface.
2) Press the F6 (Add) function key.
3) Enter the name (ID) you want to assign to the group.

   **Tip:** Group names must begin with a colon and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

**Edit User Group**

Use this task to edit a user group.

**To edit user group**

1) Access the **Work with User Groups** interface.
2) In the OPT column for the desired group, enter 2 (Edit).
3) Press **Enter**.
4) Modify the description as necessary.

   **Note:** You cannot edit the name.

5) Press **Enter** twice.

**Copy User Group**

Use this task to copy a user group.

**To copy user group**

1) Access the **Work with User Groups** interface.
2) In the OPT column for the desired group, enter 3 (Copy).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

**Delete User Group**

Use this task to delete a user group

**To delete user group**

1) Access the **Work with User Groups** interface.
2) In the OPT column for the desired group, enter 4 (Delete).

3) Press Enter.

4) Review the record to ensure you are deleting the correct group.

5) Press Enter twice.

See also

Working with User Groups
Manage Users in a Group

Use this task to do the following with user groups:

- Access the Work with User Group Interface
- Edit a User
- Delete a User

**Note:** To manage users, access the Work with Users interface.

Access the Work with User Group Interface

To access the Work with User Groups interface

1) Access the Main menu.
2) Do one of the following:

**Note:** Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit  | 1. At the **Selection or command** prompt, enter the 3 (Job Activity Monitor).  
        2. Press **Enter**.  
        3. At the **Selection or command prompt**, enter the 11 (Work with User Groups). |
| TGDetect | At the **Selection or command** prompt, enter 10 (Work with User Groups). |
| TGEncrypt| 1. At the **Selection or command** prompt, enter 4 (Work with Groups).  
        2. Press **Enter**.  
        3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |
| TGSecure| 1. At the **Selection or command** prompt, enter 31 (Work with Groups).  
        2. Press **Enter**.  
        3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |

Add a User

Use this task to add a user.

To add user
1) Access the **Work with Users** interface.

2) Press the **F6** (Add) function key.

3) Enter the name (ID) you want to assign to the user.

   ![Tip: Names cannot contain spaces.](image)

4) Enter a description for the user.

5) Press **Enter** twice.

   ![Note: If the user already exists, you will see *YES in the Exists on Server field the first time you press Enter. If the user does not exist, you will see *No in the Exists on Server field the first time you press Enter.](image)

### Edit a User

Use this task to edit a user.

   ![Note: You can only edit the user description, not the user name.](image)

#### To edit user

1) Access the **Work with Users** interface.

2) In the **OPT** column for the desired user, enter **2** (Edit).

3) Press **Enter**.

4) Modify the user description as necessary.

   ![Note: You cannot edit the user name.](image)

5) Press **Enter** twice.

### Delete a User

Use this task to delete a user.

#### To delete user

1) Access the **Work with Users** interface.

2) In the **OPT** column for the desired user, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct user.

5) Press **Enter** twice.
See also

Working with User Groups
Run User Groups Report

Use this task to generate reports that display the following for user groups.

- Run User Group Configuration Report
- Run User Group Configuration Changes Report

Run User Group Configuration Report

Use this task to display user group configuration details.

To run User Group Configuration Report

1) Access the Main menu.
2) At the Selection or command prompt, enter 1 (Network Security).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (Network Reports).
5) Press Enter.
6) At the Selection or command prompt, enter 3 (Configuration Reports).
7) Press Enter.
8) At the Selection or command prompt, enter 4 (User Groups Report).
9) Press Enter.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

11) Enter the desired output format in the Report output type field.
12) Press Enter. The status of the report is displayed at the bottom of the screen.

Run User Group Configuration Changes Report

Use this task to display the list of configuration changes made to user groups.

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run User Group Configuration Changes Report

1) Access the Main menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **20** (Network Reports).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **4** (Configuration Changes).

7) Press **Enter**.

8) At the **Selection or command** prompt, enter **4** (User Groups Changes Report).

9) Press **Enter**.

10) Modify the run criteria as necessary.

   **Note:** The criteria allow you to limit the data returned in the report when you generate it.

   **Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.

12) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

*Working with User Groups*
Network Groups

This section describes how to work with Networks and Network Groups.

This section includes the following topics:

- Working with Network/Server Groups
- Display List of Network/Server Groups
- Display List of Networks in a Group
- Manage Network/Server Groups
- Manage Networks in a Group
- Run Network Groups Report

See also

Groups
Working with Network/Server Groups

**Note:** To work with network groups, you must access the *Work with Network/Server Groups* interface.

To access the *Work with Network/Server Groups* interface

1) Access the **Main** menu.

2) Do one of the following:

**Note:** Network/server groups are a common feature in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGEncrypt</td>
<td>At the <strong>Selection or command</strong> prompt, enter 4 (Work with Groups).</td>
</tr>
<tr>
<td>TGSecure</td>
<td>At the <strong>Selection or command</strong> prompt, enter 31 (Work with Groups).</td>
</tr>
</tbody>
</table>

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 2 (Work with Network/Server Groups).

5) Press **Enter**. The **Work with Network Groups** Interface is displayed.

**See also**

- Network/Server Groups
Display List of Network/Server Groups

Use this task to do the following with network groups:

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of network groups.

To display the list of network groups

1) Access the Main menu.
2) Do one of the following:

   ![Note: Network/server groups are a common feature in multiple TG products.]

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGEEncrypt</td>
<td>At the Selection or command prompt, enter 4 (Work with Groups).</td>
</tr>
<tr>
<td>TGSecure</td>
<td>At the Selection or command prompt, enter 31 (Work with Groups).</td>
</tr>
</tbody>
</table>

3) Press Enter.

4) At the Selection or command prompt, enter 2 (Work with Network/Server Groups).

5) Press Enter. The Work with Network Groups Interface is displayed.

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Group Name column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Network Groups interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

   ![Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.]

Move to Position in List
Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

**To move to a specific position within the list**

1) Access the **Work with Network Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**Filter List**

Use this task to limit the network groups displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Network Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

*Working with Network/Server Groups*
Display List of Networks in a Group

Use this task to do the following with network groups:

- Display List
- Sort List
- Move to Position in List

Display List

Use this task to display the list of networks assigned to a network group.

To display the list of networks assigned to a group

1) Access the Main menu.
2) Do one of the following:

   - Product Step
     - TGEncrypt At the Selection or command prompt, enter 4 (Work with Groups).
     - TGSecure At the Selection or command prompt, enter 31 (Work with Groups).
3) Press Enter.
4) At the Selection or command prompt, enter 2 (Work with Network/Server Groups).
5) Press Enter. The Work with Network Groups Interface is displayed.

Sort List

Use this task to sort the list of available networks.

To sort the list

1) Access the Work with Networks interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

- Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.
To move to a specific position within the list

1) Access the **Work with Networks** interface.

2) Sort the list based on the desired column heading.

3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**See also**

*Working with Network/Server Groups*
Manage Network/Server Groups

Use this task to do the following with network groups:

- Access the Work with Network Groups Interface
- Add Network Group
- Edit Network Group
- Copy Network Group
- Delete Network Group

**Note:** To manage network groups, access the Work with Network Groups interface.

Access the Work with Network Groups Interface

**To access the Work with Network Groups interface**

1) Access the Main menu.
2) Do one of the following:

**Note:** Network/server groups are a common feature in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGEencrypt</td>
<td>At the <strong>Selection or command</strong> prompt, enter 4 (Work with Groups).</td>
</tr>
<tr>
<td>TGSecure</td>
<td>At the <strong>Selection or command</strong> prompt, enter 31 (Work with Groups).</td>
</tr>
</tbody>
</table>

3) Press Enter.
4) At the **Selection or command** prompt, enter 2 (Work with Network/Server Groups).
5) Press Enter. The Work with Network Groups Interface is displayed.

Add Network Group

Use this task to add a network group.

**To add network group**

1) Access the Work with Network Groups interface.
2) Press the F6 (Add) function key.
3) Enter the name (ID) you want to assign the network group.

**Tip:** Group names must begin with a colon and cannot contain spaces.

4) Enter a description for the network group.
5) Press Enter twice.

**Edit Network Group**

Use this task to edit a network group.

**To edit network group**

1) Access the **Work with Network Groups** interface.
2) In the **OPT** column for the desired group, enter 2 (Edit).
3) Press Enter.
4) Modify the description as necessary.
5) Press Enter twice.

**Copy Network Group**

Use this task to copy a network group. This is a fast way to create a new group based on an existing group.

**To copy network group**

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter 3 (Copy).
3) Press Enter.
4) Enter the name (ID) you want to assign the group.

**Tip:** Group names must begin with a colon and cannot contain spaces.

5) Enter a description for the group.
6) Press Enter.

**Delete Network Group**

Use this task to delete a network group

**To delete network group**

1) Access the **Work with Network Group** interface.
2) In the **OPT** column for the desired group, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct group.
5) Press Enter twice.
See also

Working with Network/Server Groups
Manage Networks in a Group

Use this task to do the following with network groups:

- Access the Work with Networks Interface
- Add Network
- Edit Network
- Delete Network

**Note:** To manage networks, access the **Work with Networks** interface.

Access the Work with Networks Interface

**To access the Work with Networks interface**

1. Access the **Main** menu.
2. Do one of the following:

   **Note:** Network/server groups are a common feature in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGEncrypt</td>
<td>At the <strong>Selection or command</strong> prompt, enter 4 (Work with Groups).</td>
</tr>
<tr>
<td>TGSecure</td>
<td>At the <strong>Selection or command</strong> prompt, enter 31 (Work with Groups).</td>
</tr>
</tbody>
</table>

3. Press **Enter**.
4. At the **Selection or command** prompt, enter 2 (Work with Network/Server Groups).
5. Press **Enter**.
6. In the **OPT** column, enter 10 (Work with Networks).
7. Press **Enter**. The **Work with Networks** interface is displayed.

Add Network

Use this task to add a network.

**To add network**

1. Access the **Work with Networks** interface.
2. Press the **F6** (Add) function key.
3. Enter the name (ID) you want to assign to the network.

**Tip:** Names cannot contain spaces.
4) Enter a description for the network.
5) Press Enter twice.

**Edit Network**

Use this task to edit a network.

**To edit network**

1) Access the **Work with Networks** interface.
2) In the OPT column for the desired network, enter 2 (Edit).
3) Press Enter.
4) Modify the network parameters as necessary.

<i>Note: You cannot edit the network name.</i>

5) Press Enter twice.

**Delete Network**

Use this task to delete a network.

**To delete network**

1) Access the **Work with Networks** interface.
2) In the OPT column for the desired network, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct network.
5) Press Enter twice.

**See also**

*Working with Network/Server Groups*
**Run Network Groups Report**

Use this task to run a report that displays the list of network groups.

- **Access the Network Reports Interface**
- **Run Network Group Configuration Report**
- **Run Network Group Configuration Changes Report**

**Note:** Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with Network Group reports, access the **Network Reports** interface.

**Access the Network Reports Interface**

**To access the Network Reports interface**

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter 1 (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter 20 (Network Reports).
5) Press **Enter**. The **Network Reports** interface is displayed.

**Run Network Group Configuration Report**

Use this task to display user group configuration details.

**To run the Network Group Configuration Report**

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter 3 (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter 5 (Network Groups Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report when you generate it.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Network Group Configuration Changes Report**

Use this task to display the list of configuration changes made to network groups.

- **Tip**: You must enable auditing to produce change reports. See [Enable Access Escalation Change Auditing](#) for additional information.

**To run the Network Group Configuration Changes Report**

1) Access the Network Reports interface.

2) At the **Selection or command** prompt, enter 4 (Configuration Changes).

3) Press Enter.

4) At the **Selection or command** prompt, enter 5 (Network Groups Changes Report).

5) Press Enter.

6) Modify the run criteria as necessary.

- **Note**: The criteria allow you to limit the data returned in the report when you generate it.

- **Tip**: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press Enter. The status of the report is displayed at the bottom of the screen.

**See also**

[Working with Network/Server Groups](#)
Operation Groups

This section describes how to work with Operations and Operation Groups.

This section includes the following topics:

- Working with Operation Groups
- Display List of Operation Groups
- Display List of Operations in a Group
- Manage Operation Groups
- Manage Operations in a Group
- Run Operation Groups Report

See also

Groups
Working with Operation Groups

Use the Operation Groups feature to do the following:

- Display List of Operation Groups
- Display List of Operations in a Group
- Manage Operation Groups
- Manage Operations in a Group
- Run Operation Groups Report

Note: To work with operations, you must access the Work with Operation Groups interface.

To access the Work with Operation Groups interface

1) Access the Main menu.

2) At the Selection or command prompt, enter 31 (Work with Groups).

3) Press Enter.

4) At the Selection or command prompt, enter 3 (Work with Operation Groups).


See also

Operation Groups
Display List of Operation Groups

Use this task to do the following with operation groups:

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of operation groups.

To display the list of operation groups

1) Access the Main menu.
2) At the Selection or command prompt, enter 31 (Work with Groups).
3) Press Enter.
4) At the Selection or command prompt, enter 3 (Work with Operation Groups).

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Group Name column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Operation Groups interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Operation Groups interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**Filter List**

Use this task to limit the operation groups displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

---

**To filter the list using a subset**

1) Access the **Work with Operation Groups** interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter. The system filters the results based on the criteria you defined for the subset.

**See also**

*Working with Operation Groups*
Display List of Operations in a Group

Use this task to do the following with operation groups:

- Display List
- Sort List
- Move to Position in List

Display List

Use this task to display the list of operations assigned to an operations group.

To display the list of operations assigned to a group

1) Access the Main menu.

2) At the Selection or command prompt, enter 31 (Work with Groups).

3) Press Enter.

4) At the Selection or command prompt, enter 3 (Work with Operation Groups).

5) Press Enter.

6) In the OPT column, enter 10 (Work with Operations).

7) Press Enter. The Work with Operations interface is displayed.

Sort List

Use this task to sort the list of available operations.

To sort the list

1) Access the Work with Operations interface.

2) Place your cursor on the desired column heading.

3) Press the F10 (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Operations interface.

2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**See also**

*Working with Operation Groups*
Manage Operation Groups

Use this task to do the following with operation groups:

- Add Operation Group
- Edit Operation Group
- Copy Operation Group
- Delete Operation Group

Note: To manage operation groups, access the Work with Operation Groups interface.

To access the Work with Operation Groups interface

1) Access the Main menu.
2) At the Selection or command prompt, enter 1 (Network Security).
3) Press Enter.
4) At the Selection or command prompt, enter 4 (Work with Groups).
5) Press Enter.
6) At the Selection or command prompt, enter 3 (Work with Operation Groups).
7) Press Enter. The Work with Operation Groups interface is displayed.

Add Operation Group

Use this task to add an operation group.

To add an operation group

1) Access the Work with Operation Groups interface.
2) Press the F6 (Add) function key.
3) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon and cannot contain spaces.

4) Enter a description for the group.
5) Press Enter twice.

Edit Operation Group

Use this task to edit an operation group.

To edit operation group
1) Access the **Work with Operation Groups** interface.

2) In the **OPT** column for the desired group, enter **2 (Edit)**.

3) Press **Enter**.

4) Modify the description as necessary.

5) Press **Enter** twice.

**Copy Operation Group**

Use this task to copy an operation group. This is a fast way to create a new group based on an existing group.

**To copy network group**

1) Access the **Work with Operation Groups** interface.

2) In the **OPT** column for the desired group, enter **3 (Copy)**.

3) Press **Enter**.

4) Enter the name (ID) you want to assign the group.

[Tip: Group names must begin with a colon and cannot contain spaces.]

5) Enter a description for the group.

6) Press **Enter**.

**Delete Operation Group**

Use this task to delete an operation group.

**To delete operation group**

1) Access the **Work with Operation Groups** interface.

2) In the **OPT** column for the desired group, enter **4 (Delete)**.

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct group.

5) Press **Enter** twice.

**See also**

*Working with Operation Groups*
Manage Operations in a Group

Use this task to do the following with operation groups:

- Add Operation
- Edit Operation
- Delete Operation

**Note:** To manage operations, access the **Work with Operations** interface.

**To access the Work with Operations interface**

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter 31 (Work with Groups).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 3 (Work with Operation Groups).

5) Press **Enter**.

6) In the OPT column, enter 10 (Work with Operations).

7) Press **Enter**. The **Work with Operations** interface is displayed.

**Add Operation**

Use this task to add an operation.

**To add operation**

1) Access the **Work with Operations** interface.

2) Press the F6 (Add) function key.

3) Enter the name (ID) you want to assign to the operation.

**Tip:** Names cannot contain spaces.

4) Enter a description for the operation.

5) Press **Enter** twice.

**Edit Operation**

Use this task to edit an operation.

**To edit operation**

1) Access the **Work with Operations** interface.
2) In the **OPT** column for the desired operation, enter **2** (Edit).

3) Press **Enter**.

4) Modify the operation parameters as necessary.

![Note: You cannot edit the name.]

5) Press **Enter** twice.

**Delete Operation**

Use this task to delete an operation.

**To delete an operation**

1) Access the **Work with Operations** interface.

2) In the **OPT** column for the desired operation, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct operation.

5) Press **Enter** twice.

**See also**

*Working with Operation Groups*
Run Operation Groups Report

Use this task to run a report that displays the list of operation groups.

- Access the Network Reports Interface
- Run Operation Groups Configuration Report
- Run Operation Group Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Network Group reports, access the Network Reports interface.

Access the Network Reports Interface

To access the Network Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 1 (Network Security).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (Network Reports).
5) Press Enter. The Network Reports interface is displayed.

Run Operation Groups Configuration Report

Use this task to display operation group configuration details.

To run the Operation Group Configuration Report

1) Access the Network Reports interface.
2) At the Selection or command prompt, enter 3 (Configuration Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 6 (Operation Groups Report).
5) Press Enter.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Operation Group Configuration Changes Report**

Use this task to display the list of configuration changes made to operation groups.

> **Tip:** You must enable auditing to produce change reports. See [Enable Access Escalation Change Auditing](#) for additional information.

**To run the Operation Group Configuration Changes Report**

1) Access the **Network Reports** interface.

2) At the **Selection or command** prompt, enter **4** (Configuration Changes).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **6** (Operation Groups Changes Report).

5) Press **Enter**.

6) Modify the run criteria as necessary.

> **Note:** The criteria allow you to limit the data returned in the report when you generate it.

> **Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

*Working with Operation Groups*
Object Groups

This section describes how to work with Objects and Object Groups.

This section includes the following topics:

- Working with Object Groups
- Display List of Object Groups
- Display List of Object in a Group
- Manage Object Groups
- Manage Objects in a Group
- Run Object Groups Report

See also

Groups
Working with Object Groups

Use the **Object Groups** feature to do the following:

- Display List of Object Groups
- Display List of Object in a Group
- Manage Objects in a Group
- Manage Objects in a Group
- Run Object Groups Report

**Note**: To work with object groups, you must access the **Work with Object Groups** interface.

To access the **Work with Object Groups** interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Groups).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).

5) Press **Enter**. The **Work with Object Groups** interface is displayed.

See also

**Object Groups**
Display List of Object Groups

Use this task to do the following with object groups:

- Display List
- Sort List
- Move to a Position in the List

Display List

Use this task to display the list of object groups.

To display the list of object groups

1) Access the Main menu.
2) At the Selection or command prompt, enter 31 (Work with Groups).
3) Press Enter.
4) At the Selection or command prompt, enter 4 (Work with Object Groups).
5) Press Enter. The Work with Object Groups interface is displayed.

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Group Name column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Object Groups interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to a Position in the List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Object Groups interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**Filter List**

Use this task to limit the object groups displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Object Groups** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

**Working with Object Groups**
Display List of Object in a Group

Use this task to do the following with object groups:

- Display List
- Sort List
- Move to Position in List

Display List

Use this task to display the list of operations assigned to an operations group.

To display the list of operations assigned to a group

1) Access the Main menu.
2) At the Selection or command prompt, enter 31 (Work with Groups).
3) Press Enter.
4) At the Selection or command prompt, enter 4 (Work with Object Groups).
5) Press Enter.
6) In the OPT column, enter 10 (Work with Objects).
7) Press Enter. The Work with Objects interface is displayed.

Sort List

Use this task to sort the list of available objects.

To sort the list

1) Access the Work with Objects interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Objects interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**See also**

*Working with Object Groups*
Manage Object Groups

Use this task to do the following with object groups:

- Add Object Group
- Edit Object Group
- Copy Object Group
- Delete Object Group

*i Note: To manage object groups, access the Work with Object Groups interface.*

To access the Work with Object Groups interface

1) Access the Main menu.

2) At the Selection or command prompt, enter 31 (Work with Groups).

3) Press Enter.

4) At the Selection or command prompt, enter 4 (Work with Object Groups).

5) Press Enter. The Work with Object Groups interface is displayed.

Add Object Group

Use this task to add an object group.

*To add object group*

1) Access the Work with Object Groups interface.

2) Press the F6 (Add) function key.

3) Enter the name (ID) you want to assign the group.

*Tip: Group names must begin with a colon and cannot contain spaces.

4) Enter a description for the group.

5) Press Enter twice.

Edit Object Group

Use this task to edit an object group.

*To edit object group*

1) Access the Work with Object Groups interface.

2) In the OPT column for the desired group, enter 2 (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

**Copy Object Group**

Use this task to copy an object group. This is a fast way to create a new group based on an existing group.

**To copy object group**

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

![Tip: Group names must begin with a colon and cannot contain spaces.](image)

5) Enter a description for the group.
6) Press **Enter**.

**Delete Object Group**

Use this task to delete an object group

**To delete object group**

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

**See also**

[Working with Object Groups](#)
Manage Objects in a Group

Use this task to do the following with object groups:

- Access the Work with Objects Interface
- Add Object
- Edit Object
- Delete Object

Note: To manage objects, access the Work with Objects interface.

Access the Work with Objects Interface

To access the Work with Objects interface

1) Access the Main menu.
2) At the Selection or command prompt, enter 31 (Work with Groups).
3) Press Enter.
4) At the Selection or command prompt, enter 4 (Work with Object Groups).
5) Press Enter.
6) In the OPT column, enter 10 (Work with Objects).
7) Press Enter. The Work with Objects interface is displayed.

Add Object

Use this task to add an object.

To add operation

1) Access the Work with Objects interface.
2) Press the F6 (Add) function key.
3) Enter the name (ID) you want to assign to the object.

Tip: Names cannot contain spaces.

4) Enter a description for the object.
5) Press Enter twice.

Edit Object

Use this task to edit an object.
To edit object

1) Access the Work with Objects interface.

2) In the OPT column for the desired object, enter 2 (Edit).

3) Press Enter.

4) Modify the object parameters as necessary.

5) Press Enter twice.

Delete Object

Use this task to delete an object.

To delete an object

1) Access the Work with Objects interface.

2) In the OPT column for the desired object, enter 4 (Delete).

3) Press Enter.

4) Review the record to ensure you are deleting the correct object.

5) Press Enter twice.

See also

Working with Object Groups
Run Object Groups Report

Use this task to run a report that displays the list of object groups.

- Access the Network Reports Interface
- Run Object Group Configuration Report
- Run Object Group Configuration Changes Report

Tip: Refer to the TGSecure Report Reference for a complete list of report definitions.

Note: To work with Network Group reports, access the Network Reports interface.

Access the Network Reports Interface

To access the Network Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 1 (Network Security).
3) Press Enter.
4) At the Selection or command prompt, enter 20 (Network Reports).
5) Press Enter. The Network Reports interface is displayed.

Run Object Group Configuration Report

Use this task to display operation group configuration details.

To run the Object Group Configuration Report

1) Access the Network Reports interface.
2) At the Selection or command prompt, enter 3 (Configuration Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 7 (Object Groups Report).
5) Press Enter.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### Run Object Group Configuration Changes Report

Use this task to display the list of configuration changes made to object groups.

- **Tip**: You must enable auditing to produce change reports. See [Enable Access Escalation Change Auditing](#) for additional information.

### To run the Object Groups Configuration Changes Report

1) Access the **Network Reports** interface.

2) At the **Selection or command** prompt, enter **4** (Configuration Changes).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **7** (Object Groups Changes Report).

5) Press **Enter**.

6) Modify the run criteria as necessary.

- **Note**: The criteria allow you to limit the data returned in the report when you generate it.

- **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

### See also

- [Working with Object Groups](#)
Calendars

This section describes how to work with **Calendars**.

**Calendars** allow you to enable a rule or entitlement for a specific duration (e.g., after hours, during weekends, on a holiday, etc.).

This section includes the following topics:

- Working with Calendars
- Display List of Calendars
- Manage Calendars
- Manage Calendar Day/Time Access
Troubleshooting

This section provides resources to help you troubleshoot issues:

- TGSecure FAQ
- Error Messages
TGSecure FAQ

This section provides troubleshooting information you can use to resolve issues you might encounter.

Why does my report have no data?

If you generate a report and it contains no data, you need to ensure that auditing has been enabled (see Audit Configuration).
Error Messages

Go here: IBM Errors
Appendices

- APPENDIX - TGSecure Revisions
  - Version 2.5 - TGSecure User Guide Revisions
  - Version 2.4 - TGSecure User Guide Revisions
  - Version 2.3 - TGSecure User Guide Revisions
  - Version 2.2 - TGSecure User Guide Revisions
  - Version 2.1 - TGSecure User Guide Revisions

- APPENDIX - TGSecure Collectors

- APPENDIX - TG Fix

- APPENDIX - TG Management

- APPENDIX - TG Save and Restore

- APPENDIX - TG Job Scheduler

- APPENDIX - TG Journal Cleanup

- APPENDIX - TG Transaction Cleanup
APPENDIX - TGSecure Revisions

This section includes enhancement by version.

- Version 2.5 - TGSecure User Guide Revisions
- Version 2.4 - TGSecure User Guide Revisions
- Version 2.3 - TGSecure User Guide Revisions
- Version 2.2 - TGSecure User Guide Revisions
- Version 2.1 - TGSecure User Guide Revisions
Version 2.5 - TGSecure User Guide Revisions

This release includes the following:

Enhancements

System Value Management (SYS)
- Added support for numeric data

Command Security (CMD)
- Added granular parameter restriction per rule (CMD/Lib/User/IP)
- Added option to use function key F2 to add exits out of sync
Version 2.4 - TGSecure User Guide Revisions

This release includes the following:

**New Features**

**System Value Management**

The *System Value Management* feature is now available.

The following new *System Value Management* reports are now available:

- All System Values
- Security System Values
- System Value Changes
- System Value Configuration
- System Value Defaults
- System Value Valid Values
- System Value Configuration Changes
- System Value Default Changes
- System Value Valid Value Changes

The following new *collectors* are now available:

- SYS_VAL_CONFIG
- SYS_VAL_DEFAULT
- SYS_VAL_VALID

**Enhancements**

**User Profile Manager**

Addition of two new options to *archive inactive profiles*:

- *SAVSEC* - Save user profile data using SAVSECDTA command
- *SAVPRF* - Save user profile data to a database file

**Resource Manager**

Addition additional support for *authority schemas*:

- IFS Filter Support
- IFS Depth Support
Version 2.3 - TGSecure User Guide Revisions

This release includes the following:

**New Features**

- Network Security - Artificial Intelligence (AI) rules engine
- Resource Manager - Schemas filter feature

**Enhancements**

- Network Security – Database Parser granularity of rules extended to the `command` level
Version 2.2 - TGSecure User Guide Revisions

This release contains the following:

New Features

Command Security (CMD)

The Command Security feature is now available.

The following new Command Security reports are now available:

- Command Security Config Settings
- Command Security Parameter Level
- Command Security Rules
- Command Security Configuration Changes
- Command Security Command Rule Changes
- Command Security Command Parameter Level Changes
- Commands Allowed via Command Security
- Commands Rejected via Command Security

The following new collectors are now available:

- CMD_SEC_COMMANDS
- CMD_SEC_CONF_SETTINGS
- CMD_SEC_PARAM_LEVEL
- CMD_SEC_RULES

Enhancements

Network Security

- Added support for swap profiles in exit point transaction rule definitions

Job Scheduler

- Added Job Scheduler

User Profile Manager

- Added support of the Initial Menu (INLMENU) special value of *SIGNOFF
- Changed TGPRFCMP command to support generic users in TG user groups
- Changed TGPRFMGR command to support generic users in TG user group
- Changed TGPROFILE - PRF00010D/P to validate objects as per IBM standards
Version 2.1 - TGSecure User Guide Revisions

This release includes the following:

**Enhancements**

**Groups**

In the **Network Security Default** settings, you can now do the following:

- Enable group profile inheritance

**Exit Program**

The following exit program is now available for use:

- Showcase

**Note:** See Manage Exit Points for instruction on adding (installing) an exit program.

**Report**

The following report is now available:

- Network Transaction Showcase

**Note:** See the TGSecure Report Reference Guide for information about individual reports.
## APPENDIX - TGSecure Collectors

<table>
<thead>
<tr>
<th>Collector ID</th>
<th>Collector Name</th>
<th>Collector Category</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS_ESCAL_ACC_CONTROLS</td>
<td>Access Escalation Access Controls</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_DEFAULTS</td>
<td>Access Escalation Defaults</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_ENTITLEMENTS</td>
<td>Access Escalation Entitlements</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_FILE_EDITORS</td>
<td>Access Escalation File Editors</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCALATION_USAGE</td>
<td>Access Escalation Usage</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTH_USERS_VIA_AUTH_LISTS</td>
<td>Authorized Users through Authorization Lists</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COL_ALI</td>
<td>Authority Collection Report (*ALL)</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COL_IFS</td>
<td>Auth Collection For Objects IFS Report</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COL_OBJECT</td>
<td>Auth Collection For Objects Native Report</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COLLECTION</td>
<td>Authority Collection Data</td>
<td>Journal</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COMPLIANCE</td>
<td>Authority Compliance</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_LIST</td>
<td>Authority List Data</td>
<td>System</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_3RD_PARTY_FILE</td>
<td>Blueprint 3rd Party Integration File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_AUTH_SETTINGS_FILE</td>
<td>Blueprint Authority List Settings File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_MASTER</td>
<td>Blueprint Master</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_NON_COMPLIANCE_USER</td>
<td>Blueprint Non-Compliance User Profiles</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_OBJECT_AUTH_FILE</td>
<td>Blueprint Object Authority File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_PARAMETER_FILE</td>
<td>Blueprint Parameter File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_PERMISSION_FILE</td>
<td>Blueprint Permission File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_COMMANDS</td>
<td>Commands Allowed/Rejected via Command Security</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_CONF_SETTINGS</td>
<td>Command Security Config Settings</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_PARAM_LEVEL</td>
<td>Command Security Parameter Level</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_RULES</td>
<td>Command Security Config Settings</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CONTROLLER_ATTACHED_DEVICES</td>
<td>Command Security Parameter Level</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>CONTROLLER_DESCRIPTION_DATA</td>
<td>Controller Description Information</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------</td>
<td>---------</td>
<td>-----</td>
</tr>
<tr>
<td>DATA_AREA_AUDITING</td>
<td>Audit data area changes</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_ACCESS</td>
<td>Database File Access</td>
<td>N/A</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_AUDITING</td>
<td>Monitor Database changes</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_CONTENT</td>
<td>Database Content</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_FIELD_ACTIVITY</td>
<td>Database Field Activity</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_MONITORING</td>
<td>Database Monitoring</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_OPERATIONS</td>
<td>Database Operations</td>
<td>N/A</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_ACT_HISTORY</td>
<td>Detect Activity History</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_DEFAULTS</td>
<td>Detect Defaults</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_CMD_RULES</td>
<td>Command Monitor Rules</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_JRN_SEIM_RULES</td>
<td>Journal Monitor Rules for SEIM</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_JRNMON_ALERTS</td>
<td>Journal Monitor Alerts</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_JRNMON_RULES</td>
<td>Journal Monitor Rules</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_MON_MASTER</td>
<td>Monitor Master</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_MSQ_CMD_ALR</td>
<td>Message Queue and Command Alerts</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_MSQ_RULES</td>
<td>Message Queue Rules</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_SEIM_PROVIDERS</td>
<td>SEIM Providers</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET_SNMP_TRP_PKG</td>
<td>SNMP Trap Packages</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DEVICE_DESCRIPTION_APPC</td>
<td>Device Description APPC Information</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DEVICE_DESCRIPTION_DATA</td>
<td>Device Description Information</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE_OPERATIONS_JRN</td>
<td>Database Operations by Journal</td>
<td>N/A</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT_DATABASE_FIELD</td>
<td>Encryption Database Field Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT_DATABASE_FILE</td>
<td>Encryption Database File Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT_DATABASE_FILTER</td>
<td>Encryption Database File Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT_DATABASE_RULES</td>
<td>Encryption Database Rule Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPTION_DEFAULTS</td>
<td>Encryption Defaults</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>EXIT_POINTS</td>
<td>Display Exit Point Data</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>FIELD_AUTHORITY</td>
<td>Display Field Level Authorities</td>
<td>Object</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_ATTRIBUTES</td>
<td>Display the attributes for the IFS objects</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_AUTHORITIES</td>
<td>Display the public and private authorities associated with the object</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Type</td>
<td>Platform</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------</td>
</tr>
<tr>
<td>IFS_CONTENT</td>
<td>IFS Content</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_JOURNALING</td>
<td>Display extended journaling information for the IFS object</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_STATUS</td>
<td>Display status information about an IFS file</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>INACTIVITY_DISCONNECTS</td>
<td>Inactivity Disconnections</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>INCOMING_TRANSACTIONS</td>
<td>Incoming Transactions</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ISL_CONFIGURATION_SETTINGS</td>
<td>ISL Configuration Settings</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ISL_DISCONNECT_OPTIONS</td>
<td>ISL Disconnect Options</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ISL_RULES</td>
<td>ISL Inclusion Exclusion Rules</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_ACTIVITY_DETAILS</td>
<td>Job Activity Details</td>
<td>Log</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_ACTIVITY_SUMMARY</td>
<td>Job Activity Summary</td>
<td>Log</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_DATABASE_ACTIVITY</td>
<td>Job and Database Activity</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_DESCRIPTIONS</td>
<td>Job Description Data</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AD</td>
<td>Object Auditing Attribute Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AF</td>
<td>Authority Failures</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AP</td>
<td>Programs that Adopt Authority were Executed</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AU</td>
<td>EIM Attribute Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AX</td>
<td>Row and Column Access Control</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CA</td>
<td>Authorization List or Object Authority Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CD</td>
<td>Commands Executed</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CO</td>
<td>Create Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CP</td>
<td>User Profile Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CQ</td>
<td>Change Request Descriptor Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CU</td>
<td>Cluster Operation</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL.CV</td>
<td>Connection Verification</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CY</td>
<td>Cryptographic Configuration Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_DI</td>
<td>LDAP Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_DO</td>
<td>Delete Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_DS</td>
<td>Changes to Service Tools Profiles</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_EV</td>
<td>Environment Variable Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_GR</td>
<td>Exit Point Maintenance Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_GS</td>
<td>Socket Descriptor Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IM</td>
<td>Intrusion Monitor Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------</td>
<td>---------</td>
<td>-----</td>
</tr>
<tr>
<td>JOURNAL_IP</td>
<td>Inter-process Communication Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IR</td>
<td>Actions to IP Rules</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IS</td>
<td>Internet Security Management Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_JD</td>
<td>Job Descriptions – USER Parameter Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_JS</td>
<td>Job Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_KF</td>
<td>Key Ring File Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_LD</td>
<td>Directory Link, Unlink, and Search Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M0</td>
<td>Db2 Mirror Setup Tools</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M6</td>
<td>Db2 Mirror Communication Services</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M7</td>
<td>Db2 Mirror Replication Services</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M8</td>
<td>Db2 Mirror Product Services</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M9</td>
<td>Db2 Mirror Replication State</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ML</td>
<td>OfficeVision Mail Services Actions</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_NA</td>
<td>Network Attribute Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ND</td>
<td>Directory Search Violations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_NE</td>
<td>APPN Endpoint Filter Violations</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_O1</td>
<td>Single Optical Object Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_O2</td>
<td>Dual Optical Object Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_O3</td>
<td>Optical Volume Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_OM</td>
<td>Object Management Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_OR</td>
<td>Objects Restored</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_OW</td>
<td>Object Ownership Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PA</td>
<td>Program Changes to Adopt Owner Authority</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PF</td>
<td>PTF Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PG</td>
<td>Primary Group Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PO</td>
<td>Printer Output Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PS</td>
<td>Swap Profile Events</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL PU</td>
<td>PTF Object Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PW</td>
<td>Invalid Sign-on Attempts</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RA</td>
<td>Authority Changes to Restored Objects</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RJ</td>
<td>Job Descriptions that Contain User Profile Names were Restored</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RO</td>
<td>Ownership Changes for Restored Objects</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>JOURNAL_RP</td>
<td>Programs Restored that Adopt Owner Authority</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RQ</td>
<td>Change Request Descriptors Restored</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RU</td>
<td>Authority Restored for User Profiles</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RZ</td>
<td>Primary Group Changes for Restored Objects</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SD</td>
<td>System Directory Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SE</td>
<td>Subsystem Routing Entry Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SF</td>
<td>Spooled File Actions</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SG</td>
<td>Asynchronous Signals Processed</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL(SK)</td>
<td>Secure Socket Connections</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SM</td>
<td>Systems Management Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SO</td>
<td>Server Security User Information Actions</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ST</td>
<td>Service Tools Actions</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SV</td>
<td>System Values Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VA</td>
<td>Access Control List Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VC</td>
<td>Connections Started, Ended, or Rejected</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VF</td>
<td>Close Operations on Server Files</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VL</td>
<td>Exceeded Account Limit Events</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VN</td>
<td>Network Log On and Off Events</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VO</td>
<td>Actions on Validation Lists</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VP</td>
<td>Network Password Errors</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VR</td>
<td>Network Resource Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VS</td>
<td>Server Sessions Started or Ended</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VU</td>
<td>Network Profile Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VV</td>
<td>Service Status Change Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_X0</td>
<td>Network Authentication Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_X1</td>
<td>Identity Token Events</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_XD</td>
<td>Directory Server Extensions</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_YC</td>
<td>DLO Object Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_YR</td>
<td>DLO Object Reads</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ZC</td>
<td>Object Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ZR</td>
<td>Object Reads</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Description</td>
<td>Platform</td>
<td>Provider</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>KEYSTORE_DATA</td>
<td>KeyStore Configuration</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>LIBRARY_STAT</td>
<td>Library Statistics</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>LINE_DESCRIPTION_DATA</td>
<td>Line Description Information</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>MESSAGE_QUEUE</td>
<td>Message Queue Details</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>MESSAGE_QUEUE_DATA</td>
<td>Message Queue Data</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETSERVER_CONFIG</td>
<td>NetServer Configuration</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETSERVER_SHARES</td>
<td>NetServer Shares</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_ATTRIBUTES</td>
<td>Network Attribute Information</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_CONNECTIONS</td>
<td>Network Connections Ipv4 and Ipv6</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_EXIT_CONFIG</td>
<td>Exit Point Configuration Report</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_INTERFACE_IPV4</td>
<td>Network Interface Data Ipv4</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_INTERFACE_IPV6</td>
<td>Network Interface Data Ipv6</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_ROUTE_IPV4</td>
<td>Network Route Data Ipv4</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_ROUTE_IPV6</td>
<td>Network Route Data Ipv6</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_SERVER_DESCRIPTIONS</td>
<td>Network Server Description Data</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_SVR_ENCRYPT_STATUS</td>
<td>Network Server Encryption Status</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TCP_IPV4</td>
<td>TCP/IP Ipv4 Stack Attributes/Remote Exit Rule</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TCP_IPV6</td>
<td>TCP/IP Ipv6 Stack Attributes/Remote Exit Rule</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_CENTRAL</td>
<td>Central Server Transactions</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_COMMAND</td>
<td>Remote Command Transactions</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_DATABASE</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_DATAQ</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_DDM</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_FILE</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_FTP_REX_EC</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_PRINTER</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_SHOWCASE</td>
<td>Network Trans Showcase</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_SIGNON</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>NETWORK_TRANS_TELNET</td>
<td>Remote Exit Rules</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>OBJECT_AUTHORITY</td>
<td>Display Object Authority</td>
<td></td>
<td>IBMi</td>
</tr>
<tr>
<td>Resource</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT_DETAILS</td>
<td>Display Object Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT_STAT</td>
<td>Object/File Statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUTPUT_QUEUE</td>
<td>Output Queue Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRODUCT_INFO</td>
<td>Basic Information about a software product</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROFILE_COMPLIANCE</td>
<td>Profile Compliance Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROFILE_INACTIVITY_SETTINGS</td>
<td>Profile Inactivity Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROFILE_MANAGER_DEFAULTS</td>
<td>Profile Manager Defaults</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROGRAM_ADOPT</td>
<td>Programs that Adopt Authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROGRAM_REFERENCE_DATA</td>
<td>Program Reference Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTF_DATA</td>
<td>Program Temporary Fix Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QHST_MSG_INFO</td>
<td>QHST History Log Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.ACTIVE_JOB_INFO</td>
<td>Active job information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.DATA_QUEUE_ENTRIES</td>
<td>Data Queue Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.DRDA_AUTHENTICATION</td>
<td>DRDA and DDM User access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.EXIT_POINT_INFO</td>
<td>Exit Point Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.EXIT_PROGRAM_INFO</td>
<td>Exit Program Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.FUNCTION_INFO</td>
<td>Function usage identifiers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.FUNCTION_USAGE</td>
<td>Function usage configuration details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.GROUP_PTF_INFO</td>
<td>Group PTFs Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.JOURNAL_INFO</td>
<td>Journal and remote journal information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.JOURNALIZED_OBJECTS</td>
<td>Journal object information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.LICENSE_INFO</td>
<td>Products license information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.MEDIA_LIBRARY_INFO</td>
<td>Media Library Status details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.MEMORY_POOL</td>
<td>Memory pool details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.MEMORY_POOL_INFO</td>
<td>Active memory pools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.MESSAGE_QUEUE_INFO</td>
<td>Message Queue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QSYS2.NETSTAT_JOB_INFO</td>
<td>IPv4 and IPv6 network connection details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Code</td>
<td>Description</td>
<td>Type</td>
<td>Vendor</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>QSYS2.OBJECT_LOCK_INFO</td>
<td>Object lock information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.OUTPUT_QUEUE_ENTRIES</td>
<td>Spooled file in output queue</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.RECORD_LOCK_INFO</td>
<td>Record lock information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.REPLY_LIST_INFO</td>
<td>Current job's reply list entry information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SCHEDULED_JOB_INFO</td>
<td>Job Schedule Entry information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SERVER_SBS_ROUTING</td>
<td>Alternate subsystem configurations</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SERVER_SHARE_INFO</td>
<td>Server Share Information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SOFTWARE_PRODUCT</td>
<td>Server Software Product information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSCONTROLS</td>
<td>Permissions or column mask defined</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSCONTROLSDEP</td>
<td>Dependencies of row permissions and column masks</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSDISKSTAT</td>
<td>Disk Information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSTEM_STATUS_INFO</td>
<td>Partition information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSTMPSTG</td>
<td>IBM i temporary storage pool detail</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.USER_INFO</td>
<td>User Profile Information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.USER_STORAGE</td>
<td>Storage usage by user profile</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>REMOTE_TRAN_SUMMARY_BY_SERVER</td>
<td>Remote Summary Server</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>REMOTE_TRAN_SUMMARY_BY_USER</td>
<td>Remote Summary User</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_COMPLIANCE_DATA</td>
<td>Resource Manager Authority Out of compliance data</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_CONFIG</td>
<td>Resource Manager Configuration</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_SCHEMADETAILS</td>
<td>Resource Manager Authority Schema Details</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_SCHEMA_HEADER</td>
<td>Resource Manager Authority Schema Header</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SENSITIVE_DATABASE_CONTENT</td>
<td>Sensitive Database Content</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>SERVICE_TOOL_SECURITY_ATTR</td>
<td>Service Tool Security Attributes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>SERVICE_TOOL_USERS</td>
<td>Service Tool User Data</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOCKET_SUMMARY_BY_SERVER</td>
<td>Socket Summary by Server</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>Table Name</td>
<td>Description</td>
<td>Category</td>
<td>Platform</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>SOCKET_SUMMARY_BY_USER</td>
<td>Socket Summary by User</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOCKET_TRAN_RULES</td>
<td>Socket Rules</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOCKET_TRANSACTIONS</td>
<td>Socket Transactions</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOFTWARE_RESOURCES</td>
<td>Installed Software Resources Data</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_AUTOSTART</td>
<td>Subsystem Autostart Jobs</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_COMMUNICATIONS</td>
<td>Subsystem Communication Entries</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_INFORMATION</td>
<td>Subsystem Information Details</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_JOB_QUEUE</td>
<td>Subsystem Job Queue</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_POOL_DATA</td>
<td>Subsystem Pool Data</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_PRESTART</td>
<td>Subsystem Prestart Jobs</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_REMOTE</td>
<td>Subsystem Remote Entries</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_ROUTING</td>
<td>Subsystem Routing Entries</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_WORKSTATION_NAMES</td>
<td>Subsystem Workstation Names</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_WORKSTATION_TYPES</td>
<td>Subsystem Workstation Types</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYS_VAL_CONFIG</td>
<td>System Value Configuration</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYS_VAL_DEFAULT</td>
<td>System Value Default</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYS_VAL_VALID</td>
<td>System Value Default</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCOLAUTH</td>
<td>Privileges Granted on a Column</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCONTROLS</td>
<td>Permission or Column Mask Defined</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCONTROLSDEP</td>
<td>Dependencies of Row Permissions and Column Masks</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCONTROLSDEP</td>
<td>Privileges Granted on a Row</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSFIELDS</td>
<td>Columns with Field Procedures</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSPACKAGEAUTH</td>
<td>Privileges Granted on a Package</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSPROGRAMSTAT</td>
<td>Program, Service Program, and Module with SQL Statements</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSRoutineAUTH</td>
<td>Privileges Granted on a Routine</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSSCHEMAAUTH</td>
<td>Privileges Granted on a Schema</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSSEQUENCEAUTH</td>
<td>Privileges Granted on a Sequence</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTABAUTH</td>
<td>Privileges Granted on a Table or View</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>Table Statistics Include all Partitions and Members</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>Table Title</td>
<td>Description</td>
<td>Module</td>
<td>Platform</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>SYSTEM_VALUES</td>
<td>Display System Value Data</td>
<td>System</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTOOLS.GROUP_PTF_CURRENCY</td>
<td>PTF Groups Installed per IBM Recommendations</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTOOLS.GROUP_PTF_DETAILS</td>
<td>PTFs within PTF Groups Installed per IBM Recommendations</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSUDTAUTH</td>
<td>Privileges Granted on a Type</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSVARIABLEAUTH</td>
<td>Privileges Granted on a Global Variable</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSXSROBJECTAUTH</td>
<td>Privileges Granted on an XML Schema</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>TGMOBJINF</td>
<td>Object Information</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_NETWORK_GROUPS</td>
<td>TG Network Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_OBJECT_GROUPS</td>
<td>TG Object Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_OPERATION_GROUPS</td>
<td>TG Operation Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_USER_GROUPS</td>
<td>TG User Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_OBJECT_AUTHORITIES</td>
<td>User Profile Object Authorities</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PRF_VIA_BLUEPRINT</td>
<td>User Profile via Blueprint</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILE_ACTIVITY</td>
<td>User Profile Activity</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILE_ARCHIVE</td>
<td>User Profile Archive</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILE_EXCLUSIONS</td>
<td>User Profile Exclusions</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILES</td>
<td>Display User Profile Data</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
</tbody>
</table>
APPENDIX - TG Fix

The TG Fix tool allows you to install fixes via the TG menu quickly and easily. This feature also includes verification features that ensure the fix is installed properly.

See also

Working with TG Fix
APPENDIX - TG Management

The **TG Management** tool allows you to configure TG product administrative elements (e.g., licensing, user authorization, report output formats, etc.).

**See also**

*Working with TG Management*
APPENDIX - TG Save and Restore

The **TG Save and Restore** tool allows you to save the configuration of a specific instance of TGSecure or TGAudit. Once you save a configuration, you can then use that saved configuration file to do the following:

- Create a back-up (archive) of the current configuration to be used later to restore the configuration of an agent (server)
- Create multiple instances with identical configuration

A saved file stores the configuration for the following:

- Calendars
- Entitlement
- Groups
- Networks
- Reports
- Rules (i.e., Socket Rules, Exit Rules, etc.)

**See also**

*Working with the TG Save and Restore*
APPENDIX - TG Job Scheduler

The TG Job Scheduler tool allows you to select the desired scheduler:

- IBM
- IBMAJS
- ROBOT

See also

Working with the TG Job Scheduler
APPENDIX - TG Journal Cleanup

The **TG Journal Cleanup** (TGJRNCLEAN) tool is a command-line tool that allows you to manage journal receiver data.

Journaling is widely used on IBM i servers to keep track of database changes as well as system and security level audit information. Journal data cannot be altered or corrupted. Therefore, it is very useful for forensic analysis and makes IBM i the best platform for security. With all these journaling capabilities, cleaning up old journal data becomes a critical task for the system administrator or storage issues could result.

⚠️ **Important**: Before using this tool, review your data retention policy and make a backup of the receivers for later retrieval. In case of a security incident investigation, old receiver data is required for forensic analysis.

See also

- Journal Cleanup Tool
- Journaling Concepts
- Journal Management
APPENDIX - TG Transaction Cleanup

The **TG Incoming Transaction Cleanup** (TGNTWCLEAN) tool is a command-line tool that allows you to manage incoming transaction data.

**See also**

[Working with TGNTWCLEAN](#)