NetIQ Security Solutions for IBM i

TGSecure 26.4 (v4.2)

Migration User Guide

Revised June 2026

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 © 2026 Trinity Guard LLC. All rights reserved.

TGMigrate Introduction 2
Setup 3
Getting Started 4
Use TGMigrate 5
Log into TGMigrate 7
Run Migration Report 8
View Migration Report 9
Migrate Elements 13
Exit Points 15
Working with Exit Points 17
Display List of Exit Points 18
Manage Exit Points 20
Run Exit Points Report 28

TGMigrate Introduction

TGMigrate is a migration tool that provides a fast and efficient way to migrate the following data elements from PSSecure® to TGSecure®:

- Rules
- Groups
- Calendars
- File Editors

Tip: You must have the authority to modify files in both PSSecure and TGSecure to perform a migration.

See also

Setup

Getting Started

Exit Points

Setup

Use this task to grant a user access to the TGMigrate command/tool/work object.

> ⚠ **WARNING**: By default, the TGSecure administrator should have authority to use the TGMigrate tool. Therefore, if the TGSecure administrator is performing the migration, this step is not necessary. In other words, the administrator by default should have authority to migrate data. Instead, you could use this task to view the list of users who have authority to use the TGMigrate tool, which is a powerful tool that has the ability to override security rules established in TGSecure with those established in PSSecure.

To set up TGMigrate authorities

1) Access the **IBM i Main** menu.

2) At the **Selection or command** prompt, enter **WRKOBJ**. The **Work with Objects** (WRKOBJ) interface is displayed.

3) In the **Object** field, enter **TGMIGRATE**.

4) In the **Library** field, enter ***LIBL** (indicating all libraries).

5) In the **Object type** field, enter ***ALL** (indicating all objects).

6) Press **Enter**.

7) In the **Opt** column beside the TGMigrate command, enter **2** (Edit authority).

8) Press **Enter**.

9) Press the **F6** (Add new users) function key. The **Add New Users** interface is displayed.

10) In the **User** field, enter the user's ID.

11) In the **Object Authority** field, enter ***ALL**.

12) Press **Enter**.

See also

TGMigrate Introduction

Getting Started

This section includes the following topics:

- Use TGMigrate
- Log into TGMigrate
- Run Migration Report
- View Migration Report
- Migrate Elements

See also

TGMigrate Introduction

Use TGMigrate

TGMigrate allows you to migrate data elements from PSSecure to TGSecure.

> **Tip**: You must have reporting authority in PSSecure and migration authority in TGSecure to use TGMigrate. Please refer to the PSSecure product documentation for instruction on user authorities.

- **Network Security** - Import rules (i.e., socket rules and exit rules)
- **Access Escalation Management** - Import entitlements
- **Groups** - Import groups (i.e., user, network, operation, and object)
- **Calendars** - Import calendars
- **File Editors** -Import file editors

Tasks

Each project is unique, but here is the basic workflow for using TGMigrate.

	Instructions
1	Log into TGMigrate to begin the migration process.
2	Run migration report to identify the data elements (i.e., rules, groups, calendars, etc.) available in PSSecure for import.
3	View migration report to determine whether you want to merge or replace the data elements from PSSecure to TGSecure: -- **Merge** - TGMigrate compares the data elements in PSSecure with the data elements in TGSecure and imports only the data elements that do not already exist in TGSecure. In other words, only non-duplicate PSSecure elements are appended to the list of existing TGSecure elements. -- **Replace** - TGMigrate clears (deletes) all existing TGSecure data elements (i.e., rules, groups, calendars, etc.) and imports in PSSecure data elements. **Tip**: Before creating any elements in TGSecure, determine if you plan to migrate information from PSSecure. If you do plan to migrate elements, you might want to hold off on making modifications in TGSecure until the migration is complete. **Note**: See the TGSecure User Guide for instructions on creating, modifying and deleting elements. You can

	download TGSecure product documentation from the TrinityGuard.com Customer Portal.
4	Migrate elements to move data

See also

Getting Started

Log into TGMigrate

Use this task to log in and access the TGMigrate tool.

To log in and prompt the TGMigrate tool

1) Sign into your IBM i server.

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

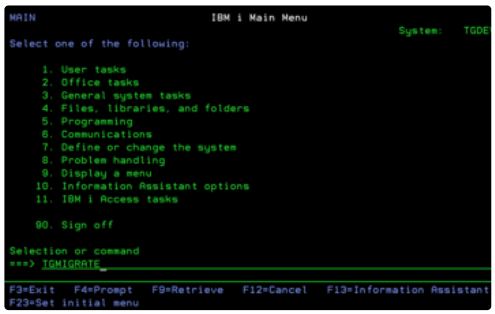


Figure: IBM i Main Menu

3) Press the **F4** (Prompt) function key. The **Migrate PS Data to TG Files** (TGMIGRATE) interface is displayed.

See also

Getting Started

Run Migration Report

Use this task to run a report that displays the data elements (i.e., rules, entitlements, groups, calendars, file editors) in PSSecure that are available for migration to TGSecure.

Tip: Before migrating elements, it's important to understand what exists in PSSecure.

To run the migration report

1) Access the **IBM i Main** menu.

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

3) Press the **F4** (Prompt) function key. The **Migrate PS Data to TG Files** (TGMIGRATE) interface is displayed.

4) Complete the following fields:

Field	Description
Product Name	Identify the TGSecure feature (i.e., Network Security or Access Escalation) for which you want to import data elements. ***NTW** - Enter this text to import elements used in network security only ***ACC** - Enter this text to import elements used in access escalation only ***ALL** - Enter this text to import elements used in both network security and access escalation
Copy Type	***MERGE** - Identify only the PSSecure elements that do not exist in TGSecure ***REPLACE** - Identify all PSSecure elements available for import regardless if an element with the same name exists in TGSecure

5) In the **Action** field enter ***REPORT**.

6) Complete the following field:

Field	Description
Run Interactively	***YES** - Enter this option to run the report immediately ***NO** - Enter this option to add the report to a job queue (run in batch mode)

7) Press **Enter**.

Note: A spool file is generated (see the message at the bottom of the IBM i screen).

8) Make a note of the spool file name. You will need the file name when you search for the report in the **Work with All Spooled Files** (WRKSPLF) interface.

See also

Getting Started

View Migration Report

Use this task after you run a migration report to perform an analysis of the data elements (i.e., rules, entitlements, groups, calendars, file editors) in PSSecure available for migration to TGSecure. This report gives you an opportunity to identify issues with the migration. The migration report identifies failures and successes (See the **Migration Status** column of the report). Elements with a status of **Success** should migrate from PSSecure to TGSecure with no compatibility issues. Elements with a status of **Failure**, should be investigated. Compatibility issues are specific to each element and, therefore, cannot be described here. It is the responsibility of the individual to perform the migration to investigate and resolve each unique situation.

To view the migration report

1) Access the **IBM i Main** menu.

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

3) Press **Enter**. The **Work with All Spooled Files** (WRKSPLF) interface is displayed.

4) Scroll through the list of reports until you locate the migration report spool file.

> **Note**: You should have made a note of the spool file name at the time you ran the report (**CMN74000O**).

5) In the **Opt** column beside the migration report spool file, enter **5** (Display) to see the results. The **Display Spooled File** interface displays.

6) Review the report details.

Information common to all report sections:

Each element type appears in a separate section of the spool file (report). The number of sections is dependent on the elements found. At the end of each section is a summary identifying the number of elements of each type available for import.

> **Note**: Some elements produce two data files (e.g., calendars elements). The first file contains the element header details and the second file contains the element component details.

Calendars: Header

Field	Description
Calendar Name	Name (ID) assigned to the calendar
Start Date	Start date on which the calendar is valid
Start Time	Start time at which the calendar is valid
End Date	End date on which the calendar is valid
End Time	End time at which the calendar is valid
Calendar Description	Short description identifying the purpose of the calendar

Calendars: Details

Field	Description
Calendar Name	Name (ID) assign to the calendar
Days of the Week	The day of the week on which the calendar is valid
Start Time	Start time (specific to a day of the week) at which the calendar is valid
End Time	End time (specific to a day of the week) at which the calendar is valid
Migration Status	Status of migration **Note**: Fail rate should be 100% when you are running a migration report because no migrations should occur in *REPORT mode. **Tip**: If failures occur in *MERGE mode, investigate the failure before proceeding.

Groups: User Groups and Members

Field	Description
Group Name	Name (ID) assigned to the user group
User Name	Name of group member (a user is this case) **Note:** Each group member appears in a separate row.
Group / User Description	Description assigned to the user group
Profile St	Profile status of the group member (a user in the case)
PWD E. Date	Date on which user's password expires
User Text	Description assigned to group member (a user in this case)

Groups: Network Groups and Members

Field	Description
Group Name	Name (ID) assigned to the network group
Network Address	IP address of server
Description	Description assigned to network group
Migration Status	Status of migration: **Success** - There are no compatibility issues stopping the migration of this element **Failure** - There are compatibility issues. The migration of this element will not occur

Groups: Object Groups and Members

Field	Description
Command Group	Name (ID) assigned to the object group
Object Name	Name of group member (an object in the case of an object group) **Note:** Each group member appears in a separate row.
Object Library	Library in which object resides
Object Type	Type of object
Migration Status	Status of migration: **Success** - There are no compatibility issues stopping the migration of this element **Failure** - There are compatibility issues. The migration of this element will not occur

Groups: Operation Groups and Members

Field	Description
Operation Name	Name assigned to the user group
Operation	Name assigned to the group member, in this case, an operation
Description	Description of the operation
Migration Status	Status of migration : **Success** - There are no compatibility issues stopping the migration of this element **Failure** - There are compatibility issues. The migration of this element will not occur

Editor Commands (File Editors)

Field	Description
Edit command	Name (ID) assigned to the IBM UPDDTA command or third-party command
Editor Library	Library in which the command resides
Editor Parameter	The type of file objects the command can modify
Migration Status	Status of migration : **Success** - There are no compatibility issues stopping the migration of this element **Failure** - There are compatibility issues. The migration of this element will not occur

Exit Point

Field	Description
Exit Point	Name (ID) assigned the exit point
ExitFmt	Exit point format
Text	Description assigned to the exit point
SecMod	Identifies whether the exit point is used in security monitoring
Pgm	Exit (security monitory) program associated with the exit point
PgmL	Library in which the exit program resides
Pga	Custom program associated the exit point
Pgal	Library in which the custom program resides
ColMod	Identifies the collection mode: *__ALL__ - collect all transactions, including R (rejects) and A (allowed) *__NONE__ - collect no transactions *__REJECTED__ - collect rejected transactions only *__UNSECURED__ - collect transactions not addressed by a rule
Serv	Identifies the server, function, command combination associated with the exit point (e.g., DRDA, FTPSRV, FILE, DBSQL, etc.).

See also

Getting Started

Migrate Elements

Use this task to migrate elements (i.e., rules, groups, calendars, file editors, etc.) from PSSecure to TGSecure.

WARNING : During the migration process, the system changes the exit point **Secure Status** to ***NO**, which means that exit rule security is disabled. As soon as you complete the migration and you are satisfied that data is being collected as expected, then you should immediately enable exit point security (switch the **Secure Status** to ***YES**).

Tip: You should perform the migration immediately after installing TGSecure. If you first add elements to TGSecure and then perform a migration, you run the risk of replacing the elements you added before the migration. Therefore, to avoid duplicating work, perform the migration before creating new elements in TGSecure.

To Migrate Elements

1) Access the **IBM i Main** menu.

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

3) Press the **F4** (Prompt) function key. The **Migrate PS Data to TG Files** (TGMIGRATE) interface is displayed.

4) Complete the following fields:

Field	Description
Product Name	Identify the type TGSecure feature (i.e., Network Security or Access Escalation) for which you want to import data elements: ***NTW** - Enter this text to import elements used in network security only ***ACC** - Enter this text to import elements used in access escalation only ***ALL** - Enter this text to import elements used in both network security and access escalation
Copy Type	Identify how you want to deal with copies: ***MERGE** - Import element from PSSecure that do not conflict with existing elements in TGSecure (i.e., append the file) ***REPLACE** - Import all elements from PSSecure, overriding the existing set of elements in TGSecure (i.e., replace the file)

5) In the **Action** field enter ***MIGRATE**.

Note: ***MIGRATE** generates the same report (spool file) produced when you select ***REPORT**, but the system takes the additional action of replacing the element files. In other words, it completes the migration.

6) Complete the following field:

Field	Description

Run Interactively	***YES** - Enter this option to run the report immediately ***NO** - Enter this option to add the report to a job queue (run in batch mode)

7) Press **Enter**.

> **Note**: After the migration is complete, access TGSecure and review the imported elements. See the TGSecure User Guide for instructions on creating, modifying and deleting elements.

8) Tests the TGSecure is collecting data as expected.

9) Once you are satisfied that the migration was a success, immediately enable exit point security (change the **Security Status** to ***YES**).

> **Note**: Objects in a group that are migrated are given the file system type of ***SYS**.

See also

Getting Started

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 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

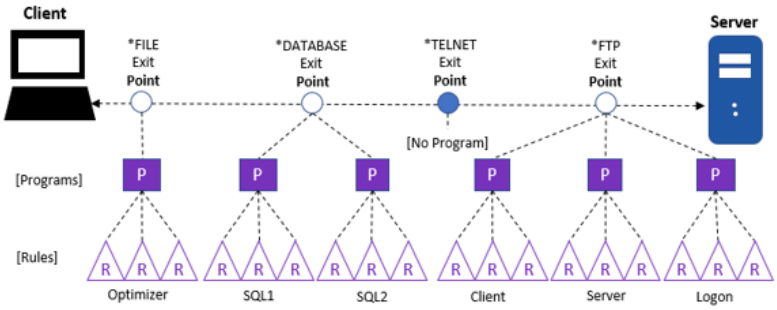
The prior paragraph uses a lot of jargon, so here is an analogy to help you conceptualize what an exit point represents. Say that your IBM server is a building. In the past, if someone wanted to access your building, they would just walk to it. Then, at some point, people started riding horses, and then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



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.

See also

Working with Exit Points

Working with Exit Points

This section includes the following topics:

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

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

To access the Network Security Configuration interface

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

See also

Exit Points

Display List of Exit Points

Use this task to display the list of exit points.

To display the list of exit points

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

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

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

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

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

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

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

	However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. 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 Points

Manage Exit Points

Use this task to do the following with exit points.

- Access the 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 Program from Exit Point
- 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 Network Security Configuration Interface

To access the Work with Network Security Configuration 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 **10** (Exit Point Configuration).

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

Display Exit Point Details

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

To display exit point details

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

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

3) Press **Enter**.

Field	Description
Network Server	Name of the server type

Exit Point	Name assigned to the exit point
Exit Format	IBM format associated with the exit point
Exit Description	Description of the exit point
Exit Program Installed	Indicates whether the exit point is installed on the server ***YES** - Exit points are installed and ready for use ***NO** - Exit points are not installed **Note**: The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to ***YES**.
Function Usage Rule	Indicates whether an IBM function usage rule is being applied at the exit point. This indicator is important because it helps to identify conflicts between exit rules and function usage rules. If there is a conflict (e.g., an exit rule states to do one thing, but a function usage rule states to do something different), then the system might produce an unexpected outcome. ***YES** - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists ***NO** - No function usage rule is applied at the exit point ***NA** - Not applicable because IBM does not provide a function usage rule for this exit point
Audit Status	Indicates whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports **{**}YES* - Record incoming transaction data in the audit journal ***NO** - Do not record incoming transaction data in the audit journal **Tip**: If auditing is disabled at the module level, then this setting is ignored. In other words, if auditing is disabled at the network security (module) level, then auditing will not occur even if auditing is enabled at the exit point (secondary) level. The module-level setting takes precedence. However, if auditing is enabled at the module level, you must also enable alerting at the secondary level if you want to record auditing data for a specific exit point. **Note**: See Manage Network Security Defaults for information about enabling/disabling auditing globally.
Security Status	Indicates whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go in to effect. **{**}YES* - Apply exit rules (enable network security) ***NO** - Disable exit rules (disable network security)
Alert Status	Indicates whether alerts are enabled for a specific exit point. Alerts are required if you plan to send alert notifications ***ALL** - Record an alert for all (PASS and FAIL) connection attempts ***FAIL** - Record only FAIL connection attempts ***NONE** - Do not record alerts **Tip**: If alerts are disabled at the module level, then this setting is ignored. In other words, if alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module-level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level

	if you want to record alerts for a specific exit point. See Manage Network Security Defaults for information about enabling/disabling alerting globally.
Smart Mode	Indicates whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules **Note**: The system administrator can delete rules created by the Rules Intelligence Engine at any time.
Collector Status	Indicates which incoming transactions you want to track (collect) in the **Incoming Transaction** interface ***ALL** - Collect and display all (PASS and FAIL) incoming transactions ***FAIL** - Collect and display only rejected (FAIL) incoming transactions ***NONE** - Do not collect or display any incoming transactions

Enable Exit Point Auditing

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

Prerequisite

Auditing must be enabled in the Network Security Module. See Manage Network Security Defaults.

To enable auditing for an exit point

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

Enable Exit Point Security

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

Prerequisite

Create the exit rules you want to apply. 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, 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**.

Note: 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 exit programs 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 a 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 exit programs from exit points

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

2) Press the **F21** (Remove Exit Programs) function key.

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

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

4) Press **Enter**.

Cycle Server

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

To cycle a single server

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

2) In the **OPT** column for the desired exit point, enter **13** (Cycle Server).

3) Press **Enter**.

4) Ensure that the correct server is selected.

5) Enter one of the following options:

   – **Y** - Initiate cycling immediately (run in interactive mode)

   – **N** - Place cycling request in the queue (run as part of a job queue)

6) Press **Enter**.

Cycle Servers (Mass Update)

Use this task to restart multiple servers.

To cycle multiple servers

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

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

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

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

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

5) Press **Enter**.

Update all Exit Points (Mass Update)

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

To update all exit points

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

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

3) Modify the setting as necessary.

Note: All editable settings are underlined.

Field	Description
Audit Status	Indicates whether auditing is enabled. Auditing is required if you plan to run network security reports. ***YES** - Record incoming transaction data in the audit journal for all installed exit points ***NO** - Do not record incoming transaction data in the audit journal for all installed exit points ***SAME** - Do not perform a mass update of the **Audit Status**. In other words, skip this setting. **Tip**: See Manage Network Security Defaults for information about enabling auditing globally. Global defaults take precedence over local settings.
Security Status	Indicates whether the exit rules associated with the exit point should be applied. ***YES** - Apply exit rules for all installed exit points ***NO** - Do not apply exit rules for all installed exit points ***SAME** - Do not perform a mass update of the **Security Status**. In other words, skip this setting during the mass update.
Alert Status	Indicates whether alerting is enabled. Alerting is required if you plan to send alert notifications. ***ALL** - Record an alert for all (PASS and FAIL) connection attempts ***FAIL** - Record only FAIL alerts for all installed exit points ***NONE** - Do not record alerts for all installed exit points ***SAME** - Do not perform a mass update of the **Alert Status**. In other words, skip this setting during the mass update. **Tip**: See Manage Network Security Defaults for information about enabling alerting globally. Global defaults take precedence over local settings.
Smart Mode	Indicates whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules ***SAME** - Do not perform a mass update of the **Smart Mode**. In other words, skip this setting during the mass update.
Collector Status	Indicates which incoming transactions are tracked (collect) in the **Incoming Transaction** interface. ***ALL** - Collect and display all (PASS and FAIL) connection attempts ***FAIL** - Collect and display only FAIL connection attempts ***NONE** - Do not collect or display any connection attempts

	***SAME** - Do not perform a mass update of the **Collector Status**. In other words, skip this setting during the mass update.

4) Press **Enter**.

See also

Working with Exit Points

Run Exit Points Report

Use this task to generate reports that display the following for exit points:

- 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. 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 Exit Point Configuration Changes Report

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

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

To run the Exit Point Configuration Change Report

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

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

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

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

See also

Working with Exit Points