NetIQ Security Solutions for IBM i
TGSecure 1.6
Migration Guide

Revised October 2017

Legal Notice

Table of Contents

1. Introduction

1.1. Product Overview

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

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

- Rules
- Groups
- Calendars
- File Editors

See also:

Set up TGMigrate Authorities

Using TGMigrate

2. Setup

2.1. To Set Up TGMigrate Authorities

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**.

Note: 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.

Note: 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

Use TGMigrate

3. Getting Started

3.1. Getting Starting Using 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

3.1.1. Tasks

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

Step 1	Log into to TGMigrate to begin the migration process.
Step 2	Run the migration report to identify the data elements (i.e., rules, groups, calendars, etc.) available in PSSecure for import.
Step 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.
Step 4	Migrate the elements.

See also

Set Up TGMigrate Authorities

3.2. 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.

Note: The **Migrate PS Data to TG Files** (TGMIGRATE) interface is displayed.

3.3. 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.

Note: 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

View Migration Report

3.4. 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 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**.

Note: 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.

Note: 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

Field	Description
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 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

Run Migration Report

3.5. 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.

Note: 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	***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**.

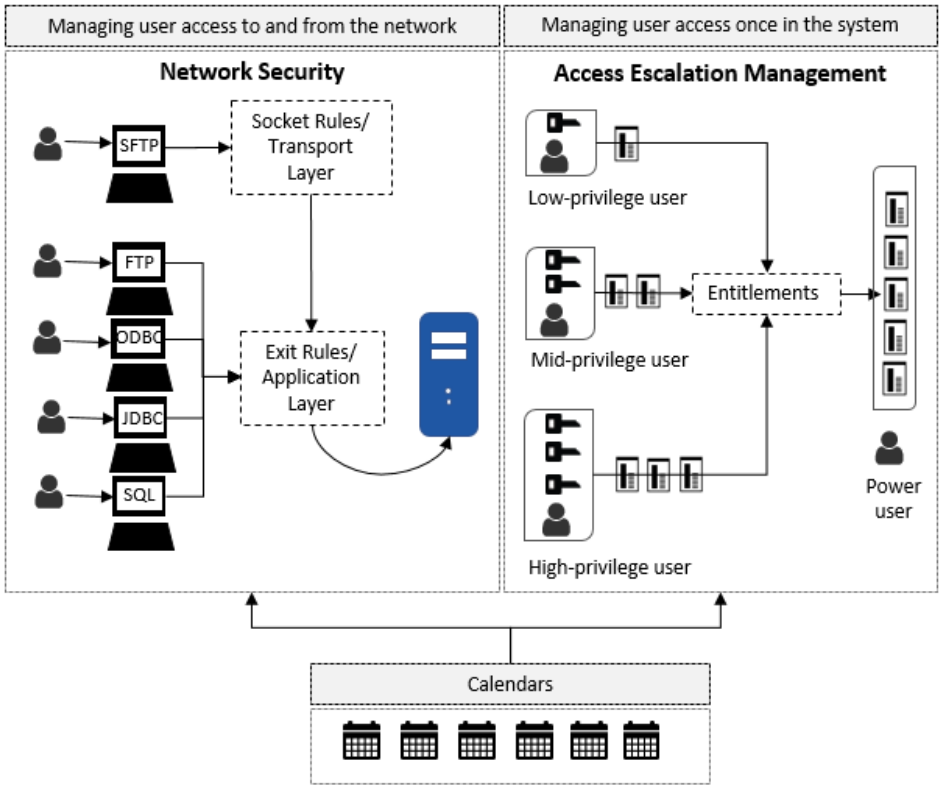
See also:

Enable Exit Point Security

4. Glossary

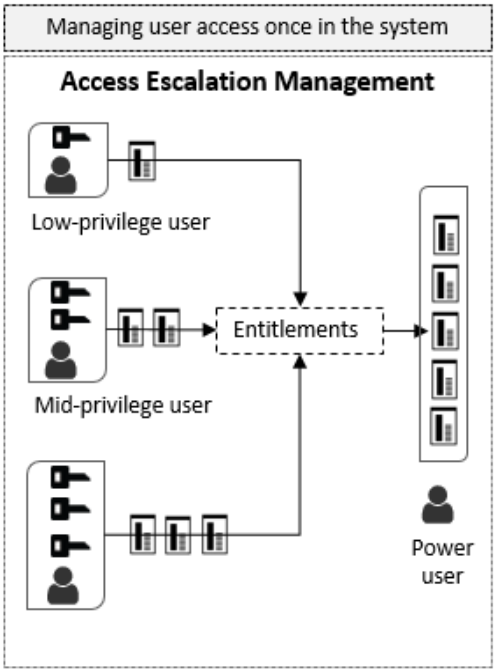
Calendars

The calendar allows you to enable a rule or entitlement for a specific duration (e.g., after hours, during weekends, on a holiday, etc.).



Entitlement

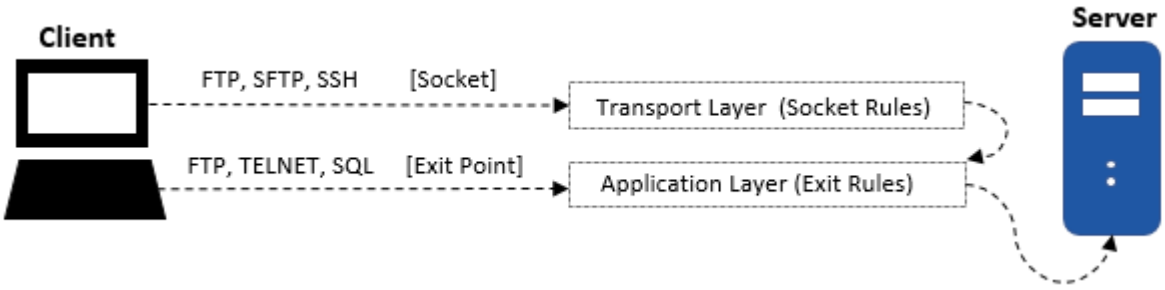
Entitlements are a form of rule associated with access management. Entitlements allow you to control the access level of a user or a user group at a very granular level. For example, a user might be required to perform a high-level task at the end of each fiscal year. Instead of granting the user high-level access throughout the year, you could create an entitlement that allows the user to perform the task at a designated time. In addition to identifying the specific task to be performed, you must also identify a swap user. A swap user is normally a user with higher-level privileges. In most cases, the user will need to temporarily borrow the swap users' privileges to perform the high-level task identified in the entitlement.



Exit Rules

Exit rules allow you to define criteria that control network access via TLS (Transport Layer Security). Exit rules are applied at exit points.

Note: Socket rules (if they exist) are applied before exit rules. In addition, function usage rules, which are also applied at exit points have the potential to conflict with exit rules. See Manage Exit Points for additional information about identifying conflicts.



Tip: There is a third type of rule called a function usage rule. These are generic rules provided by IBM that clients can apply at exit points. Function usage rules have limited functionality compared to exit rules, but your company might have applied one or more of these lower-capability function usage rules prior to implementing higher-capability exit rules. Therefore, there is the possibility that an existing function usage rule might conflict with a newly created exit rule. It is important that you identify and resolve any conflicts before deploying exit rules. See Manage Exit Points for more information about how to identify conflicts.

File Editors

File editors are custom IBM UPDDTA commands or third-party commands that you can use in addition to the standard IBM iSeries commands.

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 it as a command.

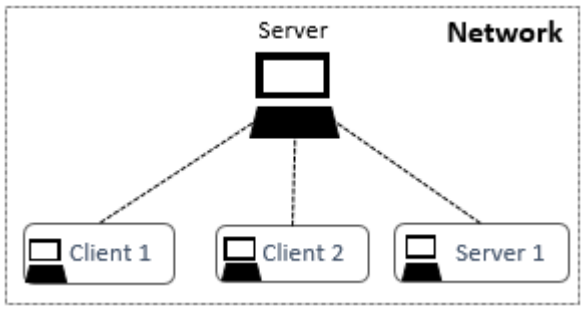
Groups

Groups are a means by which to organize system elements (which will be referred to as members). Once you create a group, you can use that group for different purposes. For example, you could use a group as a parameter when defining a rule. Therefore, the rule would apply to all user in the group. You can also use a group as a parameter when generating a report. For example, you might want your report to include information about a network group versus a specific server.

Note: The types of groups and reports available to you are dependent on your license agreement.

Networks

A network consists of a hub of computers. Normally, in a network, a more powerful, centralized computer (called the server) is connected to less powerful, distributed personal computers (called clients).



Objects

An object is a unit that exists (occupies space) in storage. Journals provide a means by which you can record the activity of an object.

Operations

An operation consists of a server, a function, and a command referenced by an incoming (remote) transaction. For example, the following table displays a list of functions and commands that might be received from an FTP server.

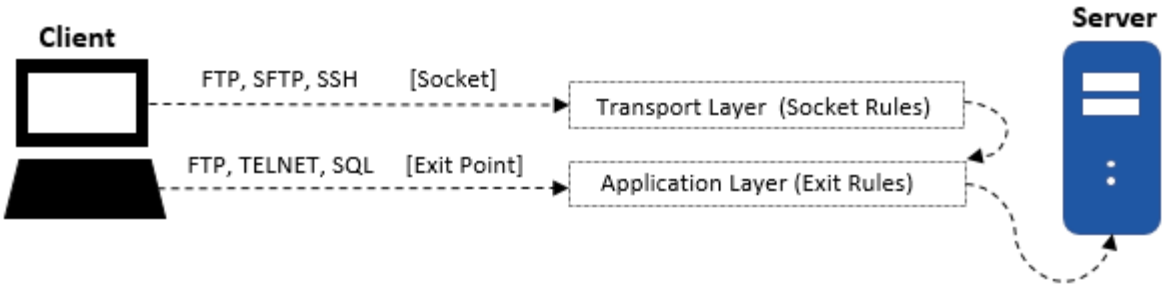
	Server	Function	Command
1	FTP	*ALL	*ALL
2	FTP	PUT	*ALL
3	FTP	GET	*ALL
4	FTP	CD	*ALL
5	FTP	DEL	*ALL

Rules

A rule allows you to control or limit an action or activity.
Note: The types of rules available to you are dependent on your license agreement.

Socket Rules

Socket rules allow you to define criteria that control network access via a socket. The socket provides an extra layer of security (or vulnerability) prior to the application layer, which provides security through exit rules.



User

A user when referenced in this documentation is referring to an individual who required access to the system.