Legal Notice

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

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

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

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

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

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

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

TABLE OF CONTENTS .................................................................................................................................................. III

1. INTRODUCTION ........................................................................................................................................................ 4
1.1. PRODUCT OVERVIEW ............................................................................................................................................... 4

2. SETUP ........................................................................................................................................................................ 5
2.1. TO SET UP TGMIGRATE AUTHORITIES .................................................................................................................. 5

3. GETTING STARTED .................................................................................................................................................... 7
3.1. GETTING STARTING USING TGMigrate .................................................................................................................... 7
   3.1.1. Tasks ................................................................................................................................................................. 7
3.2. LOG INTO TGMIGRATE ............................................................................................................................................. 7
3.3. RUN MIGRATION REPORT .................................................................................................................................... 8
3.4. VIEW MIGRATION REPORT .................................................................................................................................. 9
3.5. MIGRATE ELEMENTS ........................................................................................................................................... 12
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 TG Migrate

TG Migrate 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 TG Migrate. 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 TG Migrate.

**Step 1**  
Log into TG Migrate 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** - TG Migrate 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** - TG Migrate 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 TG Migrate Authorities

3.2. Log into TG Migrate

Use this task to log in and access the TG Migrate tool.

To log in and prompt the TG Migrate tool
1) Sign into your IBM i server.
2) At the Selection or command prompt, enter TGMIGRATE.

![IBM i Main Menu](image)

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Interactively</td>
<td>*YES - Enter this option to run the report immediately</td>
</tr>
<tr>
<td></td>
<td>*NO - Enter this option to add the report to a job queue (run in batch mode)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar Name</td>
<td>Name (ID) assigned to the calendar</td>
</tr>
<tr>
<td>Start Date</td>
<td>Start date on which the calendar is valid</td>
</tr>
<tr>
<td>Start Time</td>
<td>Start time at which the calendar is valid</td>
</tr>
<tr>
<td>End Date</td>
<td>End date on which the calendar is valid</td>
</tr>
<tr>
<td>End Time</td>
<td>End time at which the calendar is valid</td>
</tr>
<tr>
<td>Calendar Description</td>
<td>Short description identifying the purpose of the calendar</td>
</tr>
</tbody>
</table>

## Calendars: Details

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

## Groups: User Groups and Members

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name (ID) assigned to the user group</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of group member (a user is this case)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Each group member appears in a separate row.</td>
</tr>
<tr>
<td>Group / User</td>
<td>Description assigned to the user group</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Profile St</td>
<td>Profile status of the group member (a user in the case)</td>
</tr>
<tr>
<td>PWD E. Date</td>
<td>Date on which user’s password expires</td>
</tr>
<tr>
<td>User Text</td>
<td>Description assigned to group member (a user in this case)</td>
</tr>
</tbody>
</table>
### Groups: Network Groups and Members

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name (ID) assigned to the network group</td>
</tr>
<tr>
<td>Network Address</td>
<td>IP address of server</td>
</tr>
<tr>
<td>Description</td>
<td>Description assigned to network group</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Group</td>
<td>Name (ID) assigned to the object group</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Name</td>
<td>Name assigned to the user group</td>
</tr>
<tr>
<td>Operation</td>
<td>Name assigned to the group member, in this case, an operation</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the operation</td>
</tr>
</tbody>
</table>
| 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)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit command</td>
<td>Name (ID) assigned to the IBM UPDDTA command or third-party command</td>
</tr>
<tr>
<td>Editor Library</td>
<td>Library in which the command resides</td>
</tr>
<tr>
<td>Editor Parameter</td>
<td>The type of file objects the command can modify</td>
</tr>
</tbody>
</table>
### Field Description

**Migration Status**
- **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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit Point</td>
<td>Name (ID) assigned the exit point</td>
</tr>
<tr>
<td>ExitFmt</td>
<td>Exit point format</td>
</tr>
<tr>
<td>Text</td>
<td>Description assigned to the exit point</td>
</tr>
<tr>
<td>SecMod</td>
<td>Identifies whether the exit point is used in security monitoring</td>
</tr>
<tr>
<td>Pgm</td>
<td>Exit (security monitor) program associated with the exit point</td>
</tr>
<tr>
<td>PgmL</td>
<td>Library in which the exit program resides</td>
</tr>
<tr>
<td>Pga</td>
<td>Custom program associated the exit point</td>
</tr>
<tr>
<td>Pgal</td>
<td>Library in which the custom program resides</td>
</tr>
<tr>
<td>ColMod</td>
<td>Identifies the collection mode:</td>
</tr>
<tr>
<td></td>
<td>*ALL - collect all transactions, including R (rejects) and A (allowed)</td>
</tr>
<tr>
<td></td>
<td>*NONE - collect no transactions</td>
</tr>
<tr>
<td></td>
<td>*REJECTED - collect rejected transactions only</td>
</tr>
<tr>
<td></td>
<td>*UNSECURED - collect transactions not addressed not addressed by a rule</td>
</tr>
<tr>
<td>Serv</td>
<td>Identifies the server, function, command combination associated with the exit point (e.g., DRDA, FTPSRV, FILE, DBSQL, etc.).</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:

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