One Identity Safeguard for Privileged Passwords 2.1 (or later)

TPAM Migration Guide

IMPORTANT: Contact One Identity Professional Services to acquire the tool for TPAM migration and receive guidance specific to your organization. The tool and custom support is not available through One Identity Support.

Safeguard TPAM Migration Guide
Updated - August 2020
Version - 2.1

Contents

1

Migration overview

IMPORTANT: Contact One Identity Professional Services to acquire the tool for TPAM migration and receive guidance specific to your organization. The tool and custom support is not available through One Identity Support.

The TPAM to Safeguard Migration Guide includes step-by-step instructions for migrating data from TPAM to Safeguard for Privileged Passwords as well as what to consider before and after the migration.

The following elements can be selected for migration.

- Users are migrated with default permissions. Passwords are randomly generated and are available in a .csv file.
- Accounts and Systems relationships are migrated to Safeguard. Systems (Assets) are set up on a default partition profile and Accounts are tied to the Systems (Assets) migrated.
- TPAM Collections are migrated and are assigned to Systems/Accounts in Safeguard.

Versions

The following versions are required to perform the TPAM to Safeguard migration:

- TPAM 2.5.919 (or later)
- Safeguard 2.1 (or later)

2

Pre-migration activities

Activities to complete before performing the migration follow.

Timing

Plan the timing of the migration. Once started, if you close the migration tool, the migration will stop and partial data may be migrated.

Post migration considerations

Before starting the migration, ensure you have planned for post migration activities. For more information, see Post migration activities.

Identify the order of migration

You can migrate Systems/Accounts, Collections, and Users from TPAM all at once. Or, you can perform the migration in smaller increments by entity or records in an entity. Some Administrators prefer migrating smaller datasets because of the shorter timeframes, ease of checking smaller datasets, and impact on the organization.

Follow these guidelines as you determine how you will migrate the data:

- **Systems/Accounts**: Systems/Accounts must be migrated before Collections so the Collections can be assigned to Safeguard Systems/Accounts. Accounts can be migrated with or without passwords. For example, you may migrate Accounts without passwords, check the data, and then migrate the passwords. Or, you may want to enter passwords directly in Safeguard.

  IMPORTANT: Before migrating account passwords, stop the TPAM password reset schedule to prevent the account passwords being reset by the schedule while the migration is in progress.

- **TPAM Collections**: Collections must be migrated after Systems/Accounts so Safeguard Systems/Accounts can be assigned to Collections. Collections migration will not include files, permissions, roles, or affinity from TPAM.
- **Users**: Users can be migrated with other elements or alone. Passwords are randomly generated and are available in a .csv file you will be prompted to save before the migration is finished.

Ensure permissions are in place

To perform the migration, you will need the following permissions.

- TPAM permissions: The User must be a CLI (command line interface) user in TPAM with ISA permissions to pull asset account passwords in TPAM and pass the asset account passwords to Safeguard.
- Safeguard permissions: The User must have Asset Administrator, Security Policy Administrator, and User Administrator permissions in Safeguard.

Secure the SSH key

TPAM authentication requires an SSH key. You will be asked to enter the SSH key file path (for example, a .txt file) before migrating data.

Map platforms

Ensure the correct platform is part of the Asset.

System (Assets) mapping file

The file “platform_mapping.json” is included with the migration tool for customization of the Systems (assets) mappings.

If Safeguard contains custom Systems, modify the mapping file to include corresponding TPAM and Safeguard Systems (assets).

Syntax

The JSON file includes a list of keys with corresponding value objects where key is the name of the System (asset) in TPAM and the corresponding value is an asset name and type from Safeguard.

“<Key>”: {“PlatformType”: “<SafeguardAssetType>”,
"DisplayName": “<SafeguardAssetName>”},

Examples

"HP ILO2": {"PlatformType": "HPiLO",
"DisplayName": "HP iLO 2 x86"},

"HP ILO3": {
"PlatformType": "HPiLO",
"DisplayName": "HP iLO 3 x86"},

"Linux": {
"PlatformType": "LinuxOther",
"DisplayName": "" },

If system type (PlatformType) in Safeguard is unique (for example, “Linux”), there is no need for DisplayName, but if the system type is not unique (for example, “HPiLO”), the display name needs to be added to make the target system unique.

TPAM assets

A list of Safeguard assets can be obtained using Swagger:

https://<Server Name Or IP>/service/core/swagger/ui/index#/Assets

The list of TPAM assets follows.

Table 1: TPAM assets

AIX
AIX LDAP
AS400
BoKS
BoKS Linux
Cache Server
CheckPoint SP
Cisco ACS
Cisco CATOS
Cisco PIX
Cisco Router (tel)
Cisco Router (ssh)
Cyberguard
DELL iDRAC 8, 9
Dell Remote Access
DPA
ForeScout CounterAct
Fortinet
Fortinet 5
FreeBSD
HC3
HP Non-stop

HP- ILO
HP - ILO2
HP - ILO3
HP - ILO4
HP - NonStop
HP-UX
HP-UX Shadow
HP US Untrusted
IBM Datapower
IBM HMC
JunOS
LDAP
LDAPS
Linux tty
Mac 10.4
Mac 10.5, 19.6
Mac 10.7 - 10.11
Mainframe
Mainframe (ACF2)
Mainframe LDAP ACF2
Mainframe LDAP RACF
Mainframe LDAP TS
Mainframe TS
MS SQL Server
MySQL
MySQL 5.6,5.7
Net App Filer
NetScreen
NIS Plus
Nokia IPSO

Nokia IPSO 6.X
Novell NDS
OpenVMS
Oracle (Legacy)
Other
PAN-OS
POS 4690
ProxySG
PSM ICA Access
PSM Web Access
SAP
SCO
Solaris
Sonicwall (SonicOS)
SPCW
SPCW (DC)
SPCW 2
SPCW (DC) 2
SPCW Pwd
Stratus VOS
Sybase
Teradata
Tru64 Enhanced Sec.
Tru64 Untrusted
Unixware
Unixware 7.x
VMware Vsphere
Windows
Windows Active Dir
Windows Desktop

3

Migration activities

Launching and connecting

Follow the steps below to launch the One Identity Migration Tool. Make sure you have the Safeguard for Privileged Passwords and TPAM IP addresses for authentication.

1. Click the **One Identity Migration Tool** icon () and connect to Safeguard.
    a. In the **Appliance** field, enter or select the IP address of the Safeguard appliance.
    b. Click **Connect** to go to the login screen.

    NOTE: If the appliance does not have a secure certificate, the following standard message displays: "`This site is not secure. This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.`" If you know the site is secure, click **More information** then click **Go on to the webpage (not recommended)** to accept the certificate.
2. On the **One Identity Safeguard** login screen, perform the following:
    a. Enter a user name and password that has privileges to write to Safeguard. If the privileges do not include Asset Administrator, Security Policy Administrator, and User Administrator, the following error message displays: "`Sorry. You don't have sufficient rights to migrate TPAM.`"
    b. After entering valid login credentials, click **Log in**.
3. The **One Identity Migration Tool** page displays with the **Connection** tab selected so you can connect to TPAM.

a. Complete the following fields:

- **TPAM Network Address**: Enter the IP address of the TPAM machine to migrate.
- **TPAM User ID**: Enter the TPAM CLI user ID with ISA permissions to pull asset account passwords and pass them to Safeguard.
- **SSH Key**: TPAM authentication requires an SSH key. Click **Browse** and navigate to and select the SSH key file (for example, a .txt file).

b. Click **Connect**. If the connection is successful, the status of `Connected` displays.

4. Continue to Collecting data and starting the migration.

Collecting data and starting the migration

After the connection is made, you will select the entities (Systems/Accounts, Collections, and Users) to migrate, review the data, and then start the migration.

1. After the `Connected` status displays on the **Connection** tab, click **Select Data to Migrate**. The **Selection** tab displays.
2. On the **Selection** tab, select the entities to migrate from TPAM in the order you determined earlier (see Identify the order of migration).

   IMPORTANT: Do not migrate directory Assets and Accounts. After the migration, you can add them to Safeguard.

   If you select **Accounts/Systems**, you can migrate Account passwords or not:

   - Select **Include Passwords** to migrate the Account passwords.

     IMPORTANT: You must stop the password reset schedule on TPAM so account passwords are not reset by the schedule during the migration.

   - Leave **Include Passwords** clear to not include passwords in the migration. Later, you can perform another migration of Systems/Accounts and include the passwords or you can enter the passwords directly in Safeguard.
3. Once the selections are made, click **Collect Data**.

   The message "`Collecting data`" displays along with a the number of objects collected and the total objects (e.g. 2 of 7).

   When collection is complete, the following message displays: "`TPAM data collection complete.`" The number of records collected in the temporary database displays in parenthesis.
4. You can migrate all the data or select records to be migrated. To view and potentially select records:

a. Click ✎.

b. In the search field, enter characters to search all the fields and filter the results.

c. Select the records that you want to migrate to Safeguard, if any. If you do not select records, all the records will be migrated. To toggle between viewing selected records or all records, click **Show Only Selected** or **Show All**.

> IMPORTANT: Do not migrate users that are in TPAM and Safeguard because permissions will be modified, the password will be reset, and other problems may occur.

d. Click **Save**. The number of selected records and all records display in the parenthesis.

> NOTE: If you selected Systems, the number of accounts reflects the accounts for the selected Systems. For example, the collection may return 1000 Systems and 1300 accounts. If you select 300 of the 1000 Systems, there may be 500 accounts associated with the selected Systems.

5. Export the data to a .csv file to review the data details prior to starting the migration.

a. Click  to export all entities or individual entities, as applicable.

b. Save the file in the desired location. The .csv file name identifies the data is from TPAM (for example TPAM_Users_Export.csv).

c. Review the TPAM .csv data before starting the migration. For example, you will see that a disabled designation for a **Disabled** user in TPAM carries over to Safeguard. You will also see the time zones are matched or, if there is no match, the default assigned. Columns on the right pertaining to the migration will be populated after the migration (for example, **Is Valid** and **Is Exported**).

6. When the data is ready to migrate, click **Start Migration**.

7. This message displays: "`Overwrite data? Would you like to overwrite previously migrated data.`" Click **Yes** to overwrite the data or click **No** to migrate only data that is not already in Safeguard.

   During the migration, this message displays: "`Migrating data to Safeguard...`".

   > IMPORTANT: Do not exit the migration tool. If you exit, the migration will stop and partial data may be migrated. If you do exit, you will need to start the migration again and overwrite existing Safeguard data.

   When the migration data is ready for your review, this message displays "`Migration Complete.`" The number in parenthesis is the total migrated and the second represents all the records originally collected from TPAM. The bar represents the number of successful records (green), overwritten (yellow), and failed (red).

8. When the migration processing is done, continue to Reviewing data and finishing the migration.

Reviewing data and finishing the migration

In the previous steps, the data was migrated from the temporary database to Safeguard for Privileged Passwords and this message displayed: "`Migration Complete.`" Next, review the migration result, save passwords, and finish the migration.

1. Click to see the following information:
    - The first line shows the number of total records, records successfully migrated, failures, and records over-written.
    - The following icons show the results for each record.

✓	Success: The data has been migrated to Safeguard.
⊗	Failure: The data did not migrate to Safeguard.
⚠	Overwritten: The data overwrote existing Safeguard data.

2. Export the data to a .csv file to review the data details and migration process information.
    a. Click to export all entities or individual entities, as appropriate.
    b. Save the file in the desired location. The .csv file name identifies the data is from Safeguard (for example SGUsers_Export.csv).
    c. Review the .csv data file before finishing the migration. In addition to all the records migrated from TPAM to Safeguard, the columns on the right display migration information, including passwords. The order of the fields (below) may be slightly different based on the entity you selected.
        - **Is Valid** is **TRUE** if the data is valid per the checks or **FALSE** if, for example, there is an error mapping data.
        - **Is Exported** is **TRUE** if the data was exported to Safeguard or **FALSE** if the data was not exported.
        - **Is Already Exists** is **FALSE** if the data was not in Safeguard or **TRUE** if the data was in Safeguard at the time of migration.
        - **Is Selected** is **TRUE** for each record selected for migration by the user (or System if all records are migrated) and **FALSE** for records not selected.
        - **Error Message** describing any errors encountered in the migration.
        - **Is Failed** is **FALSE** if there is no error message or **TRUE** if there is an error message.
        - **Password** lists the generated user passwords.

d. Save the .csv file so the Administrator can supply the generated passwords to the users, as needed.

   IMPORTANT: The password information is not retained after you complete the next step so the .csv file must be saved now.

3. To finish the migration, click **Done** on the **One Identity Migration Tool** page.
4. This message reminds you to export the .csv file displays: "`Export Data. Would you like to export any migration data before finishing? User password information won't be retained after closing.`" If you have saved the migration .csv file, click **No** to finish the migration.

   You are returned to the **Connection** tab. You can start another migration, if desired. Or, you can sign out or close the utility.

4

Post migration activities

After the migration, Administrators may have activities to complete based on migration decisions and organizational procedures. The list that follows offers considerations for post migration activities.

- Users
  - Permissions: The migration utility set user permissions to defaults. If necessary, change the defaults after the migration for users and groups.
  - Passwords: Distribute the randomly generated user passwords collected in the .csv file, as needed.
- Assets (Systems in TPAM)
  - Asset account passwords: If the passwords were not migrated, set up passwords in Safeguard.
  - Directory assets or accounts: Use the Safeguard wizard to add directory assets and accounts to Safeguard.
  - Partitions: All migrated assets are placed in Safeguard's default partition profile. Change partitions, as necessary. TPAM partition data (including Users, Assets, Accounts, and so on) may need to be added to Safeguard.
  - Operating system platforms: Check the operating systems to ensure matches identified as "other" are assigned correctly in Safeguard.
- Services and configurations the Administrators may want to consider adding or updating in Safeguard after the migration follow:
  - Access policy data
  - Account discovery
  - Affinity data
  - Archive servers / logs
  - Authentication services
  - Batch processing
  - Custom platforms
  - File or file group data
  - Generic integration

- ISA policy
- LDAP integration
- Messages of the day
- Password cache
- Password check and change profiles
- PSM connection profiles
- PSM connection profiles data
- Reporting data
- Research
- Restricted commands / management
- Schedulers or jobs
- Schedules
- Session logs data
- Session(s) data
- Templates
- Ticketing system
- Users that are not local (for example, externally primary authenticated users)

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product