One Identity Manager 8.1

Administration Guide for Privileged Account Governance

Contents

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Administration Guide for Privileged Account Governance
Updated - March 2019
Version - 8.1

1

Mapping a Privileged Account Management system in One Identity Manager

One Identity Manager offers simplified user account administration for a Privileged Account Management system. One Identity Manager concentrates on setting up and editing user accounts and assigning the user accounts to user groups. Via their user groups, the user accounts receive the required entitlements, for example, for requesting a password for an asset account or a session for the accounts and assets in the Privileged Account Management system. The assignment of entitlements to user groups is performed in Privileged Account Management and not in the One Identity Manager. User groups and requests for passwords and sessions can be requested via the Web Portal.

One Identity Manager provides company employees with the necessary user accounts. For this, you can use different mechanisms to connect employees to their user accounts. You can also manage user accounts independently of employees and therefore set up administrator user accounts.

The user accounts, user groups, assets, asset groups, accounts, account groups, directories, entitlements, and access request policies of a Privileged Account Management systems are mapped in One Identity Manager. These objects are imported into the One Identity Manager database during synchronization. This makes it possible to use Identity and Access Governance processes such as attesting, identity audit, user account management and system entitlements, IT Shop, or report subscriptions for Privileged Account Management systems.

Architecture overview

To access the data of a Privileged Account Management system, a connector for the Privileged Account Management system is installed on a synchronization server. The synchronization server ensures data is compared between the One Identity Manager database and the Privileged Account Management system.

One Identity Manager supports synchronization with One Identity Safeguard. The One Identity Safeguard connector of the One Identity Manager uses Windows PowerShell for communication with the One Identity Safeguard appliance.

One Identity Manager Users for managing a Privileged Account Management system

The following users are included in setting up and managing a Privileged Account Management system.

Table 1: User

User	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Privileged account management** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop.

User	Tasks
	• Can create employees with an identity that differs from the **Primary identity**. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required. • Authorize employees as owners of privileged objects within their area of responsibility.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in Designer as required. • Create system users and permissions groups for non-role-based login to administration tools in Designer as required. • Enable or disable additional configuration parameters in Designer as required. • Create custom processes in Designer as required. • Create and configures schedules as required. • Create and configure password policies as required.
Product owner for the IT Shop	Product owners must be assigned to the **Request & Fulfillment | IT Shop | Product owner** application role or a child application role. Users with this application role: • Approve through requests. • Edit service items and service categories under their management.
Owners of privileged objects	The owners of privileged objects such as PAM assets, PAM asset accounts, or PAM directory accounts must be assigned to an application role under the application role **Privileged Account Governance | Asset and account owners**. Users with this application role: • Make decisions on the requesting of access requirements for privileged objects. • Attest the possible user access to these privileged objects

Configuration parameters

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. You can find an overview of all configuration parameters in **Base data | General | Configuration parameters** in Designer.

For more information, see Appendix: Configuration parameters for the management of a Privileged Account Management system on page 146.

2

Synchronizing a Privileged Account Management system

One Identity Manager supports synchronization with One Identity Safeguard version 2.5.

One Identity Manager is responsible for synchronizing data between the One Identity Safeguard database and the One Identity Manager Service appliance.

This sections explains:

- how to set up synchronization to import initial data from a One Identity Safeguard appliance to the One Identity Manager database,
- how to adjust a synchronization configuration, for example, to synchronize different One Identity Safeguard appliances with the same synchronization project,
- how to start and deactivate the synchronization,
- how to evaluate the synchronization results.

TIP: Before you set up synchronization with a One Identity Safeguard appliance, familiarize yourself with the Synchronization Editor. For detailed information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Setting up the initial synchronization with One Identity Safeguard on page 13
- Adjusting the synchronization configuration for One Identity Safeguard on page 26
- Executing a synchronization on page 33
- Error analysis on page 39
- Appendix: Editing One Identity Safeguardsystem objects on page 149

Setting up the initial synchronization with One Identity Safeguard

The Synchronization Editor provides a project template that can be used to set up the synchronization of user accounts and permissions for a target system environment. In addition, the required processes are created that are used for the provisioning of changes to target system objects from the One Identity Manager database into the target system.

Use the **One Identity Safeguard synchronization** project template to create synchronization projects with which you import the data from a One Identity Safeguard appliance into your One Identity Manager database.

To load objects into the One Identity Manager database for the first time

1. Prepare a user with sufficient permissions for synchronization in the Privileged Account Management system.
2. One Identity Manager components for managing Privileged Account Management systems are available if the **TargetSystem | PAG** configuration parameter is enabled.
    - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with a One Identity Safeguard appliance on page 14
- Setting up the One Identity Safeguard synchronization server on page 15
- Preparing the administrative workstation for access to the One Identity Safeguard appliance on page 19
- Preparing a remote connection server for access to the One Identity Safeguard appliance on page 20
- Creating a synchronization project for initial synchronization of a One Identity Safeguard appliance on page 21
- Appendix: Configuration parameters for the management of a Privileged Account Management system on page 146
- Appendix: Default project template for One Identity Safeguard on page 148

Users and permissions for synchronizing with a One Identity Safeguard appliance

The following users are involved in synchronizing One Identity Manager with a One Identity Safeguard appliance.

Table 2: Users for synchronization

User	Permissions

Users for accessing the One Identity Safeguard appliance (synchronization users)	On the appliance, you must provide a user account with the following settings for full synchronization of One Identity Safeguard appliance objects with the supplied One Identity Manager default configuration.
	• Authentication provider **Certificate**
	• Fingerprint of a certificate saved on the appliance as a trusted certificate
	• Permissions:
	  • Authorizer
	  • User
	  • Help Desk
	  • Appliance
	  • Operations
	  • Asset
	  • Directory
	  • Security policy
	For more detailed information about users and certificates in One Identity Safeguard, refer to the *One Identity Safeguard Administration Guide*.

One Identity Manager Service user account	The user account for One Identity Manager Service requires access rights to carry out operations at file level, for example, assigning user rights and creating and editing directories and files. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user right The user account requires access rights to the internal web service. The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.

User	Permissions
	In the default installation the One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems) In the certificate store of the current user, the user account requires the certificate with the private key that is saved on the One Identity Safeguard appliance as a trusted certificate. The certificate must be the same certificate used by the synchronization user. For more detailed information about certificates in One Identity Safeguard, refer to the *One Identity Safeguard Administration Guide*. NOTE: Access via the local system account **NT AUTHORITY\SYSTEM** is not supported.
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided for executing synchronization with an application server.

Setting up the One Identity Safeguard synchronization server

All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.

The One Identity Manager Service with the One Identity Safeguard connector must be installed on the synchronization server.

Detailed information about this topic

- System requirements for the One Identity Safeguard synchronization server on page 16
- Installing One Identity Manager Service with One Identity Safeguard connector on page 16

System requirements for the One Identity Safeguard synchronization server

To set up synchronization with a One Identity Safeguard appliance, a server must be available on which the following software is installed:

- Windows operating system

  Following versions are supported:

  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- Microsoft .NET Framework Version 4.7.2 or later

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows PowerShell version 5 or later
- Windows PowerShell module `safeguard-ps`

  Copy the folder `safeguard-ps` from the `Modules\PAG\dvd\AddOn` directory of the installation medium to the `%ProgramFiles%\WindowsPowerShell\Modules` directory on the server.

Installing One Identity Manager Service with One Identity Safeguard connector

The One Identity Manager Service with the One Identity Safeguard connector must be installed on the synchronization server. The synchronization server must be known as a Job server in the One Identity Manager.

Table 3: Properties of the Job server

Property	Value
Server function	One Identity Safeguard connector
Machine role	Server | Job server | Privileged Account Management

NOTE: If several target system environments of the same type are synchronized under the same synchronization server, it is useful to set up a Job server for each target system on performance grounds. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

Use the Server Installer to install the One Identity Manager Service. The program executes the following steps:

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of One Identity Manager Service components corresponding to the machine roles.
- Configuration of One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.

For remote installation of One Identity Manager Service, you require an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

To install and configure One Identity Manager Service remotely on a server

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the **Database connection** page.
3. Specify the server on which you want to install One Identity Manager Service on the **Server properties** page.
   a. Select a Job server from the **Server** menu.

      - OR -

      To create a new Job server, click **Add**.

   b. Enter the following data for the Job server.

Table 4: Job Server Properties

Property	Description
Server	Job server name.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of servers>.<Fully qualified domain name>`

NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with Designer.

4. Select **Privileged Account Management** on the **Machine roles** page.
5. Select **One Identity Safeguard connector** on the **Server functions** page.
6. Check the One Identity Manager Service configuration on the **Service settings** page.

   NOTE: The initial service configuration is predefined already. If further changes need to be made to the configuration, you can do this later with the Designer. For detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on **Select installation source**.
10. Select the file with the private key on the page **Select private key file**.

    NOTE: This page is only displayed when the database is encrypted.

11. Enter the service's installation data on the **Service access** page.

Table 5: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server*** • Enter a name for the server. - OR - • Select a entry from the list.
Service account	User account data for the One Identity Manager Service. ***To enter a user account for the One Identity Manager Service*** • Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** • Enable **Advanced**. • Enable **Current user**. This uses the user account of the current user.

Data	Description
	- OR - • Enter user account, password and password confirmation.

12. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.

13. Click **Finish** on the last page of Server Installer.

    NOTE: The service is entered with the name **One Identity Manager Service** in the server service management.

Preparing the administrative workstation for access to the One Identity Safeguard appliance

To configure synchronization with a One Identity Safeguard appliance in Synchronization Editor, One Identity Manager must load the data directly from the appliance. If the appliance is accessed directly from the work station on which the Synchronization Editor is installed, the following software must also be installed on this workstation:

- Windows PowerShell version 5 or later
- Windows PowerShell module `safeguard-ps`

  Copy the folder `safeguard-ps` from the `Modules\PAG\dvd\AddOn` directory of the installation medium to the `%ProgramFiles%\WindowsPowerShell\Modules` directory on the server.

In the certificate store of the user logged on to the administrative workstation, the user account requires the certificate with the private key that is saved on the One Identity Safeguard appliance as a trusted certificate. The certificate must be the same certificate used by the synchronization user. For more detailed information about certificates in One Identity Safeguard, refer to the *One Identity Safeguard Adminstration Guide*.

If direct access from the workstation to the appliance is not possible, you can set up a remote connection.

Related Topics

- Users and permissions for synchronizing with a One Identity Safeguard appliance on page 14
- Preparing a remote connection server for access to the One Identity Safeguard appliance on page 20

Preparing a remote connection server for access to the One Identity Safeguard appliance

To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection.

The remote connection server and the workstation must be in the same Active Directory domain.

Remote connection server configuration:

- One Identity Manager Service is started
- `RemoteConnectPlugin` is installed
- Windows PowerShell version 5 or above is installed
- Windows PowerShell module `safeguard-ps` is installed

  Copy the `safeguard-ps` folder from the `Modules\PAG\dvd\AddOn` directory of the installation medium to the `%ProgramFiles%\WindowsPowerShell\Modules` directory on the server.
- One Identity Safeguard connector is installed

The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements and user account certificate). Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well.

For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related Topics

- Setting up the One Identity Safeguard synchronization server on page 15
- Users and permissions for synchronizing with a One Identity Safeguard appliance on page 14
- Preparing the administrative workstation for access to the One Identity Safeguard appliance on page 19

Creating a synchronization project for initial synchronization of a One Identity Safeguard appliance

Use the Synchronization Editor to configure synchronization between the One Identity Safeguard database and a One Identity Manager appliance. The following describes the steps for initial configuration of a synchronization project. For more detailed information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

After the initial configuration, you can customize and configure workflows within the synchronization project. Use the workflow wizard in the Synchronization Editor for this. The Synchronization Editor also provides different configuration options for a synchronization project.

Related Topics

- Information required for setting up a synchronization project on page 21
- Creating an initial synchronization project for One Identity Safeguard on page 22
- Preparing the administrative workstation for access to the One Identity Safeguard appliance on page 19
- Preparing a remote connection server for access to the One Identity Safeguard appliance on page 20

Information required for setting up a synchronization project

Have the following information available for setting up a synchronization project.

Table 6: Information Required for Setting up a Synchronization Project

Data	Explanation
Appliance hostname or IP	Host name or IP address of the One Identity Safeguard appliance.
Trusted certificate thumbprint	Fingerprint of the trusted certificate that is used by the synchronization user and the user account of the One Identity Manager Service. For more information, see Users and permissions for synchronizing with a One Identity Safeguard appliance on page 14.
Synchronization server for the appliance	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity

Data	Explanation
	Manager database are processed by the synchronization server. The One Identity Manager Service with the One Identity Safeguard connector must be installed on the synchronization server. **Table 7: Additional properties for the Job server** **Property** / **Value** Server function: One Identity Safeguard connector Machine role: Server | Job server | Privileged Account Management For more information, see System requirements for the One Identity Safeguard synchronization server on page 16.
One Identity Manager database connection data	• Database server • Database • SQL Server Login and password • Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	For more information, see Preparing a remote connection server for access to the One Identity Safeguard appliance on page 20.

Creating an initial synchronization project for One Identity Safeguard

NOTE: The following sequence describes how you configure a synchronization project if Synchronization Editor is both:

- executed In default mode, and
- started from the launchpad

If you execute the project wizard in expert mode or directly from Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.

To set up an initial synchronization project for One Identity Safeguard

1. Start the Launchpad and log on to the One Identity Manager database.

   NOTE: If synchronization is executed by an application server, connect the database through the application server.

2. Specify how One Identity Manager can access the target system on the **System access** page.
   - If access is possible from the workstation on which you started Synchronization Editor, you do not need to make any settings.
   - If access is not possible from the workstation on which you started Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.

3. On the **Connection parameters** page, enter the following information:
   - **Appliance hostname or IP**: Enter the host name or IP address of the appliance.
   - **Trusted certificate thumbprint**: Enter the fingerprint of the trusted certificate used by the synchronization user and by the user account of One Identity Manager Service.
   - **Ignore SSL connection errors**: You should only activate this option for test purposes, because this may lead to potential trusting of insecure connections.
   - Click **Test connection data** to test the connection. The system tries to establish a connection to the appliance.

4. You can save the connection data on the last page of the system connection wizard.
   - Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
   - Click **Finish**, to end the system connection wizard and return to the project wizard.

5. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not shown if a synchronization project already exists.

6. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.

7. On the **Restrict target system access** page, you specify how system access should work. You have the following options:

Table 8: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**. • Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the **Target system**. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the **Target system**. • Synchronization steps are only created for such schema classes whose schema types have write access.

8. Select the synchronization server to execute synchronization on the **Synchronization server** page.

   If the synchronization server is not declared as a Job server in the One Identity Manager database yet, you can add a new Job server.

   a. Click to add a new Job server.

   b. Enter a name for the Job server and the full server name conforming to DNS syntax.

   c. Click **OK**.

      The synchronization server is declared as Job server for the target system in the One Identity Manager database.

      NOTE: After you save the synchronization project, ensure that this server is set up as a synchronization server.

9. To close the project wizard, click **Finish**.

   This creates and allocates a default schedule for regular synchronization. Enable the schedule for regular synchronization.

   The synchronization project is created, saved and enabled immediately.

   NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

   NOTE: The connection data for the target system is saved in a variable set and can be modified under **Configuration | Variables** in Synchronization Editor.

Related Topics

- Users and permissions for synchronizing with a One Identity Safeguard appliance on page 14
- Setting up the One Identity Safeguard synchronization server on page 15
- Configuring the synchronization log on page 25
- Adjusting the synchronization configuration for One Identity Safeguard on page 26
- Appendix: Default project template for One Identity Safeguard on page 148

Configuring the synchronization log

All the information, tips, warnings, and errors that occur during synchronization are recorded in the synchronization log. You can configure the type of information to record separately for each system connection.

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the category **Configuration | Target system** in Synchronization Editor.

   - OR -

   To configure the synchronization log for the database connection, select **Configuration | One Identity Manager connection** in Synchronization Editor.
2. Select the **General** view and click **Configure**.
3. Select the **Synchronization log** view and set **Create synchronization log**.

4. Enable the data to be logged.

   NOTE: Some content generates a particularly large volume of log data!

   The synchronization log should only contain data required for error analysis and other analyses.

5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In Designer, enable the **DPR | Journal | LifeTime** configuration parameter and enter the maximum retention period.

Related Topics

- Show synchronization results on page 34

Adjusting the synchronization configuration for One Identity Safeguard

You have used the Synchronization Editor to set up a synchronization project for initial synchronization of a One Identity Safeguard appliance. You can use this synchronization project to load PAM objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Privileged Account Management system.

NOTE: If you want to change the configuration of existing synchronization projects, check the possible effects of these changes on the data that has already been synchronized.

Adjust the synchronization configuration in order to reconcile the One Identity Safeguard appliance on a regular basis and to synchronize changes.

- To use One Identity Manager as the master system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- To specify which PAM objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing methods, for example.

- Use variables to set up a synchronization project for the synchronization of multiple appliances. Save the connection parameters for logging on to the appliance as variables.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

For detailed information about configuring synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Configuring synchronization to a One Identity Safeguard appliance on page 27
- Configuring synchronization of multiple One Identity Safeguard appliances on page 28
- Updating schemas on page 28
- Configuring the provisioning of memberships on page 30
- Configuring single object synchronization on page 31
- Adjusting the Windows PowerShell definition of the One Identity Safeguard connector on page 32

Configuring synchronization to a One Identity Safeguard appliance

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the master system during synchronization, you also require a workfow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing to the appliance

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   Creates a workflow with **Target system** as its synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related Topics

- Configuring synchronization of multiple One Identity Safeguard appliances on page 28

Configuring synchronization of multiple One Identity Safeguard appliances

In some circumstances, it is possible to use a synchronization project to synchronize multiple appliances.

Prerequisites

- The target system schemas of the appliances are identical.
- All virtual schema properties used in the mapping must exist in the extended schemas of the appliances.
- The connection parametes to the target system are defined as variables.

To customize a synchronization project for synchronizing another appliance

1. Set up a user with sufficient permissions in the additional appliance.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the appliance. Use the wizards to attach a base object.
    - In the wizard, select the One Identity Safeguard connector and declare the connection parameters. The connection parameters are saved in a special variable set.

      A start up configuration is created, which uses the newly created variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related Topics

- Configuring synchronization to a One Identity Safeguard appliance on page 27

Updating schemas

All the schema data (schema types and schema properties) of the target system schema and the One Identity Manager schema are available when you are editing a synchronization project. Only a part of this data is really needed for configuring synchronization. If a synchronization project is finished, the schema is compressed to remove unnecessary data from the synchronization project. This can speed up loading the synchronization project.

Deleted schema data can be added to the synchronization configuration again at a later point.

If the target system schema or the One Identity Manager schema has changed, these changes must also be added to the synchronization configuration. Then the changes can be added to the schema property mapping.

To include schema data that have been deleted through compressing and schema modifications in the synchronization project, update each schema in the synchronization project. This may be necessary if:

- A schema was changed by:
  - Changes to a target system schema
  - Customizations to the One Identity Manager schema
  - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
  - enabling the synchronization project
  - saving the synchronization project for the first time
  - compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target systems**.

   - OR -

   Select the category **Configuration | One Identity Manager connection**.
3. Select the view **General** and click **Update schema**.
4. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Mappings**.
3. Select a mapping in the navigation view.

   Opens the Mapping Editor. For more detailed information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

NOTE: The synchronization is deactivated if the schema of an activated synchronization project is updated. Reactivate the synchronization project to synchronize.

Speeding up synchronization with revision filtering

Synchronization with a One Identity Safeguard appliance does not support revision filtering.

Configuring the provisioning of memberships

Memberships, for example, user accounts in groups, are saved in assignment tables in the One Identity Manager database. During provisioning of modified memberships, changes made in the target system will probably be overwritten. This behavior can occur under the following conditions:

- Memberships are saved in the target system as an object property in list form (Example: List of users in the `Users` property of a PAM user group (`UserGroup`)).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; previously deleted memberships are added again.

To prevent this, provisioning can be configured such that only the modified membership is provisioned in the target system. The corresponding behavior is configured separately for each assignment table.

To allow separate provisioning of memberships

1. In the Manager, select **Privileged Account Management | Basic configuration data | Target system types**.
2. Select **Privileged Account Management** in the result list.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - This option can only be enabled for assignment tables that have a base table with `XDateSubItem` or `CCC_XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Enable merging**.
6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target

system is compared to the entries in this table. This means that only modified memberships are provisioned and the members list does not get entirely overwritten.

NOTE: The complete members list is updated by synchronization. During this process, objects with changes but incomplete provisioning are not handled. These objects are logged in the synchronization log.

For detailed information about provisioning memberships, see the *One Identity Manager Target System Synchronization Reference Guide*.

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a member list is belongs to one of these properties, then the entries in the allocation table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

- A synchronization step exists that can import the changes to the changed object into One Identity Manager.
- The path to the base object of the synchronization is defined for the table that contains the changed object.

Single object synchronization is fully configured for synchronization projects created using the default project template. If you want to incorporate custom tables into this type of synchronization project, you must configure single object synchronization for these tables. For detailed information, see *One Identity Manager Target System Synchronization Reference Guide*.

To define the path to the base object for synchronization for a custom table

1. In the Manager, select **Privileged Account Management | Basic configuration data | Target system types**.
2. In the result list, select the target system type **Privileged Account Management**.
3. Select **Assign synchronization tables**.
4. In **Add assignments**, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select **Configure tables for publishing**.
7. Select the custom table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

Example: `FK(UID_PAGAppliance).XObjectKey`

8. Save the changes.

Related Topics

- Synchronizing single objects on page 35
- Post-processing outstanding objects on page 36

Adjusting the Windows PowerShell definition of the One Identity Safeguard connector

You can use this setting to adjust the definition used by the One Identity Safeguard connector.

IMPORTANT: You should only make changes to the connector definition with the help of support desk staff. Changes to this setting will have wide ranging effects on synchronization and must be made carefully.

NOTE: A customized connection definition is not overwritten by default and must be made with careful consideration.

To customize the connector definition

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target systems**.
3. Click **Edit connection**.

   This starts the system connection wizard.
4. Enable **Show advanced options** on the system connection wizard's start page.
5. Customize the connector definition as required on the **Advanced options** page.
   a. Select **Customize connector definition**.
   b. Edit the definition according to the instructions given by the support desk staff. You take the following action:
      - Choose to load the definition from a file.
      - Use to test the definition for errors.
      - Choose to display the differences to the standard version.
6. Save the changes.

Executing a synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization was terminated unexpectedly, you must reset the start information to be able to restart synchronization.

Detailed information about this topic

- Starting synchronizations on page 33
- Deactivating synchronization on page 35
- Show synchronization results on page 34
- Synchronizing single objects on page 35

Starting synchronizations

When setting up the initial synchronization project using the Launchpad, a default schedule for regular synchronizations is created and assigned. To execute regular synchronizations, activate this schedule.

To synchronize on a regular basis

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Start up configurations**.
3. Select a start up configuration in the document view and click **Edit schedule**.
4. Edit the schedule properties.
5. To enable the schedule, click **Activate**.
6. Click **OK**.

You can also start synchronization manually if there is no active schedule.

To start initial synchronization manually

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Start up configurations**.
3. Select a start up configuration in the document view and click **Execute**.
4. Confirm the security prompt with **Yes**.

IMPORTANT: As long as synchronization is running, you must not start another synchronization for the same target system. This applies especially, if the same synchronization objects would be processed.

- If another synchronization is started with the same start up configuration, this process is stop and is assigned the **Frozen** execution status. An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration. Group start up configurations with the same start up behavior.

Show synchronization results

Synchronization results are summarized in the synchronization log. You can specify the extent of the synchronization log for each system connection individually. One Identity Manager provides several reports in which the synchronization results are organized under different criteria.

To display a synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. Select **Logs**.
3. Click ▶ in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking on it.

   An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log.

1. Open the synchronization project in the Synchronization Editor.
2. Select **Logs**.
3. Click ⚡ in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking on it.

   An analysis of the provisioning is show as a report. You can save the report.

The log is marked in color in the navigation view. This mark shows you the execution status of the synchronization/provisioning.

Related Topics

- Configuring the synchronization log on page 25
- Error analysis on page 39

Deactivating synchronization

Regular synchronization cannot be started until the synchronization project and the schedule are active.

To prevent regular synchronization

1. Open the synchronization project in the Synchronization Editor.
2. Select the start up configuration and deactivate the configured schedule.

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited extend. The schema in the synchronization project must be updated if schema modifications are required. The synchronization project is deactivated in this case and can be edited again.

Furthermore, the synchronization project must be deactivated if synchronization should not be started by any means (not even manually).

To deactivate the synchronization project

1. Open the synchronization project in the Synchronization Editor.
2. Select **General** on the start page.
3. Click **Deactivate project**.

Synchronizing single objects

Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a member list is belongs to one of these properties, then the entries in the allocation table will also be updated.

NOTE: If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

To synchronize a single object

1. In Manager, select the **Privileged Account Management** category.
2. Select the object type in the navigation view.
3. In the result list, select the object that you want to synchronize.
4. Select **Synchronize this object**.

   A process for reading this object is entered in the job queue.

NOTE: The **Synchronize this object** task is executed for the object selected in the results list. If you want to synchronize changes to memberships, execute the single object synchronization on the base object of the assignment.

Example:

The base table of an assignment contains an `XDateSubItem` column containing information about the last change to the memberships.

Detailed information about this topic

- Configuring single object synchronization on page 31

Tasks after a synchronization

After the synchronization of data from the target system into the One Identity Manager database, rework may be necessary. Check the following tasks:

- Post-processing outstanding objects on page 36
- Adding custom tables to the target system synchronization on page 38
- Managing PAM user accounts through account definitions on page 39

Post-processing outstanding objects

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Outstanding objects

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

To post-process outstanding objects

1. In the manager, select the **Privileged Account Management | Target system synchronization: Privileged Account Management** category.

   All tables assigned to the target system type **Privileged Account Management** as synchronization tables are displayed in the navigation view.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

   All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was executed. The **No log available** entry can mean the following:

   - The synchronization log has already been deleted.

     - OR -

   - An assignment from a member list has been deleted in the target system.

     The base object of the assignment has been updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

   - An object that contains a member list has been deleted in the target system.

     During synchronization, the object and all corresponding entries in assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.

   TIP:

   To display object properties of an outstanding object

   a. Select the object on the target system synchronization form.

   b. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.
4. Click one of the following icons in the form toolbar to execute the respective method.

Table 9: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted in the One Identity Manager database. Deferred deletion is not taken into account. The **Outstanding** label is removed for the object. Indirect memberships cannot be deleted.
	Publish	The object is added in the target system. The **Outstanding** label is removed for the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target

Icon	Method	Description
		system.
	Reset	The **Outstanding** label is removed for the object.

5. Confirm the security prompt with **Yes**.

NOTE: By default, the selected objects are processed in parallel, which speeds up execution of the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.

Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.

To disable bulk processing

- Deactivate in the form toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. This means that the **Connection is read only** option is not set in the target system connection.

Adding custom tables to the target system synchronization

You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization

1. In the result list, select the target system type **Privileged Account Management**.
2. Select **Assign synchronization tables**.
3. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
4. Save the changes.
5. Select **Configure tables for publishing**.
6. Select custom tables whose outstanding objects can be published in the target system and set **Publishable**.
7. Save the changes.

Related Topics

- Post-processing outstanding objects on page 36

Managing PAM user accounts through account definitions

Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the appliance is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

Detailed information about this topic

- Assigning account definitions to linked PAMuser accounts on page 64

Error analysis

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating Synchronization

  The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.

- Analyzing synchronization

  You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.

- Logging messages

  The One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.

- Reset start information

  If synchronization was terminated unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.

For more information about these topics, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related Topics

- Show synchronization results on page 34

3

Managing PAM user accounts and employees

The central component of One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems. One Identity Manager provides the possibility to manage user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

Because requirements vary between companies, One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in an appliance, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

  When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.
- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this procedure is not the default procedure for One Identity Manager. Define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

For detailed information about employee handling and administration, see the *One Identity Manager Target System Base Module Administration Guide*.

Related Topics

- Account definitions for PAM user accounts on page 41
- Automatic assignment of persons to PAM user accounts on page 59
- Editing master data for PAM user accounts on page 109

Account definitions for PAM user accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

Specify the manage level for an account definition for managing user accounts. The user account's manage level specifies the extent of the employee's properties that are inherited by the user account. This allows an employee to have several user accounts in one target system, for example:

- Default user account that inherits all properties from the employee
- Administrative user account that is associated to an employee but should not inherit the properties from the employee.

For more detailed information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Determining IT Operating Data
- Assigning account definitions to employees and target systems

Detailed information about this topic

- Creating account definitions on page 42
- Editing manage levels on page 45
- Creating mapping rules for IT operating data on page 47
- Entering IT operating data on page 49

- Assigning account definitions to employees on page 51
- Assigning account definitions to PAM appliances on page 56

Creating account definitions

To create a new account definition

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Click in the result list toolbar.
3. On the master data form, enter the master data for the account definition.
4. Save the changes.

Related Topics

- Master data for account definitions on page 42
- Editing account definitions on page 42

Editing account definitions

To edit an account definition

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data**.
4. Enter the account definition's master data.
5. Save the changes.

Related Topics

- Master data for account definitions on page 42
- Creating account definitions on page 42

Master data for account definitions

Enter the following data for an account definition:

Table 10: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts. For PAM users, select **PAGUser**.
Target system	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. For a PAM appliance, you can optionally select an Active Directory account definition or an LDAP account definition. In this case, an Active Directory or LDAP user account is first created for the employee. If this user account exists, the PAM user account is created as a directory user.
Description	Spare text box for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the configuration parameter **QER | CalculateRiskIndex** is activated. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can also be assigned directly to employees and roles outside of IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain

Property	Description
employees	this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: The account definition assignment remains in effect. The user account stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily disabled employees. Option set: The account definition assignment remains in effect. The user account stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: The account definition assignment remains in effect. The user account stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: The account definition assignment remains in effect. The user account stays the same. Option not set: The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the employee but they do no inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed**: User accounts with the **Full managed** manage level inherit defined properties of the assigned assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

To edit a manage level

1. In Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Manage levels.**
2. Select the manage level in the result list.
3. Select **Change master data**.
4. Edit the manage level's master data.
5. Save the changes.

Related Topics

- Master data for manage levels on page 46
- Creating manage levels on page 45

Creating manage levels

The One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

IMPORTANT: In Designer, extend the templates by adding the procedure for the additional manage levels. For detailed information about templates, see the *One Identity Manager Configuration Guide*.

To create a manage level

1. In Manager, select **Privileged Account Management| Basic configuration data | Account definitions | Manage levels.**
2. Click in the result list toolbar.

3. On the master data form, edit the master data for the manage level.
4. Save the changes.

Related Topics

- Master data for manage levels on page 46
- Editing manage levels on page 45

Master data for manage levels

Enter the following data for a manage level.

Table 11: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.
Description	Spare text box for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. • **Always**: Data is always updated. • **Only initially**: The data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.

Property	Description
Retain groups if user account disabled	Specifies whether locked user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the employee's primary roles.

The following IT operating data is used in the One Identity Manager default configuration for automatic creating and modifying of user accounts for an employee in the target system.

- PAM authentication provider
- Groups can be inherited
- Identity
- Privileged user account

To create a mapping rule for IT operating data

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.

3. Select **Edit IT operating data mapping** and enter the following data.

Table 12: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For detailed information, see *One Identity Manager Target System Base Module Administration Guide*.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: • Primary department • Primary location • Primary cost center • Primary business roles NOTE: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The **Employee - new user account with default properties created** mail template is used. To change the mail template, adjust the **TargetSystem | PAG | Accounts | MailTemplateDefaultValues** configuration parameter.

4. Save the changes.

Related Topics

- Entering IT operating data on page 49
- Modify IT operating data on page 50

Entering IT operating data

To create user accounts with the **Full managed** manage level, the required IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

You can also specify IT operating data directly for a specific account definition.

Example

Normally, each employee in department A obtains a default user account in the applianceA. In addition, certain employees in department A obtain administrative user accounts in the applianceA.

Create an account definition A for the default user account of the the appliance A and an account definition B for the administrative user account of appliance A. Specify the property "Department" in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

Specify the effective IT operating data of department A for the appliance A. This IT operating data is used for standard user accounts. In addition, specify the effective account definition B IT operating data for department A. This IT operating data is used for administrative user accounts.

To define IT operating data

1. In Manager, select the role in the **Organizations** or **Business roles** category.
2. Select **Edit IT operating data** in the task view and enter the following data.

Table 13: IT operating data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. ***To specify an application scope*** a. Click → next to the text box.

Property	Description
	b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table for an account definition. c. Select the specific target system or account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For detailed information, see *One Identity Manager Target System Base Module Administration Guide*.
Value	Concrete value which is assigned to the user account property.

3. Save the changes.

Related Topics

- Creating mapping rules for IT operating data on page 47
- Modify IT operating data on page 50

Modify IT operating data

If IT operating data changes, you must transfer these changes to the existing user accounts. To do this, templates must be rerun on the affected columns. Before you can run the templates, you can check what effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

Prerequisites

- The IT operating data of a department, cost center, business role, or a location was changed.

  - OR -

- The default values in the IT operating data template were modified for an account definition.

NOTE: If the assignment of an employee to a primary department, cost center business role or to a primary location changes, the templates are automatically executed.

To execute the template

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

Old value:	Current value of the object property.
New value:	Value that the object property would have following modification of the IT operating data.
Selection:	Specifies whether the modification shall be adopted for the user account.

4. Mark all the object properties in the **selection** column that will be given the new value.
5. Click **Apply**.

   The templates are applied to all selected user accounts and properties.

Assigning account definitions to employees

Account definitions are assigned to company employees.

Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations or roles. The employees are categorized into these departments, cost centers, locations or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees.

You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

NOTE: If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (department, cost center, location or business role).

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is deleted.

For detailed information about preparing role classes to be assigned, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning account definitions to business roles on page 53
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 54
- Adding account definitions in the IT Shop on page 55

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost centers** tab.

   TIP: In the **Remove assignments** area, you can remove the assignment of organizations.

   To remove an assignment

   - Select the organization and double click ✓.
5. Save the changes.

Assigning account definitions to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles**.
4. Assign business roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of business roles.

   To remove an assignment

   - Select the business role and double click .
5. Save the changes.

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data**.
4. Set **Automatic assignment to employees** on **General**.

   IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.
5. Save the changes.

The account definition is assigned to every employee that is not marked as external. New employees automatically obtain this account definition as soon as they are added. The assignment is calculated by the DBQueue Processor.

NOTE: Disable **Automatic assignment to employees** to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees**.
4. Assign employees in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of employees.

   To remove an assignment

   - Select the employee and double click ✓.
5. Save the changes.

Assigning account definitions to system roles

Installed modules: System Roles Module

NOTE: Account definitions with **Only use in IT Shop** can only be assigned to system roles that also have this option set.

To add account definitions to a system role

1. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles**.
4. Assign system roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of system roles.

   To remove an assignment

   - Select the system role and double click ✓.
5. Save the changes.

Adding account definitions in the IT Shop

A account definition can be requested by shop customers when it is assigned to an IT Shop shelf. To ensure it can be requested, further prerequisites need to be guaranteed.

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.

  TIP: In Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in Web Portal, assign a service category to the service item.

- If the account definition is only assigned to employees using IT Shop assignments, you must also set **Only for use in IT Shop**. Direct assignment to hierarchical roles may not be possible.

NOTE: IT Shop administrators can assign account definitions to IT Shop shelves if login is role-based. Target system administrators are not authorized to add account definitions in the IT Shop.

To add an account definition to the IT Shop

1. In Manager, select **Privileged Account Management | Account definitions** (role-based login).

   - OR -

   In Manager, select **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop**.
4. Assign the account definitions to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In Manager, select **Privileged Account Management | Account definitions** (role-based login).

   - OR -

   In Manager, select **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop**.
4. Remove the account definitions from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

1. In the Manager, select **Privileged Account Management| Account definitions** (with role-based login).

   - OR -

   In the Manager, select **Entitlements | Account definitions** (with role-based login).
2. Select an account definition in the result list.
3. Select **Remove from all shelves (IT Shop)**.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The account definition is removed from all shelves by One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

For detailed information about requesting company resources through IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related Topics

- Master data for account definitions on page 42

Assigning account definitions to PAM appliances

The following prerequisites must be fulfilled if you implement automatic assignment of user accounts and employees resulting in administered user accounts (state **Linked configured**):

- The account definition is assigned to the target system.
- The account definition has the default manage level.

User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.

To assign the account definition to a target system

1. In Manager, select the applicance in **Privileged Account Management | Appliances**.
2. Select **Change master data**.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

Related Topics

- Automatic assignment of persons to PAM user accounts on page 59
- Master data for manage levels on page 46

Deleting account definitions

You can delete account definitions if they are not assigned to target systems, employees, hierarchical roles or any other account definitions.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Change master data**.
    d. Disable **Automatic assignment to employees** on the **General** tab.
    e. Save the changes.
2. Remove direct assignments of the account definition to employees.
    a. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign to employees**.
    d. Remove employees from **Remove assignments**.
    e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
    a. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign organizations**.
    d. In **Remove assignments**, remove the relevant departments, cost centers, and locations.
    e. Save the changes.
4. Remove the account definition's assignments to business roles.
    a. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.

c. Select **Assign business roles**.

   Remove the business roles in **Remove assignments**.

d. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

   For more detailed information about unsubscribing requests, see the *One Identity Manager Web Portal User Guide*.

   To remove an account definition from all IT Shop shelves

   a. In the Manager, select **Privileged Account Management| Account definitions** (with role-based login).

      - OR -

      In the Manager, select **Entitlements | Account definitions** (with role-based login).

   b. Select an account definition in the result list.

   c. Select **Remove from all shelves (IT Shop)**.

   d. Confirm the security prompt with **Yes**.

   e. Click **OK**.

      The account definition is removed from all shelves by One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

   a. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.

   b. Select an account definition in the result list.

   c. Select **Change master data**.

   d. Remove the account definition in the **Required account definition** menu.

   e. Save the changes.

7. Remove the account definition's assignments to target systems.

   a. In Manager, select the applicance in **Privileged Account Management | Appliances**.

   b. Select **Change master data**.

   c. Remove the assigned account definitions on the **General** tab.

   d. Save the changes.

8. Delete the account definition.
    a. In the Manager, select **Privileged Account Management | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Click to delete an account definition.

Automatic assignment of persons to PAM user accounts

When you add a user account, an existing employee can be assigned automatically or added if necessary. In the process, the employee master data is created based for existing user master data. This mechanism can follow after a new user account has been created manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

If you run this procedure during working hours, automatic assignment of employees to user accounts takes place from that moment onwards. If you disable the procedure again later, the changes only affect user accounts added or updated after this point in time. Existing employee assignment to user accounts remain intact.

NOTE: It is not recommended to assign employees using automatic employee assignment in the case of administrative user accounts. Use **Change master data** to assign employees to administrative user account for the respective user account.

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, enable the configuration parameter **TargetSystem | PAG | PersonAutoFullsync** and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer activate the configuration parameter **TargetSystem | PAG | PersonAutoDefault** and select the required mode.
- In the **TargetSystem | PAG| PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to employees shall take place.

  Example:

  ```
  ADMINISTRATOR
  ```

- Use the configuration parameter **TargetSystem | PAG | PersonAutoDisabledAccounts** to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account

definition.

- Assign an account definition to the appliance. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employee assignment to this appliance.

NOTE:

The following applies for synchronization:

- Automatic employee assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:

- Automatic employee assignment takes effect if user accounts are added.

NOTE:

Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the appliance is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

For more information, see Managing PAM user accounts through account definitions on page 39.

For detailed information about assigning employees automatically, see the *One Identity Manager Target System Base Module Administration Guide*.

Related Topics

- Creating account definitions on page 42
- Assigning account definitions to PAM appliances on page 56
- Changing manage levels for PAM user accounts on page 63
- Editing search criteria for automatic employee assignment on page 60

Editing search criteria for automatic employee assignment

The criteria for employee assignment are defined for the appliance. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the **Search**

criteria for automatic employee assignment column (`AccountToPersonMatchingRule`) in the `PAGUser` table.

Search criteria are evaluated when employees are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly.

NOTE: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

It is not recommended to make assignment to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user account for the respective user account.

NOTE: One Identity Manager supplies a default mapping for employee assignment. Only carry out the following steps when you want to customize the default mapping.

To specify criteria for employee assignment

1. In Manager, select **Privileged Account Management | Appliances**.
2. Select the appliance in the result list.
3. Select **Define search criteria for employee assignment** in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

   Table 14: Standard search criteria for user accounts

Apply to	Column for employee	Column for user account
PAM user accounts (local users)	Central user account (`CentralAccount`)	User name (`UserName`)

5. Save the changes.

For detailed information about defining search criteria, see the *One Identity Manager Target System Base Module Administration Guide*.

Related Topics

- Automatic assignment of persons to PAM user accounts on page 59
- Finding employees and directly assigning them to user accounts on page 62

Finding employees and directly assigning them to user accounts

Based on the search criteria, you can create a suggestion list for the assignment of employees to user accounts and make the assignment directly. User accounts are grouped in different views for this.

Table 15: Manual Assignment View

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an employee is assigned.
Without employee assignment	This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.

To apply search criteria to user accounts

1. Select **Privileged Account Management | Appliances** in Manager.
2. In the result list, select the appliance.
3. Select **Define search criteria for employee assignment** in the task view.
4. At the bottom of the form click **Reload**.

   All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

TIP: By double-clicking on an entry in the view, you can view the user account and employee master data.

The assignment of employees to user accounts creates connected user accounts (status **Linked**). To create managed user accounts (status **Linked configured**), you can assign an account definition at the same time.

To assign employees directly over a suggestion list

- Click **Suggested assignments**.
  1. Click **Selection** for all user accounts to which you want to assign the suggested employees. Multi-select is possible.
  2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level**

menu.

3. Click **Assign selected.**
4. Confirm the security prompt with **Yes**.

   The employees determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

- OR -

- Click **No employee assignment**.
  1. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.
  2. Click **Selection** for all user accounts to which you want to assign the selected employees. Multi-select is possible.
  3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
  4. Click **Assign selected**.
  5. Confirm the security prompt with **Yes**.

     The employees displayed in the **Employee** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.
  1. Click **Selection** for all user accounts for which you want to delete the employee assignment. Multi-select is possible.
  2. Click **Remove selected**.
  3. Confirm the security prompt with **Yes**.

     The assigned employees are removed from the selected user accounts.

Changing manage levels for PAM user accounts

The default manage level is applied if you create user accounts using automatic employee assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.

4. On the **General** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

Related Topics

- General master data for PAM user accounts on page 109

Assigning account definitions to linked PAMuser accounts

An account definition can be subsequently assigned to user accounts with **Linked** status. This may be necessary, for example, if:

- employees and user accounts have been linked manually
- automatic employee assignment is configured, but an account definition is not yet assigned in the appliance when inserting a user account.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the appliance.
3. Assign the account definition and manage level to user accounts in **linked** status.
    a. In Manager, select **Privileged Account Management | User accounts | Linked but not configured | <Appliance>**.
    b. Select **Assign account definition to linked accounts**.

Detailed information about this topic

- Assigning account definitions to PAM appliances on page 56

Manually linking employees to PAM user accounts

An employee can be linked to multiple PAM user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One employee can also use default user accounts with different types.

NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

To manually assign user accounts to an employee

1. In Manager, select **Employees | Employees**.
2. Select the employee in the result list and run **Assign PAM user accounts** from the task view.
3. Assign the user accounts.
4. Save the changes.

Related Topics

- Supported user account types on page 65

Supported user account types

Different types of user accounts, such as default user accounts, administrative user accounts, service accounts, or privileged user accounts can be mapped in One Identity Manager.

The following properties are used for mapping different user account types.

- Identity

  The **Identity** property (`IdentityType` column) is used to describe the type of user account.

  Table 16: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.	Organizational
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account that is used for training purposes, for example.	Sponsored
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

The primary identity, the organizational identity, and the personal admin identity are used for different user accounts, which can be used by the same actual employee to execute their different tasks within the company.

To provide user accounts with a personal admin identity or an organizational identity for an employee, you create subidentities for the employee. These subidentities are then linked to user accounts, enabling you to assign the required Entitlements to the different user accounts.

User accounts with a sponsored identity, group identity, or service identity are linked to dummy employees that do not refer to a real person. These dummy employees are needed so that Entitlements can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether dummy employees need to be considered separately.

For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

- Privileged user account

  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column `IsPrivilegedAccount`).

Detailed information about this topic

- Default user accounts on page 66
- Administrative user accounts on page 67
- Providing administrative user accounts for one employee on page 68
- Providing administrative user accounts for multiple employees on page 69
- Privileged user accounts on page 70

Default user accounts

Normally, each employee obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the employee. The effect of the link and the scope of the employee's inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.

2. Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

   You use the mapping rule to define which rules are used to map the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined via a person's primary roles.

   Which IT operating data is required depends on the target system. The following setting are recommended for default user accounts:

   - In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable **Always use default value**.
   - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
5. Assign the account definition to employees.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

Related Topics

- Account definitions for PAM user accounts on page 41

Administrative user accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as **Administrator**.

Administrative user accounts are imported into One Identity Manager during synchronization.

NOTE: Some administrative user accounts can be automatically identified as privileged user accounts. To do this, enable the **Mark selected user accounts as privileged** schedule in Designer.

Related Topics

- Providing administrative user accounts for one employee on page 68
- Providing administrative user accounts for multiple employees on page 69

Providing administrative user accounts for one employee

Prerequisites

- The user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be linked to a main identity.

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
    a. In Manager, select **Privileged Account Management | User accounts**.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
2. Link the user account to the employee who will be using this administrative user account.
    a. In Manager, select **Privileged Account Management | User accounts**.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

        TIP: If you are the target system manager, you can choose to create a new person.

Related Topics

- Providing administrative user accounts for multiple employees on page 69
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for multiple employees

Prerequisite

- The user account must be labeled as a shared identity.
- A dummy employee must exist. The dummy employee must be labeled as a shared identity and must have a manager.
- The employees who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.
    a. In Manager, select **Privileged Account Management | User accounts**.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, in the **Identity** selection list, select **Shared identity**.
2. Link the user account to a dummy employee.
    a. In Manager, select **Privileged Account Management | User accounts**.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, select the dummy employee from the **Employee** selection list.

    TIP: If you are the target system manager, you can choose to create a new dummy employee.
3. Assign the employees who will use this administrative user account to the user account.
    a. In Manager, select **Privileged Account Management | User accounts**.
    b. Select the user account in the result list.
    c. Select the task **Assign employees authorized to use**.
    d. Assign employees in **Add assignments**.

    TIP: In the **Remove assignments** area, you can remove the assignment of employees.

    To remove an assignment

    - Select the employee and double click .

Related Topics

- Providing administrative user accounts for one employee on page 68
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column `IsPrivilegedAccount`).

NOTE: The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the `TSBVAccountIsPrivDetectRule` table (which is a table of the **Union** type). The evaluation is done in the script `TSB_SetIsPrivilegedAccount`.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts is created.
3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for IT operating data.

   You use the mapping rule to define, for example, which rules are used to map the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined via a person's primary roles.

   Which IT operating data is required depends on the target system. The following settings are recommended for privileged user accounts:

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and enable **Always use default value**.
   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
   - To prevent privileged user accounts from inheriting the Entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and enable **Always use default value**.

5. Enter the effective IT operating data for the target system.

   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

6. Assign the account definition directly to employees who work with privileged user accounts.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, create the template according to which the login names are formed.

Related Topics

- Account definitions for PAM user accounts on page 41

4

Managing the assignments of PAM user groups

To enable the requesting of, for example, a password for an asset account or a session for the accounts and assets in the Privileged Account Management system, users require the necessary entitlements. To simplify the administration, user accounts can be grouped into user groups. Via the user groups, user accounts receive the entitlements for requesting passwords or sessions.

In One Identity Manager, you can assign the user groups directly to the user accounts, or they can be inherited via departments, cost centers, locations, or business roles. Users can also request the user groups via the Web Portal. To do this, the user groups are provided in the IT Shop.

The assignment of entitlements to user groups is performed in Privileged Account Management and not in the One Identity Manager.

Detailed information about this topic

- Assigning PAM user groups to PAM user accounts in One Identity Manager on page 72
- Effects of PAM user group memberships on page 80
- Inheritance of PAM user groups based on categories on page 82
- Overview of all assignments on page 84

Assigning PAM user groups to PAM user accounts in One Identity Manager

In One Identity Manager, PAM user groups can be assigned directly or indirectly to user accounts.

In the case of indirect assignment, employees and PAM user groups are classified in hierarchical roles. The number of PAM user groups assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If the employee has a PAM user account, this PAM user account is assigned the PAM user groups.

User groups can also be requested in the Web Portal. To do this, add employees to a shop as customers. All PAM user groups that are assigned to this shop as products can be requested by the customers. Requested PAM user groups are assigned to the employees after approval is granted.

You can use system roles to group PAM user groups together and assign them to employees as a package. You can create system roles that contain only PAM user groups. System entitlements from different target systems can also be grouped together in a system role.

To react quickly to special requests, you can also assign the PAM user groups directly to PAM user accounts.

Prerequisites

- The assignment of employees and PAM user groups is permitted for departments, cost centers, locations, or business roles.
- PAM user accounts are labeled with **Groups can be inherited**.
- The PAM user accounts are linked to an employee.
- The PAM user accounts and PAM user groups belong to the same appliance.

For detailed information see the following guides:

Theme	Guide
Inheritance of company resources	*One Identity Manager Identity Management Base Module Administration Guide* *One Identity Manager Business Roles Administration Guide*
Assigning company resources via IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Assigning PAM user groups to departments, cost centers, and locations on page 74
- Assigning PAM user groups to business roles on page 75
- Adding PAM user groups to system roles on page 76
- Adding PAM user groups to the IT Shop on page 77
- Assigning PAM user accounts directly to a PAM user group on page 78
- Assigning PAM user groups directly to a PAM user account on page 79

Assigning PAM user groups to departments, cost centers, and locations

Assign the PAM user groups to departments, cost centers, or locations so that the PAM user group can be assigned to PAM user accounts through these organizations.

To assign a group to departments, cost centers or locations (non role-based login)

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select the group in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost centers** tab.

   TIP: In the **Remove assignments** area, you can remove the assignment of organizations.

   To remove an assignment

   - Select the organization and double click ✓.
5. Save the changes.

To assign groups to a department, cost center or location (role-based login)

1. Select **Organizations | Departments** in Manager.

   - OR -

   Select **Organizations | Cost centers** in Manager.

   - OR -

   In Manager, select **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign PAM user groups**.
4. Assign groups in **Add assignments**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

   - Select the group and double click ✓.
5. Save the changes.

Related Topics

- Assigning PAM user groups to business roles on page 75
- Adding PAM user groups to system roles on page 76
- Adding PAM user groups to the IT Shop on page 77
- Assigning PAM user accounts directly to a PAM user group on page 78
- Assigning PAM user groups directly to a PAM user account on page 79
- One Identity Manager Users for managing a Privileged Account Management system on page 9

Assigning PAM user groups to business roles

Installed modules: Business Roles Module

You assign the PAM user group to business roles, so that the PAM user group is assigned to PAM user accounts via these roles.

To assign a group to a business role (non role-based login)

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select the group in the result list.
3. Select **Assign business roles**.
4. Assign business roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of business roles.

   To remove an assignment

   - Select the business role and double click .
5. Save the changes.

To assign groups to a business role (non role-based login)

1. In Manager, select **Business roles | <role class>**.
2. Select the business role in the result list.
3. Select **Assign PAM user groups**.

   Assign groups in **Add assignments**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

   - Select the group and double click .

4. Save the changes.

Related Topics

- Assigning PAM user groups to departments, cost centers, and locations on page 74
- Adding PAM user groups to system roles on page 76
- Adding PAM user groups to the IT Shop on page 77
- Assigning PAM user accounts directly to a PAM user group on page 78
- Assigning PAM user groups directly to a PAM user account on page 79
- One Identity Manager Users for managing a Privileged Account Management system on page 9

Adding PAM user groups to system roles

Installed modules: System Roles Module

Use this task to add a group to system roles. If you assign a system role to employees, all the PAM user accounts belonging to these employees inherit the group.

NOTE: Groups with **Only use in IT Shop** set can only be assigned to system roles that also have this option set. For more detailed information, see the *One Identity Manager System Roles Administration Guide*.

To assign a group to system roles

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select the group in the result list.
3. Select **Assign system roles**.
4. Assign system roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of system roles.

   To remove an assignment

   - Select the system role and double click .
5. Save the changes.

Related Topics

- Assigning PAM user groups to departments, cost centers, and locations on page 74
- Assigning PAM user groups to business roles on page 75
- Adding PAM user groups to the IT Shop on page 77

- Assigning PAM user accounts directly to a PAM user group on page 78
- Assigning PAM user groups directly to a PAM user account on page 79

Adding PAM user groups to the IT Shop

When you assign a user group to a IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- The user group must be marked with the **IT Shop** option.
- The user group must be assigned a service item.

  TIP: In Web Portal, all products that can be requested are grouped together by service category. To make the user group easier to find in Web Portal, assign a service category to the service item.

- If you only want it to be possible for the user group to be assigned to employees through IT Shop requests, the user group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

NOTE: With role-based login, the IT Shop administrators can assign user groups to IT Shop shelves. Target system administrators are not authorized to add user groups to IT Shop.

To add a group a user groupto IT Shop.

1. In Manager, select **Privileged Account Management | User groups** (non-role-based login).

   - OR -

   In Manager, select **Entitlements | PAM user groups** (role-based login).
2. In the result list, selectthe user group.
3. Select **Add to** IT Shop.
4. In **Add assignments**the user group to the IT Shop shelves.
5. Save the changes.

To remove, a user group from individual shelves of the IT Shop

1. In Manager, select **Privileged Account Management | User groups** (non-role-based login).

   - OR -

   In Manager, select **Entitlements | PAM user groups** (role-based login).
2. In the result list, selectthe user group.
3. Select **Add to** IT Shop.

4. In **Remove assignments**, the user group from the IT Shop shelves.
5. Save the changes.

To remove, a user group from all shelves of the IT Shop

1. In Manager, select **Privileged Account Management | User groups** (non-role-based login).

   - OR -

   In Manager, select **Entitlements | PAM user groups** (role-based login).
2. In the result list, selectthe user group.
3. Select **Remove from all shelves (IT Shop)**.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The user group is removed from all shelves by the One Identity Manager Service. All requests and assignment requests withthis user group are canceled.

For detailed information about requesting company resources through IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related Topics

- General master data for PAM user groups on page 118
- Assigning PAM user groups to departments, cost centers, and locations on page 74
- Assigning PAM user groups to business roles on page 75
- Adding PAM user groups to system roles on page 76
- Assigning PAM user accounts directly to a PAM user group on page 78
- Assigning PAM user groups directly to a PAM user account on page 79

Assigning PAM user accounts directly to a PAM user group

To react quickly to special requests, you can assign groups directly to user accounts.

To assign a group directly to user accounts

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select the group in the result list.
3. Select **Assign user accounts**.

4. Assign user accounts in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of user accounts.

   To remove an assignment

   - Select the user account and double click ✓.

5. Save the changes.

Related Topics

- Assigning PAM user groups to departments, cost centers, and locations on page 74
- Assigning PAM user groups to business roles on page 75
- Adding PAM user groups to system roles on page 76
- Adding PAM user groups to the IT Shop on page 77
- Assigning PAM user groups directly to a PAM user account on page 79

Assigning PAM user groups directly to a PAM user account

To react quickly to special requests, you can assign groups directly to the user account.

To assign groups directly to user accounts

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Select **Assign groups**.
4. Assign groups in **Add assignments**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

   - Select the group and double click ✓.

5. Save the changes.

Related Topics

- Assigning PAM user groups to departments, cost centers, and locations on page 74
- Assigning PAM user groups to business roles on page 75
- Adding PAM user groups to the IT Shop on page 77

- Adding PAM user groups to system roles on page 76
- Assigning PAM user accounts directly to a PAM user group on page 78

Effects of PAM user group memberships

When groups are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually exclusive groups. To do this, you specify which of the two groups should apply to the user accounts if both are assigned.

It is possible to assign an excluded group directly, indirectly or by IT Shop request at any time. One Identity Manager determines whether the assignment is effective.

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.

The effectiveness of the assignments is mapped in the PAGUserInUsrGroup and PAGBaseTreeHasUsrGroup via the column XIsInEffect.

Example of the effect of group memberships

- Group A is defined with permissions for triggering requests in a appliance. A group B is authorized to make payments. A group C is authorized to check invoices.
- Group A is assigned through the department "Marketing", group B through "Finance" and group C through the business role "Control group".

Clara Harris has a user account in this appliance. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B and C.

By using suitable controls, you want to prevent an employee from obtaining authorizations of groups A and group B at the same time. That means, groups A, B and C are mutually exclusive. A user, who is a member of group C cannot be a member of group B at the same time. That means, groups B and C are mutually exclusive.

Table 17: Specifying excluded groups (table `AADGroupExclusionPAGUsrGroupExclusion`))

Effective Group	Excluded Group
Group A	
Group B	Group A
Group C	Group B

Table 18: Effective Assignments

Employee	Member in Role	Effective Group
Ben King	Marketing	Group A
Jan Bloggs	Marketing, finance	Group B
Clara Harris	Marketing, finance, control group	Group C
Jenny Basset	Marketing, control group	Group A, Group C

Only the group C assignment is in effect for Clara Harris. It is published in the target system. If Clara Harris leaves the business role "control group" at a later date, group B also takes effect.

The groups A and C are in effect for Jenny Basset because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

Table 19: Excluded groups and effective assignments

Employee	Member in Role	Assigned Group	Excluded Group	Effective Group
Jenny Basset	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

- The configuration parameter **QER | Structures | Inherite | GroupExclusion** is enabled.
- Mutually exclusive groups belong to the same appliance.

To exclude a group

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select a group in the result list.
3. Select **Exclude groups**.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.

   - OR -

   In **Remove assignments**, remove the groups that are not longer mutually exclusive.
5. Save the changes.

Inheritance of PAM user groups based on categories

In One Identity Manager, user groups can be selectively inherited by user accounts. For this purpose, the user groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within this mapping rule. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table enter your categories for the user groups. Each table contains the category positions **Position 1** to **Position 31**.

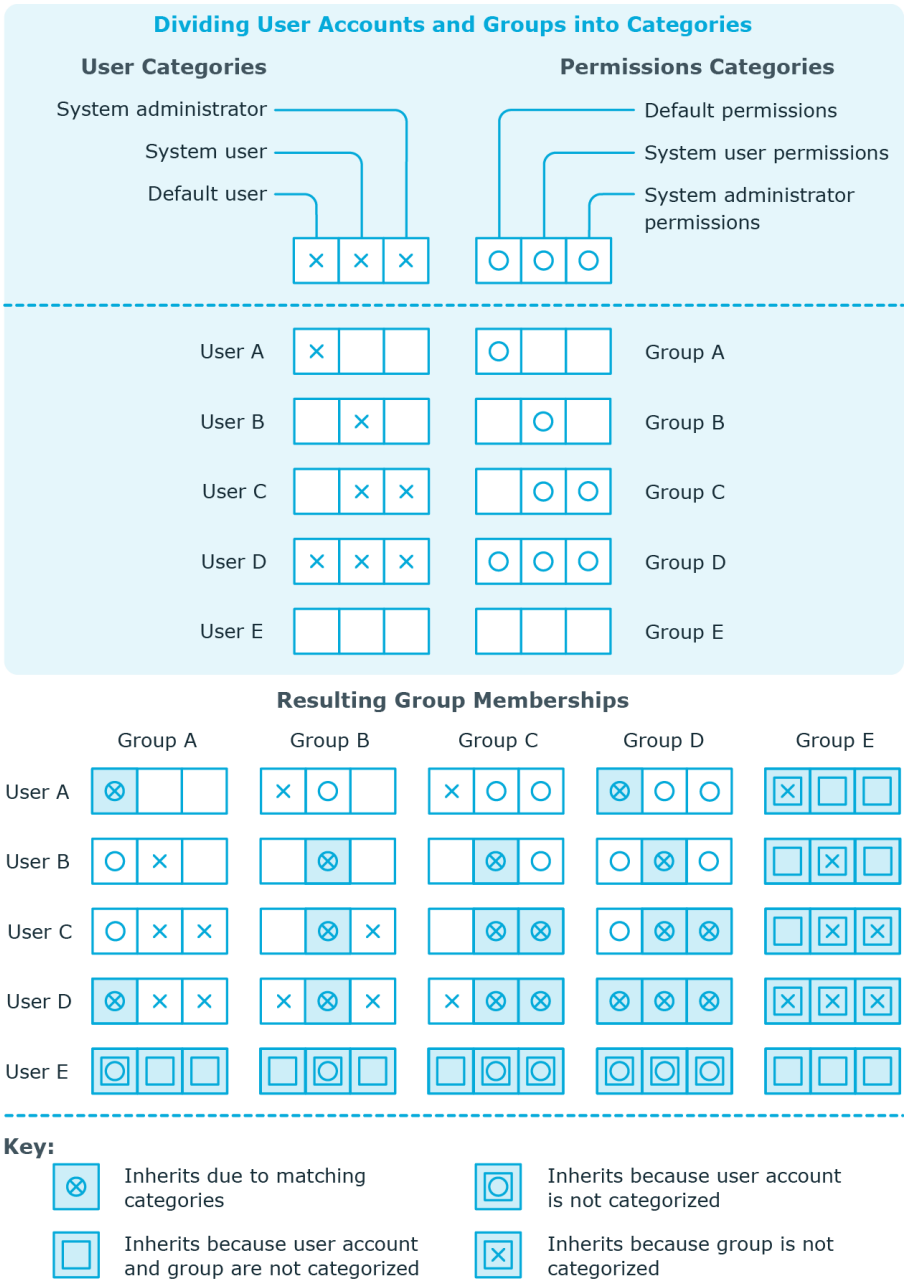
Every user account can be assigned to one or more categories. Each entitlement can also be assigned to one or more categories. If at least one of the category items between the user account and the assigned entitlement is the same, the entitlement is inherited by the user account. If the entitlement or the user account is not classified in a category, the entitlement is also inherited by the user account.

NOTE: Inheritance through categories is only taken into account when entitlements are assigned indirectly via hierarchical roles. Categories are not taken into account when entitlements are directly assigned to user accounts.

Table 20: Category Examples

Category Position	Categories for User Accounts	Categories for entitlements
1	Default user	Default group or default product
2	Administrator	Administrator group

Figure 1: Example of inheriting through categories.



To use inheritance through categories

- Define the categories on the appliance.
- Assign categories to user accounts through their master data.
- Assign categories to groups through their master data.

Overview of all assignments

The **Overview of all assignments** report is displayed for some objects, such as authorizations, compliance rules, or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees with this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the icon in the report's toolbar.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 2: Toolbar of the Overview of all assignments report.

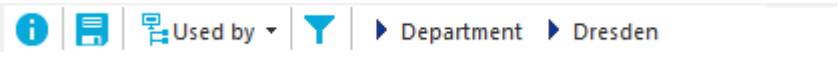


Table 21: Meaning of Icons in the Report Toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

Provision of login information for PAM user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login information generated to users.

Detailed information about this topic

- Password policies for PAM users on page 86
- Initial password for new PAM user accounts on page 97
- Email notifications about login data on page 98

Password policies for PAM users

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can user or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined password policies on page 87
- Applying password policies on page 88
- Editing password policies on page 90
- Creating password policies on page 90
- Custom scripts for password requirements on page 93

- Editing the excluded list for passwords on page 96
- Checking passwords on page 96
- Testing the generation of passwords on page 97

Predefined password policies

You can customize predefined password policies to meet your own requirements, if necessary.

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defined the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the access code for a one off log in on the Web Portal (`Person.Passcode`).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts or system users.

For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** password policy defines the settings for the (`Person.CentralPassword`) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Employee central password policy** password policy does not violate the system-specific requirements for passwords.

For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** standard policy applies. in this case, ensure that the default policy does not violate the target systems requirements.

The **PAM password policy** password policy is predefined for Privileged Account Management systems. You can apply this password policy to the passwords of user accounts (`PAGUser.Password`) of an appliance.

If the password requirements for the appliances are different, it is recommended that you set up your own password policies for each appliance.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Applying password policies

The **PAM password policy** password policy is predefined for Privileged Account Management systems. You can apply this password policy to the passwords of user accounts (`PAGUser.Password`) of an appliance.

If the password requirements for the appliances are different, it is recommended that you set up your own password policies for each appliance.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the account definition of the user account
2. Password policy of the manage level of the user account
3. Password policy for the appliance of the user.
4. Password policy **One Identity Manager password policy** (default policy)

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** standard policy applies. in this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Assign objects**.

4. Click **Add** in the **Assignments** section and enter the following data.

Table 22: Assigning a Password Policy

Property	Description
Apply to	Application scope of the password policy. ***To specify an application scope*** a. Click → next to the text box. b. Select one of the following references under **Table**: • The table that contains the base objects of synchronization. • Select the `TSBAccountDef` table to apply the password policy based on the account definition. • Select the `TSBBehavior` table to apply the password policy based on the manage level. c. Select the table that contains the base objects under **Apply to**. • If you have selected the table containing the base objects of synchronization, next select the specific target system. • If you have selected the `TSBAccountDef` table, next select the specific account definition. • If you have selected the `TSBBehavior` table, next select the specific manage level. d. Click **OK**.
Password column	The password column's identifier.
password policy	The identifier of the password policy to be used.

5. Save the changes.

To change a password policy's assignment

1. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Select the assignment you want to change in **Assignments**.
5. Select the new password policy to apply from the **Password Policies** menu.
6. Save the changes.

Editing password policies

To edit a password policy

1. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Change master data**.
4. Edit the password policy's master data.
5. Save the changes.

Detailed information about this topic

- General master data for a password policy on page 90
- Policy settings on page 91
- Character classes for passwords on page 92
- Custom scripts for password requirements on page 93

Creating password policies

To create a password policy

1. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
2. Click in the result list toolbar.
3. On the master data form, enter the master data for the password policy.
4. Save the changes.

Detailed information about this topic

- General master data for a password policy on page 90
- Policy settings on page 91
- Character classes for passwords on page 92
- Custom scripts for password requirements on page 93

General master data for a password policy

Enter the following master data for a password policy.

Table 23: Master data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Spare text box for additional explanation.Translate the given text using the button.
Error Message	Custom error message outputted if the policy is not fulfilled. Translate the given text using the button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts or system users.

Policy settings

Define the following settings for a password policy on the **Password** tab.

Table 24: Policy Settings

Property	Meaning
Initial password	Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.
Password confirmation	Reconfirm password.
Max. length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager.

Property	Meaning
	You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the **Contains name properties for password check** option is set are taken into account. Adjust this option in the column definition in Designer.

Character classes for passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 25: Character classes for passwords

Property	Meaning
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special	Specifies the minimum number of special characters the password

Property	Meaning
characters	must contain.
Permitted special characters	List of permitted characters.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Maximum number of identical character that can be repeated after each other.
Denied special characters	List of characters, which are not permitted.
Lowercase not allowed	Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.
Uppercase not allowed	Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.
Digits not allowed	Specifies whether the password can contain digits. This setting is only applies when passwords are generated.
Special characters not allowed	Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating password if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

- Script for checking a password on page 93
- Script for generating a password on page 95

Script for checking a password

You can implement a check script if additional policies need to be used for checking a password, which cannot be mapped with the available settings.

Syntax for Check Scripts

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
```

With parameters:

policy = password policy object

spwd = password to test

TIP: To use a base object, take the property `Entity` of the `PasswordPolicy` class.

Example for a script for testing a password

A password cannot start with **?** or **!**. The script checks a given password for validity.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in password")#)
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
    b. Select the password policy in the result list.
    c. Select **Change master data**.
    d. Enter the name of the script to be used to check a password in the **Check script** input field on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for generating a password on page 95

Script for generating a password

You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
```

With parameters:

policy = password policy object

spwd = generated password

TIP: To use a base object, take the property `Entity` of the `PasswordPolicy` class.

Example for a script to generate a password

In random passwords, the script replaces the **?** and **!** characters, which are not permitted.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

To use a custom script for generating a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
    b. Select the password policy in the result list.
    c. Select **Change master data**.

d. Enter the name of the script to be used to generate a password in the **Generating script** input field on the **Scripts** tab.

e. Save the changes.

Related Topics

- Script for checking a password on page 93

Editing the excluded list for passwords

You can add words to a list of restricted terms to prohibit them from being used in passwords.

NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. Select **Base Data | Security settings | Restricted passwords** in Designer.
2. Create a new entry with **Object | New** an enter the term to excluded to the list.
3. Save the changes.

Checking passwords

When you test a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To test whether a password conforms to the password policy

1. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Change master data**.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.

   A display next to the password shows whether it is valid or not.

Testing the generation of passwords

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. Select **Privileged Account Management | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Change master data**.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new PAM user accounts

You have the following possible options for issuing an initial password for a new user account.

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - In the Designer, set the configuration parameter **TargetSystem | PAG | Accounts | InitialRandomPassword**.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.
- User the employee's central password. The employee's central password is mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

Related Topics

- Password policies for PAM users on page 86
- Email notifications about login data on page 98

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text is defined in several languages in a mail template. which means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

The following prerequisites must be fulfilled in order to use notifications:

- Ensure that the email notification system is configured in One Identity Manager. For detailed information, see the *One Identity Manager Installation Guide*.
- In Designer, enable the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.
- Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
- Ensure that a language can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

When a randomly generated password is issued for the new user account, the initial login data for a user account is sent by email to a previously specified person.

To send initial login data by email

1. In Designer, set the **TargetSystem | PAG | Accounts | InitialRandomPassword** configuration parameter.
2. In Designer, set the **TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.

   If no recipient can be found, the e-mail is sent to the address stored in the **TargetSystem | PAG | DefaultAddress** configuration parameter.
3. In Designer set the **TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

   By default, the message sent uses the mail template **Employee - new user account created**. The message contains the name of the user account.
4. In Designer, set the **TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

   By default, the message sent uses the mail template **Employee - initial password for new user account**. The message contains the initial password for the user account.

TIP: Change the value of the configuration parameter in order to use custom mail templates for these mails.

6

Mapping of PAM objects in One Identity Manager

The user accounts, user groups, assets, asset groups, accounts, account groups, directories, entitlements, and access request policies of a Privileged Account Management systems are mapped in One Identity Manager. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

Detailed information about this topic

PAM appliances

The target system for the synchronization with One Identity Safeguard is the appliance. Appliances are created as base objects for the synchronization in One Identity Manager. They are used for the configuration of provisioning processes, the automatic assignment of employees to user accounts, and the passing on of PAM user groups to user accounts.

Detailed information about this topic

- PAM Creating appliances on page 101
- Editing the master data for PAM appliances on page 101
- General master data for PAM appliances on page 102
- Defining categories for the inheritance of PAM user groups on page 103

PAM Creating appliances

NOTE: The Synchronization Editor sets up the appliances in the One Identity Manager database. If necessary, appliances can also be created in Manager.

To set up an appliance

1. Select **Privileged Account Governance Module | Appliances** in Manager.
2. Click in the result list toolbar.
3. On the master data form, edit the master data for the appliance.
4. Save the changes.

Related Topics

- Editing the master data for PAM appliances on page 101
- General master data for PAM appliances on page 102
- Defining categories for the inheritance of PAM user groups on page 103

Editing the master data for PAM appliances

To edit the master data of an appliance:

1. Select **Privileged Account Governance Module | Appliances** in Manager.
2. Select the appliance in the result list.
3. Select **Change master data**.
4. Edit the master data for the appliance.
5. Save the changes.

Related Topics

- PAM Creating appliances on page 101
- General master data for PAM appliances on page 102
- Defining categories for the inheritance of PAM user groups on page 103

General master data for PAM appliances

On the **General** tab, you enter the following master data:

Table 26: General master data for an appliance

Property	Description
Appliance	Name of the appliance.
URL	Address (URL) of PAM web application This address is required to allow PAM users to log in to the system through the Web Portal on the PAM, for example, to retrieve a requested password or start a requested session.
Model	Model name of the appliance.
Appliance version	Version number of the appliance.
Network interface X0	IP address of the primary interface of the appliance in IPv4 or IPv6 format.
Network interface X01	IP address of the session module in IPv4 or IPv6 format.
Clustered	Specifies whether the appliance is clustered.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this appliance and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
target system managers	Application role in which target system managers for the appliance are defined. Target system managers only edit the objects of the appliance to which they are assigned. Each appliance can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this appliance. Use the button to add a new application role.
Synchronized by	Type of synchronization through which data is synchronized between the appliance and One Identity Manager. You can no longer change the synchronization type once objects for this appliance are present in One Identity Manager. When you create an appliance with the Synchronization Editor, **One Identity Manager** is used.

Property	Description

Table 27: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	One Identity Safeguard connector	One Identity Safeguard connector
No synchronization	none	none

NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.

Related Topics

- Assigning account definitions to PAM appliances on page 56
- Automatic assignment of persons to PAM user accounts on page 59
- Target system managers for PAM systems on page 143

Defining categories for the inheritance of PAM user groups

In One Identity Manager, user groups can be selectively inherited by user accounts. For this purpose, the user groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within this mapping rule. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table enter your categories for the user groups. Each table contains the category positions **Position 1** to **Position 31**.

To define a category

1. In Manager, select the applicance in **Privileged Account Management | Appliances**.
2. Select **Change master data**.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. Click to enable category.
6. Enter a category name of your choice for user accounts and groups and in the login language used.
7. Save the changes.

Detailed information about this topic

- Inheritance of PAM user groups based on categories on page 82

Additional tasks for managing PAM appliances

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Task	Theme
Overview of the PAM appliance	Overview of a PAM appliance on page 104
Define Search Criteria for Employee Assignment	Editing search criteria for automatic employee assignment on page 60
How to Edit a Synchronization Project	Editing the synchronization project for a PAM appliance on page 104
Synchronize object	Synchronizing single objects on page 35

Overview of a PAM appliance

To obtain an overview of an appliance

1. In Manager, select **Privileged Account Management | Appliances**.
2. Select the appliance in the result list.
3. Select **PAM appliance overview**.

Editing the synchronization project for a PAM appliance

Synchronization projects in which an appliance is already used as a base object can also be opened via Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor:

1. Select **Privileged Account Management | Appliances** in Manager.
2. Select the appliance in the result list.
3. Select **Change master data**.
4. Select **Edit synchronization project**.

Related Topics

- Adjusting the synchronization configuration for One Identity Safeguard on page 26

PAM User accounts

You use One Identity Manager to manage the user accounts of a Privileged Account Management system. A user account enables an employee to log onto the Privileged Account Management system, for example, onto One Identity Safeguard. One Identity Manager manages the local users of a Privileged Account Management system and directory users. Directory users are user accounts from an external target system, for example Active Directory or LDAP.

Via their user group the user receives the required entitlements, for example, for requesting a password for an asset account or a session for the accounts and assets in the Privileged Account Management system.

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location or a primary cost center.

Related Topics

- Managing PAM user accounts and employees on page 40
- Account definitions for PAM user accounts on page 41
- Creating local PAM user accounts on page 106
- Creating certificate-based PAM user accounts on page 106
- Creating PAM user accounts for directory users on page 107

- Editing master data for PAM user accounts on page 109
- Managing the assignments of PAM user groups on page 72

Creating local PAM user accounts

The users of a local PAM user account are authenticated by user name and password in the Privileged Account Management system.

To create a local PAM user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Click in the result list toolbar.
3. On the **General** tab, enter the following data as a minimum:
    - **Appliance**: Appliance to which the user account belongs.
    - **Authentication provider**: Select **Local**.
    - **User name**: Enter the user name for logging on to the system.
    - **Password**: Enter the password for logging on to the system.
    - **Confirmation**: Confirm the password.
    - **Time zone**: The user's time zone. The default time zone is **UTC** (Coordinated Universal Time).
4. Save the changes.

Related Topics

- General master data for PAM user accounts on page 109
- Contact information for PAM user accounts on page 112
- Secondary authentication for PAM user accounts on page 113
- Administrative entitlements for PAM user accounts on page 113
- Editing master data for PAM user accounts on page 109
- Creating certificate-based PAM user accounts on page 106
- Creating PAM user accounts for directory users on page 107

Creating certificate-based PAM user accounts

The users of a certificate-based PAM user account are authenticated using a certificate in the Privileged Account Management system.

To create a certificate-based PAM user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Click in the result list toolbar.
3. On the **General** tab, enter the following data as a minimum:
   - **Appliance**: Appliance to which the user account belongs.
   - **Authentication provider**: Select **Certificate**.
   - **User name**: Enter the user name for logging on to the system.
   - **Certificate thumbprint (SHA-1)**: Enter the unique hash value (40 hexadecimal characters) of the certificate.

     NOTE: You can copy the fingerprint value directly from the certificate and insert it here, including blank characters.
   - **Time zone**: The user's time zone. The default time zone is **UTC** (Coordinated Universal Time).
4. Save the changes.

Related Topics

- General master data for PAM user accounts on page 109
- Contact information for PAM user accounts on page 112
- Secondary authentication for PAM user accounts on page 113
- Administrative entitlements for PAM user accounts on page 113
- Editing master data for PAM user accounts on page 109
- Creating local PAM user accounts on page 106
- Creating PAM user accounts for directory users on page 107

Creating PAM user accounts for directory users

Directory users are user accounts from an external target system, for example Active Directory or LDAP. The authentication takes place via a user account of the relevant directory service, for example Active Directory user account or LDAP user account.

You can only create directory users in One Identity Manager if the Active Directory environment or the LDAP environment is imported into the One Identity Manager.

To create a PAM user account for directory users

1. In Manager, select **Privileged Account Management | User accounts**.
2. Click in the result list toolbar.

3. On the **General** tab, enter the following data as a minimum:
    - **Appliance**: Appliance to which the user account belongs.
    - **Authentication provider**: Select the Active Directory domain or the LDAP domain of the user account.

      The PAM directory is determined automatically.
    - **Authentication object**: Select the user account from the authentication provider.
        a. To do this, click → next to the input field and enter the following information:
            - **Table**: Table in which the user accounts are mapped. This table is preselected.

              For a Active Directory user account, **ADSAccount** is selected. For a LDAP user account, **LDAPAccount** is selected.
            - **Authentication object**: Select the user account.
        b. Click **OK**.

      The domain, the user name, and the display name are determined from the user account.
    - (Optional) **Require certificate authentication**: Specifies that the user can only log on using a domain-issued user certificate or SmartCard. This option is only available for the authentication provider Active Directory.
    - **Time zone**: The user's time zone. The default time zone is **UTC** (Coordinated Universal Time).
4. Save the changes.

NOTE: If you use account definitions to create PAM user accounts for employees, for a PAM appliance, you have the option to define an Active Directory account definition or a LDAP account definition as a required account definition. In this case, an LDAP or Active Directory user account is first created for the employee. If this user account exists, the PAM user account is created as a directory user.

Related Topics

- General master data for PAM user accounts on page 109
- Contact information for PAM user accounts on page 112
- Secondary authentication for PAM user accounts on page 113
- Administrative entitlements for PAM user accounts on page 113
- Editing master data for PAM user accounts on page 109
- Creating local PAM user accounts on page 106
- Creating certificate-based PAM user accounts on page 106
- Account definitions for PAM user accounts on page 41

Editing master data for PAM user accounts

To edit master data for a user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list and run **Change master data**.
3. Edit the user account's resource data.
4. Save the changes.

Related Topics

- General master data for PAM user accounts on page 109
- Contact information for PAM user accounts on page 112
- Secondary authentication for PAM user accounts on page 113
- Administrative entitlements for PAM user accounts on page 113
- Disabling PAM user accounts
- Deleting and restoring PAMuser accounts

General master data for PAM user accounts

On the **General** tab, you enter the following master data:

Table 28: Additional Master Data for a User Account

Property	Description
Appliance	Appliance to which the user account belongs.
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. For a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity** or **Service identity**, you can create a new employee. To do this, click next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.

Property	Description
	NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved.
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Authentication provider	Specifies how the user is authenticated in the Privileged Account Management system. Permitted values are: • **Certificate**: Authentication is performed using a certificate. • **Local**: The user is authenticated by a user name and password. • **<Directory name>**: The authentication takes place via a user account of the relevant directory service, for example an Active Directory user account or LDAP user account. This variant is only available if the Active Directory domain or the LDAP domain is imported into the One Identity Manager.
User name	User name of the PAM user account.
Display name	Display name of the PAM user account.
Password	The user's password (only for local PAM user accounts).
Confirmation	The user's password (only for local PAM user accounts).
Directory	Directory (only for PAM directory users) PAM.
Authentication object	User account in Active Directory or LDAP (only for PAM directory users).
Domain	Domain of the user account (only for PAM directory users).
Require certificate authentication	Specifies that the user can only log on using a domain-issued user certificate or SmartCard (only for PAM directory users). This option is only available for the authentication provider Active Directory.

Property	Description
Certificate fingerprint (SHA-1)	(Only for certificate-based PAM user accounts) unique hash value of the certificate (40 hexadecimal characters).
Last login	Time of the last login to the system.
Time zones	The user's time zone. The default time zone is **UTC** (Coordinated Universal Time).
Risk index (calculated)	Maximum risk index value of all assigned . The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is enabled. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative entitlements, used by one employee. • **Sponsored identity**: User account that is used for training purposes, for example. • **Shared identity**: User account with administrative entitlements, used by several employees. Assign all employees show use the user account. • **Service identity**: Service account.
Groups can be inherited	Specifies whether the user account can inherit groups via the employee. If this option is set, the user account inherits groups via hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Privileged user account	Specifies whether this is a privileged user account.

Property	Description
System object	Identifies the user as a part of the system.
User account is disabled	Specifies whether the user account is disable. If a user account is not required for a period of time, you can temporarily disable the user account by using the option <User account is deactivated>.
Account locked	Specifies whether the user account is locked. Depending on the configuration, the user account in the Privileged Account Management system is locked after multiple incorrect password attempts.
Created on	Time at which the user account was created.
Created by	User who created the user account.

Related Topics

- Managing PAM user accounts and employees on page 40
- Account definitions for PAM user accounts on page 41
- Automatic assignment of persons to PAM user accounts on page 59
- Inheritance of PAM user groups based on categories on page 82
- Disabling PAM user accounts on page 115
- Supported user account types on page 65

Contact information for PAM user accounts

On the **Contact information** tab, you enter the following master data:

Table 29: Contact data for a user account

Property	Description
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled with the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled with the manage level.
Phone	Telephone number. If you have assigned an account definition, the input field is automatically filled with the manage level.
Mobile phone	Mobile number. If you have assigned an account definition, the input field is automatically filled with the manage level.
Email address	User account email address. If you assigned an account definition, the email address is made up of the employee's default email address depending on the manage level of the user account.
Description	Spare text box for additional explanation.

Secondary authentication for PAM user accounts

If multi-factor authentication is required for the user, enter the following master data on the **Secondary authentication** tab.

Table 30: Secondary authentication of a user account

Property	Description
Secondary authentication	Second authentication provider for requesting multi-factor authentication by the user. All identity providers who are permitted as secondary authentication providers (table `PAGIdentityProvider`, column `AllowSecondaryAuth`).
Secondary authentication object	Character string for identifying the second authentication object for multi-factor authentication. The input depends on the selected secondary authentication provider. If the secondary authentication of a user is performed via an Active Directory user account or an LDAP user account, you can select the user account. 1. To do this, click → next to the input field and enter the following information: • **Table**: Table in which the user accounts are mapped. This table is preselected. For an Active Directory user account, **ADSAccount** is selected. For an LDAP user account, **LDAPAccount** is selected. • **Authentication object**: Select the user account. 2. Click **OK**.

Administrative entitlements for PAM user accounts

If necessary, on the **Entitlements** tab, enter the administrator entitlements of the user. For detailed information about administrative entitlements in One Identity Safeguard, see the *One Identity Safeguard Administration Guide*.

Table 31: Administrative entitlements for a user account

Administrative role	Description
Authorizer	Enables the user to grant permissions to other users.
User	Enables the user to create new users, and to approve and reset passwords for non-administrative users
Help Desk	Enables the user to create and approve passwords for non-administrative users
Appliance	Enables the user to edit, update, and configure the appliance.
Operations	Enables the user to restart the appliance and to monitor the appliance.
Auditor	Provides the user with read-only access.
Asset	Enables the user to add, edit, and delete partitions, assets, and accounts.
Directory	Enables the user to add, edit, and delete directories.
Security policy	Enables the user to add, edit, and delete entitlements and policies that control access to accounts and assets.

Additional tasks for managing PAM user accounts

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Task	Theme
Overview of PAM User Accounts	Overview of PAM user accounts on page 114
assign group	Assigning PAM user groups directly to a PAM user account on page 79
Assigning extended properties	Assigning extended properties to PAM user accounts on page 115
Synchronize object	Synchronizing single objects on page 35

Overview of PAM user accounts

For a user account, you see an overview of the user groups and entitlements associated with the user account. For directory users, the associated Active Directory user account or

LDAP user account is displayed.

To obtain an overview of a user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Select **PAM user account overview**.

Assigning extended properties to PAM user accounts

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties**.
4. Assign extended properties in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of extended properties.

   To remove an assignment

   - Select the extended property and double click ✓.
5. Save the changes.

For detailed information about extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Disabling PAM user accounts

The way you disable user accounts depends on how they are managed.

Scenario:

- The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the manage level **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `PAGUser.IsDisabled` column.

Scenario:

- The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the employee's user accounts are disabled if the employee is permanently or temporarily disabled.
- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To disable the user account when the configuration parameter is disabled.

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Enable **Account is disabled** on the **General** tab.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To disable a user account that is no longer linked to an employee.

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Enable **Account is disabled** on the **General** tab.
5. Save the changes.

For detailed information about disabling and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Related Topics

- Account definitions for PAM user accounts on page 41
- Creating manage levels on page 45
- Deleting and restoring PAMuser accounts on page 117

Deleting and restoring PAMuser accounts

If a user account is deleted in One Identity Manager, it is initially marked for deletion. The user account is therefore locked. Depending on the deferred deletion setting, the user account is either deleted from the One Identity Manager database immediately, or at a later date.

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is deleted.

To delete a user account that is not managed using an account definition

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Click to delete the user account.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. In Manager, select **Privileged Account Management | User accounts**.
2. Select the user account in the result list.
3. Click in the result list toolbar.

Configuring deferred deletion

By default, user accounts are finally deleted from the database after 30 days.The user accounts are initially disabled. You can reenable the user accounts until deferred deletion is run. After deferred deletion is run, the user account are deleted from the database and cannot be restored anymore. You can configure an alternative deletion delay in Designer using the PAGUser table.

Related Topics

- Disabling PAM user accounts on page 115

PAM user groups

Via their user group the user receives the required entitlements, for example, for requesting a password for an asset account or a session for the accounts and assets in the Privileged Account Management system.

All local user groups and directory groups of an appliance are imported into One Identity Manager during synchronization. You can only edit limited features of user groups in One

Identity Manager. For example, you adjust local user groups for use in IT Shop and assign them to user accounts.

Related Topics

- Editing master data for PAM user groups on page 118
- Managing the assignments of PAM user groups on page 72

Editing master data for PAM user groups

To edit group master data

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select the group in the result list and run **Change master data**.
3. On the master data form, edit the master data for the group.
4. Save the changes.

Related Topics

- General master data for PAM user groups on page 118

General master data for PAM user groups

On the **General** tab, edit the following master data.

Table 32: General master data for a user group

Property	Description
Name	Name of the user group
Appliance	Appliance to which the user group belongs.
Service item	Service item data for requesting the group through the IT Shop.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.

Property	Description
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the configuration parameter **QER | CalculateRiskIndex** is activated. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.
Description	Spare text box for additional explanation.
Directory	PAM directory (only for directory groups).
Target system group	Group in Active Directory or LDAP (only for directory groups).
Read only memberships	The directory group is read-only (only for directory groups). The memberships are maintained in the directory, for example in Active Directory or LDAP.
Created on	Time at which the user account was created.
Created by	User who created the user account.

Related Topics

- Inheritance of PAM user groups based on categories on page 82
- Adding PAM user groups to the IT Shop on page 77

Additional tasks for managing PAM user groups

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Task	Theme
Overview of the PAM user group	Overview of PAM user groups on page 120
Assigning extended properties	Assigning extended properties to PAM user groups on page 120
assign user accounts	Effects of PAM user group memberships on page 80
Exclude groups	Effects of PAM user group memberships on page 80

Task	Theme
Assign system roles	Adding PAM user groups to system roles on page 76
Assign business roles	Assigning PAM user groups to business roles on page 75
Assign organizations	Assigning PAM user groups to departments, cost centers, and locations on page 74
Add to IT Shop	Adding PAM user groups to the IT Shop on page 77
Synchronize object	Synchronizing single objects on page 35

Overview of PAM user groups

For a user group, you see an overview of the user accounts and entitlements associated with the user group. For directory groups, the associated Active Directory group or LDAP group is displayed.

To obtain an overview of a group

1. Select the category **Privileged Account Management | Groups**.
2. Select the group in the result list.
3. Select **PAM user group overview**.

Assigning extended properties to PAM user groups

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a group

1. Select the **Privileged Account Management | User groups** in Manager.
2. Select the group in the result list.
3. Select **Assign extended properties**.
4. Assign extended properties in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of extended properties.

   To remove an assignment

   - Select the extended property and double click ✓.
5. Save the changes.

For more detailed information about setting up extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

PAM assets

Assets are computers, servers, network devices, or applications that are managed by a PAM appliance.

Assets are imported into the One Identity Manager database during synchronization. Changes to the object properties of individual assets can be re-imported via single object synchronization.

To display the properties of an asset:

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Assets**.
2. Select the asset in the result list.
3. Select **Change master data**.

For an asset, you see an overview of the asset groups, asset accounts, and the access request policies associated with the asset.

To view an overview of an asset:

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged Objects | Assets**.
2. Select the asset in the result list.
3. Select **PAM asset overview**.

Related Topics

- Synchronizing single objects on page 35
- Specifying owners for assets on page 132

PAM asset groups

An asset group is a collection of assets. An asset group can be added to the scope of an access request policy.

Asset groups are imported into the One Identity Manager database during synchronization. You cannot edit the properties of asset groups. Changes to the object properties of individual asset groups can be re-imported via single object synchronization.

To display the properties of an asset group

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Asset groups**.
2. Select the asset group in the result list.
3. Select **Change master data**.

For an asset group, you see an overview of the assets and access request policies associated with the asset group.

To obtain an overview of an asset group

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged Objects | Asset groups**.
2. Select the asset group in the result list.
3. Select **PAM asset group overview**.

Related Topics

- Synchronizing single objects on page 35

PAM asset accounts

An asset account is a unique ID for the access to an asset, for example, a user account, a group or a service account. For asset accounts, passwords can be requested for accessing the assets.

Asset accounts are imported into the One Identity Manager database during synchronization. Changes to the object properties of individual asset accounts can be re-imported via single object synchronization.

To display the properties of an asset account:

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Asset accounts**.
2. Select the asset account in the result list.
3. Select **Change master data**.

For an asset account, you see an overview of the account groups and the access request policies associated with the asset account.

To view an overview of an asset account:

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged Objects | Asset accounts**.
2. Select the asset account in the result list.
3. Select **PAM asset account overview**.

Related Topics

- Synchronizing single objects on page 35
- Specifying owners for asset accounts on page 132

PAM directory accounts

Directory accounts are privileged user accounts in a directory, for example Active Directory or LDAP, for which a password can be requested.

Directory accounts are imported into the One Identity Manager database during synchronization. Changes to the object properties of individual directory accounts can be re-imported via single object synchronization.

To display the properties of a directory account

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Directory accounts**.
2. Select the directory account in the result list.
3. Select **Change master data**.

For a directory account, you see an overview of the user account in the directory, the PAM user accounts, and the access request policies associated with the directory account.

To view an overview of a directory account:

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged Objects | Directory accounts**.
2. Select the directory account in the result list.
3. Select **PAM directory account overview**.

Related Topics

- Synchronizing single objects on page 35
- Specifying owners for directory accounts on page 133

PAM account groups

An account group is a collection of asset account and directory accounts. An account group can be added to the scope of an access request policy.

Account groups are imported into the One Identity Manager database during synchronization. You cannot edit the properties of account groups. Changes to the object

properties of individual account groups can be re-imported via single object synchronization.

To display the properties of an account group

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Account groups**.
2. Select the account group in the result list.
3. Select **Change master data**.

For an account group, you see an overview of the asset accounts, directory accounts, and the access request policies associated with the account group.

To obtain an overview of an account group

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Account groups**.
2. Select the account group in the result list.
3. Select **PAM account group overview**.

Related Topics

- Synchronizing single objects on page 35

PAM directories

Directories represent external target system, for example Active Directory or LDAP. If the Active Directory environment or the LDAP environment is imported into One Identity Manager, you can create directory users in One Identity Manager. Directory users and directory groups are linked to the relevant Active Directory objects and LDAP objects.

Directories are imported into the One Identity Manager database during synchronization. You cannot edit the properties of directories. Changes to the object properties of individual directories can be re-imported via single object synchronization.

To display the properties of a directory

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Directories**.
2. Select the directory in the result list.
3. Select **Change master data**.

For a directory, you see an overview of the user accounts, user groups, and the directory accounts associated with the directory.

To view an overview of a directory

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Directories**.
2. Select the directory in the result list.
3. Select **PAM directory overview**.

Related Topics

- Synchronizing single objects on page 35

PAM entitlements

An entitlement is a set of access request policies that ensures only authorized users can access the system. An entitlement usually groups together a set of permissions that are required to fulfill a specific task.

An entitlement defines which users are authorized to request passwords for accounts or sessions for assets as part of the defined access request policies.

Entitlements are imported into the One Identity Manager database during synchronization. You cannot edit the properties of entitlements. Changes to the object properties of individual entitlements can be re-imported via single object synchronization.

To display the properties of an entitlement

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Entitlements**.
2. Select the entitlement in the result list.
3. Select **Change master data**.

For an entitlement, you see an overview of the user accounts, user groups, and the access request policies associated with the entitlement.

To view an overview of an entitlement

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Entitlements**.
2. Select the entitlement in the result list.
3. Select **PAM entitlement overview**.

Related Topics

- Synchronizing single objects on page 35

PAM access request policies

An access request policy defines

- the scope (i.e. which assets, asset groups, asset accounts, directory accounts, or account groups),
- the access type (password, SSH, or remote desktop), and
- the rules for requesting passwords, for example, the duration or how many approvals are required.

Access request policies are imported into the One Identity Manager database during synchronization. Changes to the object properties of individual access request policies can be re-imported via single object synchronization.

To display the properties of an access request policy

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Entitlements | <Entitlement>**.
2. Select the access request policy in the result list.
3. Select **Change master data**.

For an access request policy, will see an overview of the scope of the access request policy and the entitlements associated with the access request policy.

To obtain an overview of an access request policy

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Entitlements | <Entitlement>**.
2. Select the access request policy in the result list.
3. Select **PAM access request policy overview**.

Related Topics

- Synchronizing single objects on page 35
- Configuring the PAM access request policies on page 133

PAM object reports

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for PAM systems.

Table 33: Reports for the Target System

Report	Description
Overview of all assignments (appliance)	This report finds all roles containing employees with at least one user account in the appliance.
Overview of all assignments (user groups)	This report finds all roles containing employees who have the selected user group.
PAM user account and group admin-istration	This report contains a summary of user account and group distribution in all PAM appliances. You can find the report in the category **My One Identity Manager | Target system overviews**.
Data quality summary for PAM user accounts	This report contains different evaluations of user account data quality in all PAM appliances. You can find the report in the category **My One Identity Manager | Data quality analysis**.

7

PAM access requests

In One Identity Manager, you can request access requests for assets, asset accounts, and directory accounts of a PAM system. For requesting an access request, the following products are available in IT Shop:

- **Password release request**: To request passwords for accounts in a PAM system.
- **SSH session request**: To request SSH sessions for assets in a PAM system.
- **Remote Desktop session request**: To request remote desktop sessions for assets in a PAM system.

The access requests are requested in Web Portal. After the request is approved, a corresponding access request is created in the PAM system. To check out the requested password or session, the user logs on to the PAM system.

For more detailed information about configuring the IT Shop, see the *One Identity Manager IT Shop Administration Guide*. For more detailed information about requesting access requests in Web Portal, see the *One Identity Manager Web Portal User Guide*.

Detailed information about this topic

- System requirements for requesting PAM access requests on page 128
- Requesting PAM access requests on page 129
- Owners of PAM assets, PAM asset accounts and PAM directory accounts on page 131
- Configuring the PAM access request policies on page 133

System requirements for requesting PAM access requests

The access requirements in the PAM system are created in process and script processing. The Job server must have the same configuration as the synchronization server (in terms of the installed software and the entitlements and certificates of the user account). Use the synchronization server.

In One Identity Safeguard, the following system prerequisites must be guaranteed:

- The application-to-application service is enabled.
- An application with the following properties has been registered and activated:
  - **Name**: One Identity Manager
  - **Certificate user**: Users for access to the One Identity Safeguard appliance (synchronization user)
  - **Access request broker**: Activated

    At least one user or user group for which One Identity Safeguard will determine the access must be assigned to the access request broker.

    This list is updated when access requests are created by the One Identity Manager.
- To ensure that the access requests created are valid as far as possible,
  - no time restrictions must be placed on the user permissions.
  - no time restrictions must be placed on the access request policies.

For more detailed information about setting up the application to application service in One Identity Safeguard and configuring the entitlements and access request policies, see the *One Identity Safeguard Administration Guide*.

Related Topics

- Users and permissions for synchronizing with a One Identity Safeguard appliance on page 14
- Setting up the One Identity Safeguard synchronization server on page 15

Requesting PAM access requests

Table 34: Default objects for requesting access requests

Products	**Password release request**: To request passwords for accounts in a PAM system. **SSH session request**: To request SSH sessions for assets in a PAM system. **Remote Desktop session request**: To request remote desktop sessions for assets in a PAM system.
Service category:	Privileged access requirements
Shelf	Identity & Access Lifecycle | Privileged access
Approval procedures:	PG - owners of the requested privileged access request
Approval policies/approval workflows	Approval decision for the requests for privileged access

By requesting these default products, access requests to privileged objects of a PAM system can be created. The products are multi-request resources

The requester provides information about the required access request, such as the product and asset or account to be accessed, together with the time period for the access. The owner of the privileged object for which you are requesting access approves the order. In the PAM system, a corresponding access request is made.

In the request, it is noted whether it was possible to create the access request in the PAM system and whether the access request was approved in the PAM system. The status of an access request is checked at regular intervals in the PAM system by means of the **Read status of privileged access requests** schedule.

If the access request has been approved, the user can log on to the PAM system and retrieve the required password, or start the required session.

Prerequisites

- The requester's PAM user account has the entitlement for requesting the access request.
- In the access request policy, the **One Identity Manager enabled** option is activated. If this option is activated, access requests for assets, asset accounts, and directory accounts can be requested from the scope of the access request policy.
- An application role can be assigned to the requestable assets, asset accounts, and directory accounts under **Privileged Account Governance | Asset and account owners**.
- Employees are assigned to the application roles.
- The **Read status of privileged access requests** schedule is enabled. Adjust the schedule in Designer if necessary.
- The URL of the PAM web application is entered on the appliance. In this way, the users can log in to the PAMSystem from the Web Portal and retrieve the password or start a session.

For more detailed information about configuring the IT Shop, see the *One Identity Manager IT Shop Administration Guide*. For more detailed information about requesting access requests in Web Portal, see the *One Identity Manager Web Portal User Guide*.

Related Topics

- Owners of PAM assets, PAM asset accounts and PAM directory accounts on page 131
- Configuring the PAM access request policies on page 133
- PAM entitlements on page 125
- General master data for PAM appliances on page 102

Owners of PAM assets, PAM asset accounts and PAM directory accounts

The owners of privileged objects such as PAM assets, PAM asset accounts, or PAM directory accounts must be assigned to an application role under the application role **Privileged Account Governance | Asset and account owners**.

Users with this application role:

- Make decisions on the requesting of access requirements for privileged objects.
- Attest the possible user access to these privileged objects

The approval procedure **PG - Owner of requested privileged access** takes the application role into account when determining approvers. The approval procedure **OP - Owner of a privileged object** takes the application role into account when determining attestors.

To specify employees as owners

1. Login to Manager as target system manager.
2. In **Privileged Account Management | Basic configuration data | Asset and account owners**, select the application role.
3. Select **Assign employees**.
4. Assign employees in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of employees.

   To remove an assignment

   - Select the employee and double click .
5. Save the changes.

Detailed information about this topic

- Specifying owners for assets on page 132
- Specifying owners for asset accounts on page 132
- Specifying owners for directory accounts on page 133

Specifying owners for assets

To define the owners of an asset

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged objects | Assets**.
2. Select the asset in the result list.
3. Select **Change master data**.
4. On the **General** tab, select the application role in the **Owner (Application Role)** selection list.

   - OR -

   Next to the **Owner (Application Role)** list, click on to create a new application role.

   a. Enter the application role name and assign the parent application role **Privileged Account Governance | Asset and account owners**.

   b. Click **OK** to add the new application role.

Related Topics

- Owners of PAM assets, PAM asset accounts and PAM directory accounts on page 131

Specifying owners for asset accounts

To define the owners of an asset account

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged Objects | Asset accounts**.
2. Select the asset account in the result list.
3. Select **Change master data**.
4. On the **General** tab, select the application role in the **Owner (Application Role)** selection list.

   - OR -

   Next to the **Owner (Application Role)** list, click on to create a new application role.

   a. Enter the application role name and assign the parent application role **Privileged Account Governance | Asset and account owners**.

   b. Click **OK** to add the new application role.

Related Topics

- Owners of PAM assets, PAM asset accounts and PAM directory accounts on page 131

Specifying owners for directory accounts

To define the owners of a directory account

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Privileged Objects | Directory accounts**.
2. Select the directory account in the result list.
3. Select **Change master data**.
4. On the **General** tab, select the application role in the **Owner (Application Role)** selection list.

   - OR -

   Next to the **Owner (Application Role)** list, click on to create a new application role.

   a. Enter the application role name and assign the parent application role **Privileged Account Governance | Asset and account owners**.

   b. Click **OK** to add the new application role.

Related Topics

- Owners of PAM assets, PAM asset accounts and PAM directory accounts on page 131

Configuring the PAM access request policies

Access requests for assets, asset accounts, and directory accounts can only be requested if the **Effects on One Identity Manager** option is activated in the access request policy.

To configure the access request policy

1. In Manager, select **Privileged Account Management | Appliances | <Appliance> | Entitlements | <Entitlement>**.
2. Select the access request policy in the result list.
3. Select **Change master data**.
4. On the **General** tab, check the **Effects on One Identity Manager** option.

- If this option is activated, access requests for assets, asset accounts, and directory accounts can be requested from the scope of the access request policy.
- If this option is not activated, access requests for assets, asset accounts, and directory accounts cannot be requested from the scope of the access request policy.

Related Topics

- PAM access request policies on page 126
- Requesting PAM access requests on page 129

Handling of PAM objects in Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal. The Web Portal supports the administration of a Privileged Account Management system for the following tasks:

- Managing user accounts and employees

  An account definition can be requested by shop customers in Web Portal when it is assigned to an IT Shop shelf. The request undergoes a defined approval procedure. The user account is not created until it has been agreed by an authorized person, such as a manager.

- Managing the assignments of user groups

  When a group is assigned to an IT Shop shelf, the group can be requested by the customers of the shop in Web Portal. The request undergoes a defined approval procedure. The group is not assigned until it has been approved by an authorized person.

  In Web Portal, managers and administrators of organizations can assign groups to the departments, cost centers, or locations for which they are responsible. The groups are passed on to all persons who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, managers and administrators of business roles can assign groups in the Web Portal to the business roles for which they are responsible. The groups are passed on to all persons who are members of these business roles.

  If the System Roles Module is available, supervisors of system roles can assign groups to the system roles in the Web Portal. The groups are passed on to all persons to whom these system roles are assigned.

- Managing access requests to privileged objects

  Using IT Shop Shelf **Identity & Access Lifecycle | Privileged access** you can request password and session requests for privileged objects of a PAM system. The request undergoes a defined approval procedure. The owner of the privileged object for which you are requesting access approves the order. In the PAM system, a corresponding access request is made. If you were able to successfully create the access request, the user can log on to the PAM system and call the required password, or start the required session.

- Attestation

  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. The owners of privileged objects attest the possible user access to these privileged objects. To enable this, attestation policies are configured in Manager. The attesters use the Web Portal to approve attestation cases.

- Governance Administration

  If the Compliance Rules Module is available, you can define rules that identify the invalid entitlement assignments and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in Manager. Supervisors use the Web Portal to check and resolve rule violations and to grant exception approvals.

  If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in Manager. Supervisors use the Web Portal to check policy violations and and to grant exception approvals.

- Risk assessment

  You can use the risk index of groups to evaluate the risk of entitlement assignments for the company. The One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the employees, user accounts, and their entitlements and risks.

For more information about the named topics, see Managing PAM user accounts and employees on page 40, Assigning PAM user groups to PAM user accounts in One Identity Manager on page 72, PAM access requests on page 128 and refer to the following guides:

- *One Identity Manager Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

8

Basic data for managing a Privileged Account Management system

To manage a Privileged Account Management system in One Identity Manager, the following basic data is relevant.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

  For more information, see Account definitions for PAM user accounts on page 41.

- Password policies

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

  Predefined password policies are supplied with the default installation that you can user or customize if required. You can also define your own password policies.

  For more information, see Password policies for PAM users on page 86.

- Target system types

  Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.

  For more information, see Post-processing outstanding objects on page 36.

- Server

  In order to handle Target system-specific processes in One Identity Manager, the synchronization server and its server functions must be declared.

  For more information, see Job server for PAM-specific process handling on page 138.

- Target system managers

  A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who are permitted to edit all appliances in One Identity Manager.

  Define additional application roles if you want to limit the edit permissions for target system managers to individual appliances. The application roles must be added under the default application role.

  For more information, see Target system managers for PAM systems on page 143.

- Owners of privileged objects

  One Identity Manager includes a standard application role for the owners of privileged objects such as PAM assets, PAM asset accounts or PAM directory accounts. The owners are included in the standard approval workflows as approvers and attestors.

  For more information, see Owners of PAM assets, PAM asset accounts and PAM directory accounts on page 131.

Job server for PAM-specific process handling

In order to handle Target system-specific processes in One Identity Manager, the synchronization server and its server functions must be declared. You have several options for defining a server's functionality:

- Create an entry for the Job server in Designer under **Base Data | Installation | Job server**. For detailed information, see the *One Identity Manager Configuration Guide*.
- Select an entry for the Job server in **Privileged Account Management | Basic configuration data | Server** in Manager and edit the Job server master data.

  Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

Related Topics

- System requirements for the One Identity Safeguard synchronization server on page 16
- Editing PAM Job servers on page 139

Editing PAM Job servers

To edit a Job server and its functions

1. In Manager, select the category **Privileged Account Management | Basic configuration data | Server**.
2. Select the Job server entry in the result list.
3. Select **Change master data**.
4. Edit the Job server's master data.
5. Select **Assign server functions** in the task view and specify server functionality.
6. Save the changes.

Detailed information about this topic

- General master data for Job servers on page 139
- Specifying server functions on page 141
- Installing One Identity Manager Service with One Identity Safeguard connector on page 16

General master data for Job servers

NOTE: All editing options are also available in Designer under **Base Data | Installation | Job server**.

NOTE: More properties may be available depending on which modules are installed.

Table 35: Job Server Properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of servers>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.

Property	Meaning
Server belongs to cluster	Cluster to which the server belongs. NOTE: The properties **Server is cluster** and **Server belongs to cluster** are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when One Identity Manager Service is automatically updated. If the server is handling several queues the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.

Property	Meaning
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux** and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure `QBM_PJobQueueLoad` the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the program "Job Queue Info". For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being executed.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying server functions on page 141

Specifying server functions

NOTE: All editing options are also available in Designer under **Base Data | Installation | Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.

NOTE: More server functions may be available depending on which modules are installed.

Table 36: Permitted server functions

Server function	Remark
Update Server	This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	The server can execute SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	The server can process CSV files using the `ScriptComponent` process component.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
One Identity Safeguard connector	Server on which the One Identity Safeguard connector is installed. This server executes synchronization with the target system One Identity Safeguard.

Related Topics

- General master data for Job servers on page 139

Target system managers for PAM systems

A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who are permitted to edit all appliances in One Identity Manager.

Define additional application roles if you want to limit the edit permissions for target system managers to individual appliances. The application roles must be added under the default application role.

For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator assigns employees to be target system managers.
2. These target system managers add employees to the default application role for target system managers.

   Target system managers with the default application role are authorized to edit all Privileged Account Management systems in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual PAM systems.

Table 37: Default Application Roles for Target System Managers

Users	Tasks
target system managers	Target system managers must be assigned to the **Target systems | Privileged account management** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Can create employees with an identity that differs from the **Primary identity**. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.

Users	Tasks
	• Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required. • Authorize employees as owners of privileged objects within their area of responsibility.

To initially specify employees to be target system administrators

1. Log in to One Identity Manager as Manager administrator (**Base role | Administrators**)
2. Select **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees**.
4. Assign the employee you want and save the changes.

To add the first employees to the default application as target system managers.

1. Log yourself into Manager as target system administrator (**Target systems | Administrators**).
2. Select **One Identity Manager Administration | Target systems | Privileged Account Management**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

1. Login to Manager as target system manager.
2. Select the application role in Privileged Account Management **| Basic configuration data | Target system managers**.
3. Select **Assign employees**.
4. Assign the employees you want and save the changes.

To specify target system managers for individual Privileged Account Management systems

1. Login to Manager as target system manager.
2. Select **Privileged Account Management | Appliances**.
3. Select the appliance in the result list.
4. Select **Change master data**.
5. On the **General** tab, select the application role in the **Target system manager**

menu.

- OR -

Next to the **Target system manager** menu, click  to create a new application role.

a. Enter the application role name and assign the **Target systems | Privileged Account Management** parent application role.

b. Click **OK** to add the new application role.

6. Save the changes.
7. Assign employees to this application role who are permitted to edit the system in One Identity Manager.

Related Topics

- One Identity Manager Users for managing a Privileged Account Management system on page 9
- General master data for PAM appliances on page 102

Appendix: Configuration parameters for the management of a Privileged Account Management system

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 38: Configuration parameters for synchronizing a Privileged Account Management system

Configuration parameter	Meaning if Set
TargetSystem | PAG	Preprocessor relevant configuration parameters for controlling the model components for the administration of Privileged Account Management systems. If the parameter is set, the target system components are available. Changes to this parameter require recompilation of the database.
TargetSystem | PAG | Accounts	Parameter for configuring PAM user account data.
TargetSystem | PAG | Accounts | InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo	Specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/role, employee's manager or `XUserInserted`). If no recipient can be found, the e-mail is sent to the address stored in the **TargetSystem | PAG | DefaultAddress** configuration parameter.
TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo |	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The **Employee - new user account created** mail template is used.

Configuration parameter	Meaning if Set
MailTemplateAccountName	
TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem | PAG | Accounts | MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | PAG | Accounts | PrivilegedAccount	This configuration parameter allows configuration of settings for privileged user accounts.
TargetSystem | PAG | Accounts | TransferJPegPhoto	This configuration parameter specifies whether changes to the employee's picture are published in existing user accounts. The picture is not part of default synchronization. It is only published when employee data is changed.
TargetSystem | PAG | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem | PAG | PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | PAG | PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem | PAG | PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem | PAG | PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern.

Appendix: Default project template for One Identity Safeguard

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

The template uses mappings for the following schema types.

Table 39: Mapping One Identity Safeguard schema types to tables in the One Identity Manager schema.

Schema Type in One Identity Safeguard	Table in the One Identity Manager Schema
Appliance	PAGAppliance
IdentityProvider	PAGIdentityProvider
User	PAGUser
UserGroup	PAGUsrGroup
Entitlement	PAGEntl
AccessRequestPolicy	PAGReqPolicy
AccountGroup	PAGAccGroup
Asset	PAGAsset
AssetAccount	PAGAstAccount
AssetGroup	PAGAstGroup
Directory	PAGDirectory
DirectoryAccount	PAGDirAccount

Appendix: Editing One Identity Safeguardsystem objects

The following table describes permitted editing methods for One Identity Safeguard schema types and the necessary restrictions for processing the system objects.

Table 40: Methods available for editing schema types

Schema type	Read	Paste	Delete	Refresh
Appliance (`Appliance`)	Yes	No	No	No
User account (`User`)	Yes	Yes	Yes	Yes
User group (`UserGroup`)	Yes	No	No	Yes
Identity provider `IdentityProvider`	Yes	No	No	No
`Directory`	Yes	No	No	No
Directory account (`DirectoryAccount`)	Yes	No	No	No
Asset (`Asset`)	Yes	No	No	No
Account (`AssetAccount`)	Yes	No	No	No
Asset group (`AssetGroup`)	Yes	No	No	No
Account group (`AccountGroup`)	Yes	No	No	No
Entitlement (`Entitlement`)	Yes	No	No	No
Access request policy (`AccessRequestPolicy`)	Yes	No	No	No

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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

Index

J

L

M

N

O

P

R

S

T

U