



One Identity Manager 9.1.3

Administration Guide for Privileged Account Governance

Copyright 2024 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

 **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

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

One Identity Manager Administration Guide for Privileged Account Governance
Updated - 29 April 2024, 13:54

For the most recent documents and product information, see [Online product documentation](#).

Contents

About this guide	9
Managing a Privileged Account Management system in One Identity Manager	10
Architecture overview	10
One Identity Manager users for managing Privileged Account Management	11
Configuration parameters for managing Privileged Account Management systems	13
Synchronizing a Privileged Account Management system	15
Setting up the initial synchronization of a One Identity Safeguard	16
Users and permissions for synchronizing with a One Identity Safeguard appliance ...	17
Setting up the One Identity Safeguard synchronization server	18
System requirements for the One Identity Safeguard synchronization server	19
Installing the safeguard-ps Windows PowerShell module	19
Installing One Identity Manager Service with a One Identity Safeguard connector	20
Preparing the administrative workstation for access to the One Identity Safeguard appliance	23
Preparing a remote connection server for access to the One Identity Safeguard appliance	23
Creating a synchronization project for initial synchronization of a One Identity Safeguard appliance	24
Information required for setting up a synchronization project	25
Creating an initial synchronization project for One Identity Safeguard	26
Configuring the synchronization log	30
Customizing the synchronization configuration for One Identity Safeguard	31
Configuring synchronization to a One Identity Safeguard appliance	32
Configuring synchronization of multiple One Identity Safeguard appliances	33
Changing system connection settings of One Identity Safeguard appliances	33
Editing connection parameters in the variable set	34
Editing target system connection properties	35
Adjusting the Windows PowerShell definition of the One Identity Safeguard connector	36
Updating schemas	36
Speeding up synchronization with revision filtering	38

Configuring the provisioning of memberships	38
Configuring single object synchronization	39
Accelerating provisioning and single object synchronization	40
Running synchronization	41
Starting synchronization	42
Displaying synchronization results	43
Deactivating synchronization	44
Synchronizing single objects	44
Tasks following synchronization	45
Post-processing outstanding objects	46
Adding custom tables to the target system synchronization	48
Managing PAM user accounts through account definitions	48
Troubleshooting	49
Ignoring data error in synchronization	49
Pausing handling of target system specific processes (Offline mode)	50
Managing PAM user accounts and employees	52
Account definitions for PAM user accounts	53
Creating account definitions	54
Editing account definitions	54
Main data for account definitions	55
Editing manage levels	57
Creating manage levels	58
Assigning manage levels to account definitions	59
Main data for manage levels	60
creating mapping rules for IT operating data	60
Entering IT operating data	62
Modify IT operating data	63
Assigning account definitions to employees	64
Assigning account definitions to departments, cost centers, and locations	65
Assigning account definitions to business roles	66
Assigning account definitions to all employees	66
Assigning account definitions directly to employees	67
Assigning account definitions to system roles	67
Adding account definitions in the IT Shop	68
Assigning account definitions to PAM appliances	70

Deleting account definitions	70
Assigning employees automatically to PAM user accounts	73
Editing search criteria for automatic employee assignment	75
Finding employees and directly assigning them to user accounts	76
Changing manage levels for PAM user accounts	78
Assigning account definitions to linked PAM user accounts	78
Manually linking employees to PAM user accounts	79
Supported user account types	80
Default user accounts	81
Administrative user accounts	82
Providing administrative user accounts for one employee	82
Providing administrative user accounts for several employees	83
Privileged user accounts	84
Specifying deferred deletion for PAM user accounts	86
Managing assignments of PAM user groups	87
Assigning PAM user groups to PAM user accounts in One Identity Manager	87
Prerequisites for indirect assignment of PAM groups to PAM user accounts	88
Assigning PAM user groups to departments, cost centers, and locations	89
Assigning PAM user groups to business roles	91
Adding PAM user groups to system roles	92
Adding PAM user groups to the IT Shop	93
Adding local PAM user groups to the IT Shop automatically	94
Assigning PAM user accounts directly to a PAM user group	96
Assigning PAM user groups directly to a PAM user account	96
Effectiveness of membership in PAM user groups	97
PAM user group inheritance based on categories	99
Overview of all assignments	102
Login information for PAM user accounts	104
Password policies for PAM users	104
Predefined password policies	105
Using password policies	106
Editing password policies	107
Creating password policies	108
General main data for password policies	108

Policy settings	109
Character classes for passwords	110
Custom scripts for password requirements	112
Checking passwords with a script	112
Generating passwords with a script	113
Editing the excluded list for passwords	115
Checking passwords	115
Testing the generation of passwords	115
Initial password for new PAM user accounts	116
Email notifications about login data	116
Mapping of PAM objects in One Identity Manager	118
PAM appliances	118
Creating PAM appliances	119
Editing the main data of PAM appliances	119
General main data of PAM appliances	120
Defining categories for the inheritance of PAM user groups	121
Editing the synchronization project for a PAM appliance	122
Displaying the PAM appliance overview	122
PAM user accounts	123
Creating local PAM user accounts	124
Creating certificate-based PAM user accounts	125
Creating PAM user accounts for directory users	125
Editing main data of PAM user accounts	127
General main data of PAM user accounts	127
Contact information for PAM user accounts	132
Secondary authentication for PAM user accounts	133
Administrative entitlements for PAM user accounts	133
Assigning extended properties to PAM user accounts	134
Disabling PAM user accounts	135
Deleting and restoring PAM user accounts	136
Displaying the PAM user account overview	137
PAM user groups	137
Editing main data of PAM user groups	138
General main data of PAM user accounts	138
Administrative entitlements for PAM user groups	139

Assigning extended properties to PAM user groups	140
Displaying the PAM user group overview	141
PAM assets	141
PAM asset groups	142
PAM asset accounts	142
PAM directory accounts	143
PAM account groups	144
PAM directories	145
PAM entitlements	146
PAM access request policies	147
Reports about PAM objects	147
PAM access requests	150
System requirements for requesting PAM access requests	150
Requesting PAM access requests	151
PAM object owners	153
Automatically determining the owners	153
Manually specifying employees as PAM object owners	154
Manually specifying application roles for PAM object owners	155
Configuring PAM access request policies	156
Handling of PAM objects in the Web Portal	157
Basic data for managing a Privileged Account Management system	159
Target system managers for PAM systems	160
Job server for PAM-specific process handling	162
Editing PAM Job servers	163
General main data of Job servers	163
Specifying server functions	166
Appendix: Configuration parameters for managing a Privileged Account Management system	168
Appendix: Default project template for One Identity Safeguard	171
Appendix: Editing One Identity Safeguard system objects	172
Appendix: One Identity Safeguard connector settings	173
Appendix: Known issues about connecting One Identity Safeguard appli- ances	175

About us	177
Contacting us	177
Technical support resources	177
Index	178

About this guide

The *One Identity Manager Administration Guide for Privileged Account Governance* describes how you set up synchronization of One Identity Safeguard with One Identity Manager. You will discover, which user accounts, user groups, assets, asset groups, accounts, account groups, directories, entitlements, and access request policies of a Privileged Account Management system are mapped in One Identity Manager.

This guide is intended for end users, system administrators, consultants, analysts, and any other IT professionals using the product.

NOTE: This guide describes One Identity Manager functionality available to the default user. It is possible that not all the functions described here are available to you. This depends on your system configuration and permissions.

Available documentation

You can access One Identity Manager documentation in the Manager and in the Designer by selecting the **Help > Search** menu item. The online version of One Identity Manager documentation is available on the Support Portal under [Technical Documentation](#). You will find videos with additional information at www.YouTube.com/OneIdentity.

Managing 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. Through 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 not performed in One Identity Manager but in the Privileged Account Management. User groups and requests for passwords and sessions can be requested through the Web Portal.

One Identity Manager provides company employees with the user accounts required to allow you to use different mechanisms for connecting 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 One Identity Manager systems are mapped in Privileged Account Management. 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.

NOTE: The Privileged Account Governance Module must be installed as a prerequisite for managing Privileged Account Management systems in One Identity Manager. For more information about installing, see the *One Identity Manager Installation Guide*.

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 Privileged Account Management

The following users are included in setting up and administration of Privileged Account Management.

Table 1: Users

Users	Tasks
Target system administrators	<p>Target system administrators must be assigned to the Target systems Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Administer application roles for individual target system types.• Specify the target system manager.• Set up other application roles for target system managers if required.• Specify which application roles for target system managers are mutually exclusive.• Authorize other employees to be target system administrators.• Do not assume any administrative tasks within the target system.
Target system managers	<p>Target system managers must be assigned to the Target systems Privileged account management application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects.• Edit password policies for the target system.

Users

Tasks

	<ul style="list-style-type: none">• Prepare groups to add to the IT Shop.• Can add employees who have another identity than the Primary identity.• Configure synchronization in the Synchronization Editor and define 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	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none">• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.• Enable or disable additional configuration parameters in the Designer as required.• Create custom processes in the Designer as required.• Create and configure schedules as required.• Create and configure password policies as required.
Product owner for the IT Shop	<p>Product owners must be assigned to the Request & Fulfillment IT Shop Product owners application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Approve through requests.• Edit service items and service categories under their management. <p>The Request & Fulfillment IT Shop Product owner PAM user groups is used when local PAM user groups are</p>

Users	Tasks
Owners of privileged objects	<p>automatically added to the IT Shop.</p> <p>Owners of privileged objects, such as PAM assets, PAM asset accounts, PAM directory accounts, PAM asset groups, and PAM account groups must be assigned to an application role under the Privileged Account Governance Asset and account owners application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Make decisions about requesting access requests for privileged objects. • Attest the possible user access to these privileged objects.
Administrators for the IT Shop	<p>Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to IT Shop structures.
Administrators for organizations	<p>Administrators must be assigned to the Identity Management Organizations Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to departments, cost centers, and locations.
Business roles administrators	<p>Administrators must be assigned to the Identity Management Business roles Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to business roles.

Configuration parameters for managing Privileged Account Management systems

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. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

For more information, see [Configuration parameters for managing a Privileged Account Management system](#) on page 168.

Synchronizing a Privileged Account Management system

One Identity Manager supports synchronization with One Identity Safeguard version 6.0 or later. You will find a matching Windows PowerShell module for each version supported on the One Identity Manager installation medium in the `Modules\PAG\dvd\AddOn\safeguard-ps` directory. Versions without a matching Windows PowerShell module on the One Identity Manager installation medium, are not supported.

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

This sections explains how to:

- Set up synchronization to import initial data from One Identity Safeguard appliance to the One Identity Manager database.
- Adjust a synchronization configuration, for example, to synchronize different One Identity Safeguard appliances with the same synchronization project.
- Start and deactivate the synchronization.
- Analyze synchronization results.

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

Detailed information about this topic

- [Setting up the initial synchronization of a One Identity Safeguard](#) on page 16
- [Customizing the synchronization configuration for One Identity Safeguard](#) on page 31
- [Running synchronization](#) on page 41
- [Tasks following synchronization](#) on page 45
- [Troubleshooting](#) on page 49
- [Ignoring data error in synchronization](#) on page 49
- [Editing One Identity Safeguard system objects](#) on page 172
- [Known issues about connecting One Identity Safeguard appliances](#) on page 175

Setting up the initial synchronization of a 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.
 - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.
NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
 - 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 a 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 17](#)
- [Setting up the One Identity Safeguard synchronization server on page 18](#)
- [Preparing the administrative workstation for access to the One Identity Safeguard appliance on page 23](#)
- [Preparing a remote connection server for access to the One Identity Safeguard appliance on page 23](#)
- [Creating a synchronization project for initial synchronization of a One Identity Safeguard appliance on page 24](#)

- [Configuration parameters for managing a Privileged Account Management system](#) on page 168
- [Default project template for One Identity Safeguard](#) on page 171

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)	<p>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.</p> <ul style="list-style-type: none"> • Authentication provider Certificate • Thumbprint of a certificate saved on the appliance as a trusted certificate • Permissions: <ul style="list-style-type: none"> • Authorizer • User • Help Desk • Appliance • Operations • Asset • Directory • Security policy <p>For more information about users and certificates in One Identity Safeguard, see the <i>One Identity Safeguard Administration Guide</i>.</p>
One Identity Manager Service user account	<p>The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files).</p> <p>The user account must belong to the Domain users group.</p> <p>The user account must have the Login as a service extended user permissions.</p> <p>The user account requires permissions for the internal web service.</p>

User	Permissions
User for accessing the One Identity Manager database	<p>NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can grant permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (on 32-bit operating systems) • %ProgramFiles%\One Identity (on 64-bit operating systems) <p>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.</p> <p>For more information about certificates in One Identity Safeguard, see the <i>One Identity Safeguard Administration Guide</i>.</p> <p>NOTE: Access through the NT AUTHORITY\SYSTEM local system account is not supported.</p>
	The Synchronization default system user is provided to run synchronization using an application server.

Setting up the One Identity Safeguard synchronization server

All One Identity Manager Service actions are run 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 19

- [Installing the safeguard-ps Windows PowerShell module](#) on page 19
- [Installing One Identity Manager Service with a One Identity Safeguard connector](#) on page 20

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
The following versions are supported:
 - Windows Server 2022
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
- Microsoft .NET Framework version 4.8 or later
| **NOTE:** Take the target system manufacturer's recommendations into account.
- Windows PowerShell version 5 or later
- Windows PowerShell Module **safeguard-ps**

Related topics

- [Installing the safeguard-ps Windows PowerShell module](#) on page 19

Installing the safeguard-ps Windows PowerShell module

You will find the Windows PowerShell modules for supporting One Identity Safeguard versions on the One Identity Manager installation medium in the Modules\PAG\dvd\AddOn\safeguard-ps directory.

| **IMPORTANT:** Ensure that the major and the minor version of the Windows PowerShell module match the major and the minor version of your One Identity Safeguard appliance.

To install the Windows PowerShell module

1. Create a subdirectory called safeguard-ps, in the server's %ProgramFiles%\WindowsPowerShell\Modules directory.

2. Copy the directory with the Windows PowerShell module matching the version from the Modules\PAG\dvd\AddOn\safeguard-ps directory on the One Identity Manager installation medium to the %ProgramFiles%\WindowsPowerShell\Modules\safeguard-ps directory on the server.

Installing One Identity Manager Service with a One Identity Safeguard connector

The One Identity Manager Service must be installed on the synchronization server with the One Identity Safeguard connector. The synchronization server must be declared as a Job server in 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 recommended that you set up a Job server for each target system for performance reasons. 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).

To set up a Job server, perform the following steps.

1. Create a Job server and install and configure the One Identity Manager Service.

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

- Sets up a Job server.
- Specifies machine roles and server function for the Job server.
- Installs One Identity Manager Service components corresponding to the machine roles.
- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

Use the Server Installer to install the One Identity Manager Service locally or remotely.

To remotely install the One Identity Manager Service, provide an administrative workstation on which the One Identity Manager components are installed. Ensure that the One Identity Manager components are installed on the server before installing locally. For more information about installing One Identity Manager components, see the *One Identity Manager Installation Guide*.

2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.
3. To generate processes for the Job server, you need the provider, connection parameters and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For more information about connection data, see the *One Identity Manager Configuration Guide*.

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

1. Start the Server Installer program.

NOTE: To install remotely, start the Server Installer program on your administrative workstation. To install locally, start the program on the server.

2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

You can connect via the application server or directly to connect to the database.

3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.

- 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.

- **Server:** Name of the Job server.
- **Queue:** Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact 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.

Syntax:

<Name of server>.<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 the Designer.

4. On the **Machine roles** page, select **Privileged Account Management**.
5. On the **Server functions** page, select **One Identity Safeguard connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

For a direct connection to the database:

- a. In the module list, select **Process collection > sqlprovider**.
- b. Click the **Connection string** entry, then click the **Edit** button.
- c. Enter the connection data for the One Identity Manager database.
- d. Click **OK**.

For a connection to the application server:

- a. In the module list, select the **Process collection** entry and click the **Insert** button.
 - b. Select **AppServerJobProvider** and click **OK**.
 - c. In the module list, select **Process collection > AppServerJobProvider**.
 - d. Click the **Connection string** entry, then click the **Edit** button.
 - e. Enter the address (URL) for the application server and click **OK**.
 - f. Click the **Authentication string** entry and click the **Edit** button.
 - g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
 - h. Click **OK**.
7. To configure the installation, click **Next**.
 8. Confirm the security prompt with **Yes**.
 9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
 10. On the **Service access** page, enter the service's installation data.
 - **Computer:** Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.
To run the installation locally, select **Local installation** from the menu.
 - **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

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

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

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

NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

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

To configure synchronization with a Synchronization Editor appliance in One Identity Safeguard, 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**

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 information about certificates in One Identity Safeguard, see the *One Identity Safeguard Administration Guide*.

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

Related topics

- [Installing the safeguard-ps Windows PowerShell module](#) on page 19
- [Users and permissions for synchronizing with a One Identity Safeguard appliance](#) on page 17
- [Preparing a remote connection server for access to the One Identity Safeguard appliance](#) on page 23

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 the target

system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, 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
- 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 installing the **RemoteConnectPlugin** as well.

For more detailed information about establishing 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 18
- [Installing the safeguard-ps Windows PowerShell module](#) on page 19
- [Installing One Identity Manager Service with a One Identity Safeguard connector](#)
- [Users and permissions for synchronizing with a One Identity Safeguard appliance](#) on page 17
- [Preparing the administrative workstation for access to the One Identity Safeguard appliance](#) on page 23

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

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and a One Identity Safeguard appliance. The following describes the steps for initial configuration of a synchronization project. For more 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 25
- [Creating an initial synchronization project for One Identity Safeguard](#) on page 26
- [Preparing the administrative workstation for access to the One Identity Safeguard appliance](#) on page 23
- [Preparing a remote connection server for access to the One Identity Safeguard appliance](#) on page 23
- [One Identity Safeguard connector settings](#) on page 173

Information required for setting up a synchronization project

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

Table 4: 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. If you use a cluster of multiple One Identity Safeguard appliances, enter the primary appliance here. NOTE: This value must be adjusted if the primary appliance changes in the cluster. If the Always connect to the primary cluster node option is set in the system connection wizard, the primary appliance is calculated automatically.
Trusted certificate thumbprint	Thumbprint 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 17.
Synchronization server for the appliance	All One Identity Manager Service actions are run 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.

Data	Explanation
	<p>The One Identity Manager Service with the One Identity Safeguard connector must be installed on the synchronization server.</p> <p>The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.</p> <ul style="list-style-type: none"> • Server function: One Identity Safeguard connector • Machine role: Server Job Server Privileged Account Management <p>For more information, see Setting up the One Identity Safeguard synchronization server on page 18.</p>
One Identity Manager database connection data	<ul style="list-style-type: none"> • Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p>
Remote connection server	<p>For more information, see Preparing a remote connection server for access to the One Identity Safeguard appliance on page 23.</p>

Creating an initial synchronization project for One Identity Safeguard

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

- Run in default mode
- Started from the Launchpad

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

NOTE: Just one synchronization project can be created per target system and default project template used.

To set up an initial synchronization project for One Identity Safeguard

1. Start the Launchpad and log in on the One Identity Manager database.
 - NOTE:** If synchronization is run by an application server, connect the database through the application server.
2. Select the **Target system type Privileged Account Management** entry and click **Start**.

This starts the Synchronization Editor's project wizard.

3. On the **System access** page, specify how One Identity Manager can access the target system.
 - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
 - If access is not possible from the workstation on which you started the 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**.
4. On the **Connection parameters** page, enter the following information:
 - **Appliance hostname or IP:** Enter the host name or IP address of the appliance. If you use a cluster of multiple One Identity Safeguard appliances, enter the primary appliance here.
 - NOTE:** This value must be adjusted if the primary appliance changes in the cluster. On the **Description of the appliance** page, if the **Always connect to the primary cluster node** option is set, the primary appliance is calculated automatically.
 - **Trusted certificate thumbprint:** Enter the thumbprint 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.
5. On the **Description of the appliance** page, enter the following information:
 - **Appliance display name:** Enter a name for displaying in One Identity Manager tools.
 - **System identifier:** Enter a unique identifier to identify the device.

⚠ CAUTION: The system identifier must describe the appliance uniquely. Appliances are differentiated on the basis of the system identifier. If you use an identifier more than once for different appliances, it can cause errors and loss of data.

- **Always connect to the primary cluster node:** This option is automatically set if a One Identity Safeguard cluster is identified when the connection is tested. If you use a cluster of multiple One Identity Safeguard appliances, this option should be enabled.
6. 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.
 7. 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.
 8. 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.
 9. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 5: Specify target system access

Option	Meaning
	<p>Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none"> • 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.
<p>Read/write access to target system. Provisioning available.</p>	<p>Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization is in the direction of the Target

Option	Meaning
--------	---------

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.

10. On the **Synchronization server** page, select the synchronization server to run the synchronization.

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.

- Click  to add a new Job server.
- Enter a name for the Job server and the full server name conforming to DNS syntax.
- 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.

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

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

This sets up, saves and immediately activates the synchronization project.

NOTE:

- If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.

Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.

- 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.
- The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

Related topics

- [Information required for setting up a synchronization project on page 25](#)
- [Users and permissions for synchronizing with a One Identity Safeguard appliance on page 17](#)
- [Setting up the One Identity Safeguard synchronization server on page 18](#)
- [Configuring the synchronization log on page 30](#)
- [Customizing the synchronization configuration for One Identity Safeguard on page 31](#)
- [Tasks following synchronization on page 45](#)
- [Default project template for One Identity Safeguard on page 171](#)
- [One Identity Safeguard connector settings on page 173](#)
- [Known issues about connecting One Identity Safeguard appliances on page 175](#)

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 **Configuration > Target system** category in the Synchronization Editor.

- OR -

To configure the synchronization log for the database connection, select the **Configuration > One Identity Manager connection** category in the 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 analyzes.

5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- [Displaying synchronization results](#) on page 43

Customizing the synchronization configuration for One Identity Safeguard

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a One Identity Safeguard appliance, you can use the 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 compare the One Identity Safeguard appliance on a regular basis and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- To specify which PAM objects and database objects 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 method, 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 more 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 32](#)
- [Configuring synchronization of multiple One Identity Safeguard appliances on page 33](#)
- [Changing system connection settings of One Identity Safeguard appliances on page 33](#)
- [Updating schemas on page 36](#)
- [Configuring the provisioning of memberships on page 38](#)
- [Configuring single object synchronization on page 39](#)
- [Accelerating provisioning and single object synchronization on page 40](#)

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 primary system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing to the appliance

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.
This creates a workflow with **Target system** as its direction of synchronization.
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 33](#)

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 parameters 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. In the Synchronization Editor, open the synchronization project.
3. Create a new base object for the appliance.
 - Use the wizard to attach a base object.
 - In the wizard, select the One Identity Safeguard connector.
 - Declare the connection parameters. The connection parameters are saved in a special variable set.

A start up configuration is created that 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 32

Changing system connection settings of One Identity Safeguard appliances

When you set up synchronization for the first time, the system connection properties are set to default values that you can modify. There are two ways to do this:

- a. Specify a specialized variable set and change the values of the affected variables.
The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).
- b. Edit the target system connection with the system connection wizard and change the effected values.
The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- [Editing connection parameters in the variable set](#) on page 34
- [Editing target system connection properties](#) on page 35
- [Adjusting the Windows PowerShell definition of the One Identity Safeguard connector](#) on page 36
- [One Identity Safeguard connector settings](#) on page 173

Editing connection parameters in the variable set

The connection parameters were saved as variables in the default variable set when synchronization was set up. You can change the values in these variables to suit your requirements and assign the variable set to a start up configuration and a base object. This means that you always have the option to use default values from the default variable set.

NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project is used for synchronizing different One Identity Safeguard appliances.

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.
Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.
All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on  in the variable set view's toolbar.
 - To rename the variable set, select the variable set and click the variable set view in the toolbar . Enter a name for the variable set.
7. Select the previously added variable and enter a new value.

8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration > Base objects** category.
13. Select the base object and click .
- OR -
- To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

For more information about using variables and variable sets, or restoring default values and adding base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [Editing target system connection properties](#) on page 35

Editing target system connection properties

You can also use the system connection wizard to change the connection parameters. If variables are defined for the settings, the changes are transferred to the active variable set.

NOTE: In the following circumstances, the default values cannot be restored:

- The connection parameters are not defined as variables.
- The default variable set is selected as an active variable set.

In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit connection parameters using the system connection wizard

1. In the Synchronization Editor, open the synchronization project.
2. In the toolbar, select the active variable set to be used for the connection to the target system.

NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.

3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.

This starts the system connection wizard.

5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- [Editing connection parameters in the variable set](#) on page 34

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. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
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. Follow the system connection wizard further instructions.
7. Save the changes.

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 the loading of 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 compression 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. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
- OR -
Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.
Opens the Mapping Editor. For more 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, such as 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 may be overwritten. This behavior can occur under the following conditions:

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

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and 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 the **Privileged Account Management > Basic configuration data > Target system types** category.
2. In the result list, select the **Privileged Account Management** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.

NOTE:

- This option can only be enabled for assignment tables that have a base table with a XDateSubItem column.

- Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.

6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. Therefore, only newly added and deleted assignments are processed. 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 not the entire members list.

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.

You can restrict single provisioning of memberships with a condition. Once merge mode has been disabled for a table, the condition is deleted. Tables that have had the condition deleted or edited are marked with the following icon: . You can restore the original condition at any time.

To restore the original condition

1. Select the auxiliary table for which you want to restore the condition.
2. Right-click on the selected row and select the **Restore original values** context menu item.
3. Save the changes.

NOTE: To create the reference to the added or deleted assignments in the condition, use the *i* table alias.

Example of a condition on the PAGUserInUsrGroup assignment table:

```
exists (select top 1 1 from PAGUsrGroup g
        where g.UID_PAGUsrGroup = i.UID_PAGUsrGroup
        and <limiting condition>)
```

For more 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 membership list belongs to one of these properties, the entries in the assignment 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 more information about this, see the *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 the **Privileged Account Management > Basic configuration data > Target system types** category.
2. In the result list, select the **Privileged Account Management** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
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 44
- [Post-processing outstanding objects](#) on page 46

Accelerating provisioning and single object synchronization

To smooth out spikes in data traffic, handling of processes for provisioning and single object synchronization can be distributed over several Job servers. This will also accelerate these processes.

NOTE: You should not implement load balancing for provisioning or single object synchronization on a permanent basis. Parallel processing of objects might result in dependencies not being resolved because referenced objects from another Job server

have not been completely processed.

Once load balancing is no longer required, ensure that the synchronization server runs the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
 - Job servers that share processing must have the **No process assignment** option enabled.
 - Assign the **One Identity Safeguard connector** server function to the Job server.

All Job servers must access the same appliance as the synchronization server for the respective base object.

2. In the Synchronization Editor, assign a custom server function to the base object.

This server function is used to identify all the Job servers being used for load balancing.

If there is no custom server function for the base object, create a new one.

For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

Only select those Job servers that have the same configuration as the base object's synchronization server.

Once all the processes have been handled, the synchronization server takes over provisioning and single object synchronization again.

To use the synchronization server without load balancing.

- In the Synchronization Editor, remove the server function from the base object.

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

Detailed information about this topic

- [Editing PAM Job servers](#) on page 163

Running 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 stopped unexpectedly, you must reset the start information to be able to restart synchronization.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Starting synchronization](#) on page 42
- [Displaying synchronization results](#) on page 43
- [Deactivating synchronization](#) on page 44
- [Synchronizing single objects](#) on page 44
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 50

Starting synchronization

When you set up the initial synchronization project using the Launchpad, a default schedule for regular synchronization is created and assigned. Activate this schedule to synchronize on a regular basis.

To synchronize on a regular basis

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
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. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
 - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
 - Use the schedule to ensure that the start up configurations are run in sequence.
 - Group start up configurations with the same start up behavior.

Displaying 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. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
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 it.
An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
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 it.
An analysis of the provisioning is shown as a report. You can save the report.

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

TIP: The logs are also displayed in the Manager under the **<target system>** **synchronization log** category.

Related topics

- [Configuring the synchronization log](#) on page 30
- [Troubleshooting](#) on page 49

Deactivating synchronization

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

To prevent regular synchronization

1. In the Synchronization Editor, open the synchronization project.
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 extent. 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. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Related topics

- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 50

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 membership list belongs to one of these properties, the entries in the assignment 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 the 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 the **Synchronize this object** task.

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

Features of synchronizing memberships

If you synchronize changes in an object's member list, run single object synchronization on the assignment's root object. The base table of an assignment contains an XDateSubItem column containing information about the last change to the memberships.

Example:

Base object for assigning PAM user accounts to PAM user groups is the user group.

In the target system, a user account was assigned to a group. To synchronize this assignment, in the Manager, select the group that the user account was assigned to and run single object synchronization. In the process, all of the group's memberships are synchronized.

The user account must already exist as an object in the One Identity Manager database for the assignment to be made.

Detailed information about this topic

- [Configuring single object synchronization](#) on page 39

Tasks following 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 46
- [Adding custom tables to the target system synchronization](#) on page 48
- [Managing PAM user accounts through account definitions](#) on page 48

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 synchronizations.
- 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.

The navigation view lists all the synchronization tables assigned to the **Privileged Account Management** target system type.

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 run. 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 from the target system.
The base object of the assignment was 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 from the target system.
During synchronization, the object and all corresponding entries in the 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

1. Select the object on the target system synchronization form.
2. Open the context menu and click **Show object**.
3. Select the objects you want to rework. Multi-select is possible.
4. Click on one of the following icons in the form toolbar to run the respective method.

Table 6: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The Outstanding label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: <ul style="list-style-type: none">• The table containing the object can be published.• The target system connector has write access to the target 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 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

- Disable the  icon in the form's 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. That means, the **Connection is read-only** option must not be set for the target system connection.

Adding custom tables to the target system synchronization

You must customize your target system synchronization to synchronize custom tables.

To add custom tables to target system synchronization

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Target system types** category.
2. In the result list, select the **Privileged Account Management** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

Related topics

- [Post-processing outstanding objects](#) on page 46

Managing PAM user accounts through account definitions

In the default installation, after synchronizing, employees are automatically created for the user accounts. 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 PAM user accounts](#) on page 78

Troubleshooting

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**
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 stopped 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

- [Displaying synchronization results](#) on page 43

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > One Identity Manager connection** category.
3. In the **General** view, click **Edit connection**.
This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

This option is only effective if **Continue on error** is set in the synchronization workflow.

Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.

5. Save the changes.

IMPORTANT: If this option is set, One Identity Manager tries to ignore commit errors that could be related to data errors in a single column. This causes the data changed in the affected column to be discarded and the object is subsequently saved again. This effects performance and leads to loss of data.

Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

Pausing handling of target system specific processes (Offline mode)

If a target system connector is not able to reach the target system temporarily, you can enable offline mode for the target system. This stops target system specific processes from being frozen and having to be manually re-enabled later.

Whether offline mode is generally available for a target system connection is set in the base object of the respective synchronization project. Once a target system is truly unavailable, the target system connection can be switched offline and online again with the Launchpad.

In offline mode, all Job servers assigned to the base object are stopped. This includes the synchronization server and all Job servers involved in load balancing. If one of the Job servers also handles other tasks, these are not processed either.

Prerequisites

Offline mode can only be specified for a base object if certain prerequisites are fulfilled.

- The synchronization server is not used for any other base object as a synchronization server.
- If a server function is assigned to the base object, none of the Job servers with this server function may have any other server function (for example, update server).
- A dedicated synchronization server must be set up to exclusively process the Job queue for this base object. The same applies to all Job servers that are determined by the server function.

To allow offline mode for a base object

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Base objects** category.
3. Select a base object in the document view and click .

4. Enable **Offline mode available**.
5. Click **OK**.
6. Save the changes.

IMPORTANT: To prevent data inconsistencies, the offline phase should be kept as short as possible.

The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and the target system, all pending processes must be handled before synchronization can start.

Only use offline mode, if possible, for short system downtimes such as maintenance windows.

To flag a target system as offline

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select **Manage > System monitoring > Flag target systems as offline**.
3. Click **Run**.

This opens the **Manage offline systems** dialog. The **Base objects** section displays the base objects of target system connections that can be switched to offline.

4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

This stops all the Job servers assigned to the base object. No more synchronization or provisioning Jobs are performed. The Job Queue Info program shows when a Job server has been switched offline and the corresponding tasks are not being processed.

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

Related topics

- [Deactivating synchronization](#) on page 44

Managing PAM user accounts and employees

The main feature of One Identity Manager is to map employees together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing 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 methods 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 mechanisms 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 main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

For more 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 53](#)
- [Assigning employees automatically to PAM user accounts on page 73](#)
- [Assigning account definitions to linked PAM user accounts on page 78](#)
- [Supported user account types on page 80](#)
- [Specifying deferred deletion for PAM user accounts on page 86](#)
- [PAM user accounts on page 123](#)

Account definitions for PAM user accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees. 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.

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a central user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role. Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

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
- Collecting IT operating data
- Assigning account definitions to employees and target systems

Detailed information about this topic

- [Creating account definitions](#) on page 54
- [Editing account definitions](#) on page 54
- [Main data for account definitions](#) on page 55
- [Editing manage levels](#) on page 57
- [Creating manage levels](#) on page 58
- [Main data for manage levels](#) on page 60
- [creating mapping rules for IT operating data](#) on page 60
- [Entering IT operating data](#) on page 62
- [Modify IT operating data](#) on page 63
- [Assigning account definitions to employees](#) on page 64
- [Assigning account definitions to PAM appliances](#) on page 70
- [Deleting account definitions](#) on page 70

Creating account definitions

To create a new account definition

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Related topics

- [Main data for account definitions](#) on page 55
- [Editing account definitions](#) on page 54
- [Assigning manage levels to account definitions](#) on page 59

Editing account definitions

To edit an account definition

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

3. Select the **Change main data** task.
4. Enter the account definition's main data.
5. Save the changes.

Related topics

- [Main data for account definitions](#) on page 55
- [Creating account definitions](#) on page 54
- [Assigning manage levels to account definitions](#) on page 59

Main data for account definitions

Enter the following data for an account definition:

Table 7: Main 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	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. 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	Text field 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 assigning the account definition to employees. Set a value in the range 0 to 1 . This input field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .

Property	Description
Service item	Service item through which you can request the account definition resource 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 requested by an employee through the Web Portal and distributed using a defined approval process. The resource can also be assigned directly to employees and roles outside the 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 requested by an employee through the Web Portal and distributed using a defined approval process. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	<p>Specifies whether the account definition is automatically assigned to all internal employees. To automatically assign the account definition to all internal employee, use the Enable automatic assignment to employees. The account definition is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this account definition.</p> <p>To automatically remove the account definition assignment from all employees, use the Disable automatic assignment to employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</p>
Retain account definition if permanently disabled	<p>Specifies the account definition assignment to permanently deactivated employees.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition if temporarily disabled	<p>Specifies the account definition assignment to temporarily deactivated employees.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees.

Property	Description
	<p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on security risk	<p>Specifies the account definition assignment to employees posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • 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.

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 not 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 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.

NOTE: The **Full managed** and **Unmanaged** manage levels are analyzed in templates. You can customize the supplied templates in the Designer.

You can define other manage levels depending on your requirements. You need to amend the templates to include manage level approaches.

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. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

- Employee user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the employee is reinstated at a later date, the user accounts are also reactivated.
- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted.

To edit a manage level

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

Related topics

- [Main data for manage levels](#) on page 60
- [Creating manage levels](#) on page 58
- [Assigning manage levels to account definitions](#) on page 59

Creating manage levels

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

To create a manage level

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Manage levels** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the manage level.
4. Save the changes.

Related topics

- [Main data for manage levels](#) on page 60
- [Editing manage levels](#) on page 57
- [Assigning manage levels to account definitions](#) on page 59

Assigning manage levels to account definitions

IMPORTANT: The **Unmanaged** manage level is assigned automatically when you create an account definition and it cannot be removed.

To assign manage levels to an account definition

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage level.

TIP: In the **Remove assignments** pane, you can remove assigned manage levels.

To remove an assignment

- Select the manage level and double-click .
5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 8: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <ul style="list-style-type: none">• Never: Data is not updated. (Default)• Always: Data is always updated.• Only initially: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated 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.
Retain groups if user account disabled	Specifies whether disabled 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 automatically creating user accounts for an employee in the target system and modifying them.

- PAM authentication provider
- PAM identity provider
- PAM secondary authentication
- PAM administrative entitlements
- Groups can be inherited
- Identity
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
 - **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 more information about this, see the *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: The business role can only be used if the Business Roles Module is available.
 - Empty

If you select a role, you must specify a default value and set the **Always use default value** option.

 - **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 the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
 - **Notify when applying the default:** Specifies whether an email is sent to a specific mailbox when the default value is used. The **Employee - new user**

account with default properties created mail template is used.

To change the mail template, in the Designer, adjust the **TargetSystem | PAG | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Related topics

- [Entering IT operating data](#) on page 62
- [Modify IT operating data](#) on page 63

Entering IT operating data

To create user accounts for an employee with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An employee is assigned a primary business role, primary location, primary department, or primary cost center. 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 appliance A. In addition, certain employees in department A obtain administrative user accounts in the appliance A.

Create an account definition A for the default user account of the appliance A and an account definition B for the administrative user account of appliance A. In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property 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, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

To define IT operating data

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

- **Effects on:** Specify an 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 field.
 - b. Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.
 - c. Select the specific target system or account definition under **Effects on**.
 - d. Click **OK**.
- **Column:** Select the 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 more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
 - **Value:** Enter a fixed value to assign to the user account's property.

4. Save the changes.

Related topics

- [creating mapping rules for IT operating data](#) on page 60
- [Modify IT operating data](#) on page 63

Modify IT operating data

If IT operating data changes, you must transfer the 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, a cost center, a business role, or a location have been 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, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

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

This displays a list of all user accounts that were created with the selected account definition and whose properties were changed by modifying the IT operating data. That means:

- **Old value:** Value of the object property before changing the IT operating data.
 - **New value:** Value of the object property after changing the IT operating data.
 - **Selection:** Specifies whether the new value is copied to 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. Department managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or added directly to the IT Shop as products.

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. In this case, you must change the user account manage level afterward.

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 account definition assignment is removed, the user account that was created from this account definition, is deleted.

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (departments, cost centers, locations, or business roles).

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

For more 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 65
- [Assigning account definitions to business roles](#) on page 66
- [Assigning account definitions to all employees](#) on page 66
- [Assigning account definitions directly to employees](#) on page 67
- [Assigning account definitions to system roles](#) on page 67
- [Adding account definitions in the IT Shop](#) on page 68

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.

4. In the **Add assignments** pane, assign the organizations:

- On the **Departments** tab, assign departments.
- On the **Locations** tab, assign locations.
- On the **Cost centers** tab, assign cost centers.

TIP: In the **Remove assignments** pane, you can remove assigned organizations.

To remove an assignment

- Select the organization and double-click .

5. Save the changes.

Assigning account definitions to business roles

NOTE: This function is only available if the Business Roles Module is installed.

To add account definitions to hierarchical roles

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

TIP: In the **Remove assignments** pane, you can remove assigned business roles.

To remove an assignment

- Select the business role and double-click .

5. Save the changes.

Assigning account definitions to all employees

Use this task to assign the account definition to all internal employees. Employees that are marked as external do not obtain this account definition. Once a new internal employee is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

IMPORTANT: Only run this task 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.

To assign an account definition to all employees

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to employees** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all employees, run the **DISABLE AUTOMATIC ASSIGNMENT TO EMPLOYEES** task. 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 the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign to employees** task.
4. In the **Add assignments** pane, add employees.

TIP: In the **Remove assignments** pane, you can remove assigned employees.

To remove an assignment

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

Assigning account definitions to system roles

NOTE: This function is only available if the System Roles Module is installed.

Account definitions with the **Only use in IT Shop** option 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 the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .

5. Save the changes.

Adding account definitions in the IT Shop

An 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 the Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in the 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 the **Only for use in IT Shop** option. 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 (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To add an account definition to the IT Shop (non role-based login)

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves (non role-based login)

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from all IT Shop shelves (role-based login)

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

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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

Related topics

- [Main data for account definitions](#) on page 55

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 (**Linked configured** state):

- 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** state) 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 the Manager, select the appliance in the **Privileged Account Management > Appliances** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Related topics

- [Assigning employees automatically to PAM user accounts](#) on page 73

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 the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. Select the **Disable automatic assignment to employees** task.
 - e. Confirm the security prompt with **Yes**.
 - f. Save the changes.
2. Remove direct assignments of the account definition to employees.
 - a. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign to employees** task.
 - d. In the **Remove assignments** pane, remove employees.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign organizations** task.
 - d. In the **Remove assignments** pane, 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 the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign business roles** task.
 - d. In the **Remove assignments** pane, remove the business roles.
 - e. 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 Designer Web Portal User Guide*.

To remove an account definition from all IT Shop shelves (role-based login)

- a. In the Manager, select the **Entitlements > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

- a. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

6. Remove the required account definition assignment. 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 the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. From the **Required account definition** menu, remove the account definition.
 - e. Save the changes.
7. Remove the account definition's assignments to target systems.

- a. In the Manager, select the appliance in the **Privileged Account Management > Appliances** category.
 - b. Select the **Change main data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
8. Delete the account definition.
- a. In the Manager, select the **Privileged Account Management > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Click  to delete an account definition.

Assigning employees automatically to PAM user accounts

When you add a user account, an existing employee can automatically be assigned to it. If necessary, a new employee can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either 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 assignments 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 main data** to assign employees to administrative user accounts for the respective user account.

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

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | PAG | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the **TargetSystem | PAG | PersonAutoDefault** configuration parameter and

select the required mode.

- In the TargetSystem | ADS | PersonExcludeList configuration parameter, **define** the user accounts for which no automatic assignment to employees shall take place.

Example:

ADMINISTRATOR|GUEST

TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic employee assignment** dialog.

To edit the exclude list for automatic employee assignment

1. In the Designer, edit the **PersonExcludeList** configuration parameter.
2. Click ... next to the **Value** field.
This opens the **Exclude list for PAM user accounts** dialog.
3. To add a new entry, click  **Add**.
To edit an entry, select it and click  **Edit**.
4. Enter the name of the user account that does not allow employees to be assigned automatically.

Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.

5. To delete an entry, select it and click  **Delete**.
 6. Click **OK**.
- Use the **TargetSystem | PAG | PersonAutoDisabledAccounts** configuration parameter 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:

In the default installation, after synchronizing, employees are automatically created for the user accounts. 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 48.

Related topics

- [Creating account definitions](#) on page 54
- [Assigning account definitions to PAM appliances](#) on page 70
- [Changing manage levels for PAM user accounts](#) on page 78
- [Assigning account definitions to linked PAM user accounts](#) on page 78
- [Editing search criteria for automatic employee assignment](#) on page 75

Editing search criteria for automatic employee assignment

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.

The criteria for employee assignments are defined for the appliance. 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: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

To specify criteria for employee assignment

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

employee is linked to the user account.

Table 9: 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 more information about defining search criteria, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- [Assigning employees automatically to PAM user accounts](#) on page 73
- [Finding employees and directly assigning them to user accounts](#) on page 76

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 10: 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. In the Manager, select the **Privileged Account Management > Appliances** category.
2. Select the appliance in the result list.

3. Select the **Define search criteria for employee assignment** task.
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 main data.

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

To assign employees directly over a suggestion list

- Click **Suggested assignments**.
 1. Click the **Selection** box of 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 the **Selection** box of 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 the **Selection** box of all the user accounts you want to delete the employee assignment from. 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 the Manager, select the **Privileged Account Management > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Related topics

- [General main data of PAM user accounts](#) on page 127

Assigning account definitions to linked PAM user 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 were linked manually
- Automatic employee assignment is configured, but when a user account is inserted, no account definition is assigned in the appliance.

To manage user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the appliance.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
 - a. In the Manager, select the **Privileged Account Management > User accounts > Linked but not configured > <appliance>** category.
 - b. Select the **Assign account definition to linked accounts** task.
 - c. In the **Account definition** menu, select the account definition.
 - d. Select the user accounts that contain the account definition.
 - e. Save the changes.

Detailed information about this topic

- [Assigning account definitions to PAM appliances](#) on page 70

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 the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list and run the **Assign PAM user accounts** task.
3. Assign the user accounts.
4. Save the changes.

Related topics

- [Supported user account types](#) on page 80

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 11: 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 used for a specific purpose. For example, for training purposes.	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 personalized admin identity are used for different user accounts, which can be used by the same actual employee to perform their different tasks within the company.

To provide user accounts with a personalized 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 permissions to the different user accounts.

User accounts with a sponsored identity, shared identity, or service identity are linked to pseudo employees that do not refer to a real employee. These pseudo employees are needed so that permissions can be inherited by the user accounts.

When evaluating reports, attestations, or compliance checks, check whether pseudo employees need to be considered separately.

For more 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 labeled with the **Privileged user account** property (IsPrivilegedAccount column).

Detailed information about this topic

- [Default user accounts](#) on page 81
- [Administrative user accounts](#) on page 82
- [Providing administrative user accounts for one employee](#) on page 82
- [Providing administrative user accounts for several employees](#) on page 83
- [Privileged user accounts](#) on page 84

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 IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

The type of IT operating data required depends on the target system. The following settings are recommended for default user accounts:

- In the mapping rule for the IsGroupAccount column, use the default value **1** and enable the **Always use default value** option.

- 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 that 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 53

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, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

Related topics

- [Providing administrative user accounts for one employee](#) on page 82
- [Providing administrative user accounts for several employees](#) on page 83

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 the Manager, select the **Privileged Account Management > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - 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 the Manager, select the **Privileged Account Management > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - 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 several employees](#) on page 83
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

- The user account must be labeled as a shared identity.
- A pseudo employee must exist. The pseudo 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 the Manager, select the **Privileged Account Management > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to a pseudo employee.
 - a. In the Manager, select the **Privileged Account Management > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - d. On the **General** tab, select the pseudo employee from the **Employee** menu.
3. Assign the employees who will use this administrative user account to the user account.
 - a. In the Manager, select the **Privileged Account Management > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Assign employees authorized to use** task.
 - d. In the **Add assignments** pane, add employees.

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

TIP: In the **Remove assignments** pane, you can remove assigned employees.

To remove an assignment

- Select the employee and double-click .

Related topics

- [Providing administrative user accounts for one employee](#) on page 82
- For more 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 labeled with the **Privileged user account** property (IsPrivilegedAccount column).

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 TSB_SetIsPrivilegedAccount script.

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 are 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 the IT operating data.

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

The type of IT operating data 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 set the **Always use default value** option.
 - 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 set the **Always use default value** option.
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, specify how the login names are formatted in the template.

Related topics

- [Account definitions for PAM user accounts](#) on page 53

Specifying deferred deletion for PAM user accounts

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or blocked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is **30** days.

In the Designer, enter a different value for deferred deletion in the Deferred deletion [days] property of the **PAGUser** table.

- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

To use object-specific deferred deletion, in the Designer, create a Script (deferred deletion) for the **PAGUser** table.

Example:

Deferred deletion of privileged user accounts is 10 days. The following **Script (deferred deletion)** is entered in the table.

```
If Not $IsPrivilegedAccount:Bool$ Then
    Value = 10
End If
```

For more information on editing table definitions and configuring deferred deletion in the Designer, see the *One Identity Manager Configuration Guide*.

Managing 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. Through 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 through departments, cost centers, locations, or business roles. Users can also request the user groups through the Web Portal. To do this, the user groups are provided in the IT Shop.

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

Detailed information about this topic

- [Assigning PAM user groups to PAM user accounts in One Identity Manager](#) on page 87
- [Effectiveness of membership in PAM user groups](#) on page 97
- [PAM user group inheritance based on categories](#) on page 99
- [Overview of all assignments](#) on page 102

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. You can also group any number of company resources into a system role.

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

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	<i>One Identity Manager Identity Management Base Module Administration Guide</i> <i>One Identity Manager Business Roles Administration Guide</i>
Assigning company resources through IT Shop requests	<i>One Identity Manager IT Shop Administration Guide</i>
System roles	<i>One Identity Manager System Roles Administration Guide</i>

Detailed information about this topic

- [Prerequisites for indirect assignment of PAM groups to PAM user accounts](#) on page 88
- [Assigning PAM user groups to departments, cost centers, and locations](#) on page 89
- [Assigning PAM user groups to business roles](#) on page 91
- [Adding PAM user groups to system roles](#) on page 92
- [Adding PAM user groups to the IT Shop](#) on page 93
- [Adding local PAM user groups to the IT Shop automatically](#) on page 94
- [Assigning PAM user accounts directly to a PAM user group](#) on page 96
- [Assigning PAM user groups directly to a PAM user account](#) on page 96

Prerequisites for indirect assignment of PAM groups to PAM user accounts

In the case of indirect assignment, employees and PAM groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning PAM groups indirectly, check the following settings and modify them if necessary.

1. Assignment of employees and PAM user groups is permitted for role classes (departments, cost centers, locations, or business roles).

For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
 2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
 3. Save the changes.
2. Settings for assigning PAM user groups to PAM user accounts.
 - The PAM user account is labeled with the **Groups can be inherited** option.
 - The PAM user account is linked to an employee.
 - The PAM user account and the PAM user group belong to the same appliance.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- [Editing main data of PAM user accounts](#) on page 127
- [General main data of PAM user accounts](#) on page 127
- [Editing main data of PAM user groups](#) on page 138
- [General main data of PAM user accounts](#) on page 138

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. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

TIP: In the **Remove assignments** pane, you can remove assigned 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. In the Manager, select the **Organizations > Departments** category.
- OR -
In the Manager, select the **Organizations > Cost centers** category.
- OR -
In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign PAM user groups** task.
4. In the **Add assignments** pane, assign the groups.

TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

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

Related topics

- [Prerequisites for indirect assignment of PAM groups to PAM user accounts on page 88](#)
- [Assigning PAM user groups to business roles on page 91](#)
- [Adding PAM user groups to system roles on page 92](#)
- [Adding PAM user groups to the IT Shop on page 93](#)

- [Assigning PAM user accounts directly to a PAM user group on page 96](#)
- [Assigning PAM user groups directly to a PAM user account on page 96](#)
- [One Identity Manager users for managing Privileged Account Management on page 11](#)

Assigning PAM user groups to business roles

NOTE: This function is only available if the Business Roles Module is installed.

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

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

1. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

TIP: In the **Remove assignments** pane, you can remove assigned 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 the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign PAM user accounts task**.

In the **Add assignments** pane, assign the groups.

TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

4. Save the changes.

Related topics

- [Prerequisites for indirect assignment of PAM groups to PAM user accounts on page 88](#)
- [Assigning PAM user groups to departments, cost centers, and locations on page 89](#)

- [Adding PAM user groups to system roles](#) on page 92
- [Adding PAM user groups to the IT Shop](#) on page 93
- [Assigning PAM user accounts directly to a PAM user group](#) on page 96
- [Assigning PAM user groups directly to a PAM user account](#) on page 96
- [One Identity Manager users for managing Privileged Account Management](#) on page 11

Adding PAM user groups to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add a group to system roles.

If you assign a system role to employees, all PAM user accounts owned by 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 information, see the *One Identity Manager System Roles Administration Guide*.

To assign a group to system roles

1. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .

5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of PAM groups to PAM user accounts](#) on page 88
- [Assigning PAM user groups to departments, cost centers, and locations](#) on page 89
- [Assigning PAM user groups to business roles](#) on page 91
- [Adding PAM user groups to the IT Shop](#) on page 93
- [Assigning PAM user accounts directly to a PAM user group](#) on page 96
- [Assigning PAM user groups directly to a PAM user account](#) on page 96

Adding PAM user groups to the IT Shop

When you assign a user group to an 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 labeled with the **IT Shop** option.
- The user group must be assigned a service item.

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

- If you only want 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 group to the IT Shop.

1. In the Manager, select the **Privileged Account Management > User groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > PAM user groups** (role-based login) category.
2. In the result list, select the user group.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane the user group to the IT Shop shelves.
6. Save the changes.

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

1. In the Manager, select the **Privileged Account Management > User groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > PAM user groups** (role-based login) category.
2. In the result list, select the user group.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, the user group from the IT Shop shelves.
6. Save the changes.

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

1. In the Manager, select the **Privileged Account Management > User groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > PAM user groups** (role-based login) category.
2. In the result list, select the user group.
3. Select the **Remove from all shelves (IT Shop)** task.
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 with this user group are canceled.

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

Related topics

- [Prerequisites for indirect assignment of PAM groups to PAM user accounts](#) on page 88
- [Adding local PAM user groups to the IT Shop automatically](#) on page 94
- [General main data of PAM user accounts](#) on page 138
- [Assigning PAM user groups to departments, cost centers, and locations](#) on page 89
- [Assigning PAM user groups to business roles](#) on page 91
- [Adding PAM user groups to system roles](#) on page 92
- [Assigning PAM user accounts directly to a PAM user group](#) on page 96
- [Assigning PAM user groups directly to a PAM user account](#) on page 96
- [One Identity Manager users for managing Privileged Account Management](#) on page 11

Adding local PAM user groups to the IT Shop automatically

Using the following steps, you can add local PAM user groups to the IT Shop automatically. Synchronization ensures that the user groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor.

| NOTE: Directory group are not added to the IT Shop automatically.

To add local PAM user groups to the IT Shop automatically

1. In the Designer, set the **QER | ITShop | AutoPublish | PAGUsrGroup** configuration parameter.

From this time on, local PAM user groups are added to the IT Shop automatically.

2. In order not to add local PAM user groups to the IT Shop automatically, in the Designer, set the **QER | ITShop | PAGUsrGroupAutoPublish | PAGUsrGroup | ExcludeList** configuration parameter.

This configuration parameter contains a listing of all PAM user groups that should not be allocated to the IT Shop automatically.

You can extend this list if required. To do this, enter the name of the user groups in the configuration parameter using a pipe (|) delimited list.

3. Assign the employees that are allowed to make approval decisions about local user group request to the **Request & Fulfillment | IT Shop | Product owners | PAM user groups** application role. For more information, see the *One Identity Manager IT Shop Administration Guide*.

The **Approval of PAM user group membership requests** approval policy establishes product owners of the user groups as approvers. If no product owners are found, the requests are presented to the target system managers for approval.

The following steps are run to add a local PAM user group to the IT Shop automatically.

1. A service item is determined for the user group.

The service item is tested for each user groups and modify is required. The service item name corresponds to the name of the group.

- The service item is modified for groups with service items.
- Groups without service items are allocated new service items.

2. The service item is assigned to the **PAM user groups** service category by default.
3. The **Request & Fulfillment | IT Shop | Product owners | PAM user groups** application role is assigned to the service item as the product owner.
4. The user group is labeled with the **IT Shop** option and assigned to the **PAM** user groups IT Shop shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can request group memberships through the Web Portal.

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

Related topics

- [Adding PAM user groups to the IT Shop](#) on page 93
- [General main data of PAM user accounts](#) on page 138

Assigning PAM user accounts directly to a PAM user group

To react quickly to special requests, you can assign groups directly to user accounts. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign user accounts directly to a group

1. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

To remove an assignment

- Select the user account and double-click .
5. Save the changes.

Related topics

- [Assigning PAM user groups directly to a PAM user account](#) on page 96
- [Assigning PAM user groups to departments, cost centers, and locations](#) on page 89
- [Assigning PAM user groups to business roles](#) on page 91
- [Adding PAM user groups to system roles](#) on page 92
- [Adding PAM user groups to the IT Shop](#) on page 93

Assigning PAM user groups directly to a PAM user account

To react quickly to special requests, you can assign groups directly to user accounts. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign groups directly to user accounts

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

TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

5. Save the changes.

Related topics

- [Assigning PAM user accounts directly to a PAM user group](#) on page 96
- [Assigning PAM user groups to departments, cost centers, and locations](#) on page 89
- [Assigning PAM user groups to business roles](#) on page 91
- [Adding PAM user groups to system roles](#) on page 92
- [Adding PAM user groups to the IT Shop](#) on page 93

Effectiveness of membership in PAM user groups

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 at any time either directly, indirectly, or with an IT Shop request. 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` tables by the `XIsInEffect` column.

Example: 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 "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

Jo User1 has a user account in this appliance. They primarily belong to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to them 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 12: Specifying excluded groups (PAGUsrGroupExclusion table)

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

Table 13: Effective assignments

Employee	Member in role	Effective group
Pat Identity1	Marketing	Group A
Jan User3	Marketing, finance	Group B
Jo User1	Marketing, finance, control group	Group C
Chris User2	Marketing, control group	Group A, Group C

Only the group C assignment is in effect for Jo User1. It is published in the target system. If Jo User1 leaves the "control group" business role at a later date, group B also takes effect.

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

Table 14: Excluded groups and effective assignments

Employee	Member in role	Assigned group	Excluded group	Effective group
Chris User2	Marketing	Group A		Group C
	Control group	Group C	Group B Group A	

Prerequisites

- The **QER | Structures | Inherit | GroupExclusion** configuration parameter is set.

In the Designer, set the configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive groups belong to the same appliance.

To exclude a group

1. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.
- OR -
In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.
5. Save the changes.

PAM user group inheritance based on categories

In One Identity Manager, user accounts can selectively inherit user groups. To do this, user groups and 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 the

template. 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 target system-dependent groups. In the other tables, enter your categories for the user groups. Each table contains the category positions **position 1** to **position 63**.

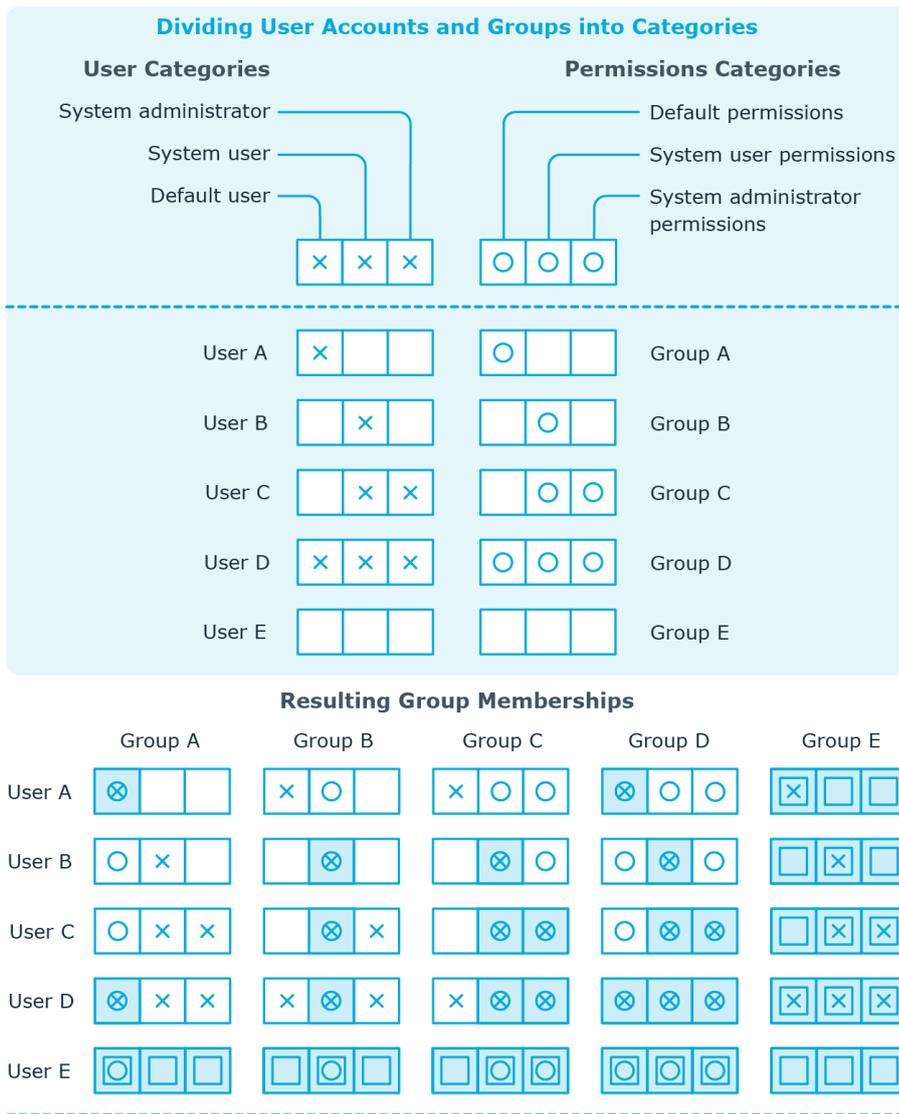
Every user account can be assigned to one or more categories. Each entitlement can also be assigned to one or more categories. If at least one of the category items between the user account and the assigned entitlement is the same, the entitlement is inherited by the user account. If the entitlement 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 through hierarchical roles. Categories are not taken into account when entitlements are directly assigned to user accounts.

Table 15: Category examples

Category position	Categories for user accounts	Categories for permissions
1	Default user	Default group or standard product
2	Administrator	Administrator group

Figure 1: Example of inheriting through categories.



Key:

<p>⊗ Inherits due to matching categories</p> <p>○ Inherits because user account and group are not categorized</p>	<p>○ Inherits because user account is not categorized</p> <p>⊗ Inherits because group is not categorized</p>
---	--

To use inheritance through categories

1. Define the categories on the appliance.
2. Assign categories to user accounts through their main data.
3. Assign categories to groups through their main data.

Related topics

- [Defining categories for the inheritance of PAM user groups](#) on page 121
- [General main data of PAM user accounts](#) on page 127
- [General main data of PAM user accounts](#) on page 138

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 employees who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Examples:

- 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 who violate 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 **Overview of all assignments** report.
- 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 employees 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 16: 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.

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 104
- [Initial password for new PAM user accounts](#) on page 116
- [Email notifications about login data](#) on page 116

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 policies 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 use or customize if required. You can also define your own password policies.

Detailed information about this topic

- [Predefined password policies](#) on page 105
- [Using password policies](#) on page 106
- [Editing password policies](#) on page 107
- [Creating password policies](#) on page 108
- [Custom scripts for password requirements](#) on page 112

- [Editing the excluded list for passwords](#) on page 115
- [Checking passwords](#) on page 115
- [Testing the generation of passwords](#) on page 115

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 defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time 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 more 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** 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** does not violate the target system-specific requirements for passwords.

For more 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** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

The **Privileged Account Management password policy** is predefined for PAM 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.

Using password policies

The **Privileged Account Management password policy** is predefined for PAM 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 user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's appliance.
4. The **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** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
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.
 - **Apply to:** Application scope of the password policy.

To specify an application scope

1. Click **→** next to the field.
2. Select one of the following references under **Table**:

- The table that contains the base objects of synchronization.
 - To apply the password policy based on the account definition, select the **TSBAccountDef** table.
 - To apply the password policy based on the manage level, select the **TSBBehavior** table.
3. Under **Apply to**, select the table that contains the base objects.
 - 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.
 4. Click **OK**.
 - **Password column**: Name of the password column.
 - **Password policy**: Name of the password policy to use.
 5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.

Detailed information about this topic

- [General main data for password policies](#) on page 108
- [Policy settings](#) on page 109
- [Character classes for passwords](#) on page 110
- [Custom scripts for password requirements](#) on page 112

Creating password policies

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

To create a password policy

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

Detailed information about this topic

- [General main data for password policies](#) on page 108
- [Policy settings](#) on page 109
- [Character classes for passwords](#) on page 110
- [Custom scripts for password requirements](#) on page 112

General main data for password policies

Enter the following main data of a password policy.

Table 17: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.
Description	Text field for additional explanation. Translate the given text using the  button.
Error Message	Custom error message generated if the policy is not fulfilled.

Property	Meaning
	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. This option cannot be changed. 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 18: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is 0 , no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is 256 .
Max. errors	<p>Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is 0, the number of failed logins is not taken into account.</p> <p>This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager.</p> <p>You can use the Password Reset Portal to reset the passwords</p>

Property	Meaning
	of employees and system users who have been blocked. For more information, see the <i>One Identity Manager Web Designer Web Portal User Guide</i> .
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is 0 , then the password does not expire.
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. If the value is 0 , then no passwords are stored in the password history.
Minimum 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 in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the Contains name properties for password check option is set. In the Designer, adjust this option in the column definition. For more information, see the <i>One Identity Manager Configuration Guide</i> .

Character classes for passwords

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

Table 19: Character classes for passwords

Property	Meaning
Required number of character classes	<p>Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for Min. number letters, Min. number lowercase, Min. number uppercase, Min. number digits, and Min. number special characters.</p> <p>That means:</p> <ul style="list-style-type: none"> • Value 0: All character class rules must be fulfilled. • Value >0: Minimum number of character class rules that must be

Property	Meaning
	fulfilled. At most, the value can be the number of rules with a value >0 .
	NOTE: Generated passwords are not tested for this.
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 characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not	Specifies whether a generated password can contain digits. This setting

Property	Meaning
generate digits	only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords 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

- [Checking passwords with a script](#) on page 112
- [Generating passwords with a script](#) on page 113

Checking passwords with a script

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

Syntax of 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 check

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

Example: Script that checks a password

A password cannot start with ? or ! . The password cannot start with three identical characters. 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. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change main data** task.
 - d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
 - e. Save the changes.

Related topics

- [Generating passwords with a script](#) on page 113

Generating passwords with a script

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 Entity property of the PasswordPolicy class.

Example: Script that generates a password

In random passwords, this script replaces the invalid characters **?** and **!** at the beginning of a password with **_**.

```
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. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change main data** task.
 - d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
 - e. Save the changes.

Related topics

- [Checking passwords with a script](#) on page 112

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. In the Designer, select the **Base data > Security settings > Password policies** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking passwords

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

To verify if a password conforms to the password policy

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
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. In the Manager, select the **Privileged Account Management > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.

3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.
This generates and displays a password.

Initial password for new PAM user accounts

You can issue an initial password for a new user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
 - In the Designer, set the **TargetSystem | PAG | Accounts | InitialRandomPassword** configuration parameter.
 - 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.

Related topics

- [Password policies for PAM users](#) on page 104
- [Email notifications about login data](#) on page 116

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 in a mail template is defined in several languages. This 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 more information, see the *One Identity Manager Installation Guide*.
- In the Designer, set 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 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 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 the Designer, set the **TargetSystem | PAG | Accounts | InitialRandomPassword** configuration parameter.
2. In the 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 the 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 the 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: To use custom mail templates for emails of this type, change the value of the configuration parameter.

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 One Identity Manager systems are mapped in Privileged Account Management. 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](#) on page 118
- [PAM user accounts](#) on page 123
- [PAM user groups](#) on page 137
- [PAM assets](#) on page 141
- [PAM asset groups](#) on page 142
- [PAM asset accounts](#) on page 142
- [PAM directory accounts](#) on page 143
- [PAM account groups](#) on page 144
- [PAM directories](#) on page 145
- [PAM entitlements](#) on page 146
- [PAM access request policies](#) on page 147
- [Reports about PAM objects](#) on page 147

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 to configure provisioning processes, automatic assignment of employees to user accounts, and to pass down PAM user groups to user accounts.

Detailed information about this topic

- [Creating PAM appliances on page 119](#)
- [Editing the main data of PAM appliances on page 119](#)
- [General main data of PAM appliances on page 120](#)
- [Defining categories for the inheritance of PAM user groups on page 121](#)
- [The PAM appliance overview](#)
- [Editing the synchronization project for a PAM appliance on page 122](#)
- [Editing search criteria for automatic employee assignment](#)
- [Synchronizing single objects on page 44](#)

Creating PAM appliances

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

To set up an appliance

1. In the Manager, select the **Privileged Account Management > Appliances** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the appliance.
4. Save the changes.

Related topics

- [Editing the main data of PAM appliances on page 119](#)
- [General main data of PAM appliances on page 120](#)
- [Defining categories for the inheritance of PAM user groups on page 121](#)

Editing the main data of PAM appliances

To edit the main data of an appliance:

1. In the Manager, select the **Privileged Account Management > Appliances** category.
2. Select the appliance in the result list.
3. Select the **Change main data** task.

4. Edit the main data of the appliance.
5. Save the changes.

Related topics

- [Creating PAM appliances](#) on page 119
- [General main data of PAM appliances](#) on page 120
- [Defining categories for the inheritance of PAM user groups](#) on page 121

General main data of PAM appliances

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

Table 20: General main data of 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)	<p>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.</p> <p>User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.</p>
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

Property	Description
	<p>system manager assigned to it.</p> <p>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.</p>

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.

If you create an appliance with the Synchronization Editor, it uses **One Identity Manager**.

Table 21: 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 70
- [Assigning employees automatically to PAM user accounts](#) on page 73
- [Target system managers for PAM systems](#) on page 160

Defining categories for the inheritance of PAM user groups

In One Identity Manager, user accounts can selectively inherit user groups. To do this, user groups and 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 the template. 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 target system-dependent groups. In the other tables, enter your categories for the user groups. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the appliance in the **Privileged Account Management > Appliances** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- [PAM user group inheritance based on categories](#) on page 99

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 in the 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. In the Manager, select the **Privileged Account Management > Appliances** category.
2. Select the appliance in the result list.
3. Select the **Change main data** task.
4. Select the **Edit synchronization project** task.

Related topics

- [Customizing the synchronization configuration for One Identity Safeguard](#) on page 31

Displaying the PAM appliance overview

Use this task to obtain an overview of the most important information about an appliance.

To obtain an overview of an appliance

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

PAM user accounts

You can use One Identity Manager to manage Privileged Account Management user accounts. 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.

Through 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 main data described in the following is mapped through templates from employee main 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 52
- [Managing assignments of PAM user groups](#) on page 87
- [Account definitions for PAM user accounts](#) on page 53
- [Creating local PAM user accounts](#) on page 124
- [Creating certificate-based PAM user accounts](#) on page 125
- [Creating PAM user accounts for directory users](#) on page 125
- [Editing main data of PAM user accounts](#) on page 127
- [General main data of PAM user accounts](#) on page 127
- [Contact information for PAM user accounts](#) on page 132
- [Secondary authentication for PAM user accounts](#) on page 133
- [Administrative entitlements for PAM user accounts](#) on page 133

- [Assigning extended properties to PAM user accounts](#) on page 134
- [Disabling PAM user accounts](#) on page 135
- [Deleting and restoring PAM user accounts](#) on page 136
- [Displaying the PAM user account overview](#) on page 137
- [Synchronizing single objects](#) on page 44

Creating local PAM user accounts

To create a local PAM user account

1. In the Manager, select the **Privileged Account Management > User accounts** category.
2. Click  in the result list.
3. On the **General** tab, enter the following data as a minimum:
 - **Appliance:** Appliance to which the user account belongs.
 - **Identity provider:** Select the **Local** value.
 - **User name:** Enter the name to display.
 - **Authentication provider:** Select how the user is authenticated in the Privileged Account Management system. Depending on the authentication provider, other data may be required.
 - **Local:** Enter the login name, password, and password confirmation.
 - **<External organization>:** Enter the email address or the name claim.
 - **<RADIUS server>:** Enter the login name of the RADIUS server.
 - **Time zone:** The user's time zone. The default time zone is **UTC** (Coordinated Universal Time).
4. Save the changes.

Related topics

- [General main data of PAM user accounts](#) on page 127
- [Contact information for PAM user accounts](#) on page 132
- [Secondary authentication for PAM user accounts](#) on page 133
- [Administrative entitlements for PAM user accounts](#) on page 133
- [Editing main data of PAM user accounts](#) on page 127
- [Creating certificate-based PAM user accounts](#) on page 125
- [Creating PAM user accounts for directory users](#) on page 125

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 the Manager, select the **Privileged Account Management > User accounts** category.
2. Click  in the result list.
3. On the **General** tab, enter the following data as a minimum:
 - **Appliance:** Appliance to which the user account belongs.
 - **Identity provider:** Select the **Local** value.
 - **User name:** Enter the name to display.
 - **Authentication provider:** Select **Certificate**.
 - **Certificate thumbprint (SHA-1):** Enter the unique hash value (40 hexadecimal characters) of the certificate.
NOTE: You can copy the thumbprint 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 main data of PAM user accounts](#) on page 127
- [Contact information for PAM user accounts](#) on page 132
- [Secondary authentication for PAM user accounts](#) on page 133
- [Administrative entitlements for PAM user accounts](#) on page 133
- [Editing main data of PAM user accounts](#) on page 127
- [Creating local PAM user accounts](#) on page 124
- [Creating PAM user accounts for directory users](#) on page 125

Creating PAM user accounts for directory users

Directory users are user accounts from an external target system, for example Active Directory or LDAP.

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 the Manager, select the **Privileged Account Management > User accounts** category.
2. Click  in the result list.
3. On the **General** tab, enter the following data as a minimum:
 - **Appliance:** Appliance to which the user account belongs.
 - **Identity provider:** Root domain of the respective directory server.
 - **Identity object:** Select the user account from the identity 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 an Active Directory user account, **ADSAccount** is selected. For an LDAP user account, **LDAPAccount** is selected.
 - **Identity object:** Select the user account.
 - b. Click **OK**.
4. Save the changes.

The domain, the user name, and the display name are determined from the user account.

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 or LDAP account definition as a required 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.

Related topics

- [General main data of PAM user accounts](#) on page 127
- [Contact information for PAM user accounts](#) on page 132
- [Secondary authentication for PAM user accounts](#) on page 133
- [Administrative entitlements for PAM user accounts](#) on page 133
- [Editing main data of PAM user accounts](#) on page 127
- [Creating local PAM user accounts](#) on page 124
- [Creating certificate-based PAM user accounts](#) on page 125
- [Account definitions for PAM user accounts](#) on page 53

Editing main data of PAM user accounts

To edit main data of a user account

1. In the Manager, select the **Privileged Account Management > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

Related topics

- [General main data of PAM user accounts](#) on page 127
- [Contact information for PAM user accounts](#) on page 132
- [Secondary authentication for PAM user accounts](#) on page 133
- [Administrative entitlements for PAM user accounts](#) on page 133
- [Disabling PAM user accounts](#) on page 135
- [Deleting and restoring PAM user accounts](#) on page 136

General main data of PAM user accounts

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

Table 22: Additional main data of a user account

Property	Description
Appliance	Appliance to which the user account belongs.
Employee	<p>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.</p> <p>You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee main data. Which login data is required depends on the selected identity type.</p> <p>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.</p>
No link to an employee required	<p>Specifies whether the user account is intentionally not assigned an employee. The option is automatically set if a user account is included in the exclusion list for automatic employee assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an employee (for example, if several employees use the user account).</p> <p>If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an employee can be filtered according to various criteria.</p>
Not linked to an employee	<p>Indicates why the No link to an employee required option is enabled for this user account. Possible values:</p> <ul style="list-style-type: none"> • By administrator: The option was set manually by the administrator. • By attestation: The user account was attested. • By exclusion criterion: The user account is not associated with an employee due to an exclusion criterion. For example, the user account is included in the exclude list for automatic employee assignment (configuration parameter PersonExcludeList).
Account definition	<p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account main data</p>

Property	Description
	<p>and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p>NOTE: The account definition cannot be changed once the user account has been saved.</p> <p>NOTE: Use the user account's Remove account definition task to reset the user account to Linked status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (XOrigin=1).</p>
Manage level	<p>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.</p>
Identity provider	<p>Source from which the user's personal information is taken from. Permitted values are:</p> <ul style="list-style-type: none"> • Local: Local PAM user account. You can enter contact data for this user account. • <Directory name>: External identity provider. Root domain of the respective directory server, for example, Active Directory or LDAP. Contact data are taken from the Active Directory or the LDAP user account. <p>This variant is only available if the Active Directory domain or the LDAP domain is imported into the One Identity Manager.</p>
Identity object	<p>User account in Active Directory or LDAP.</p>
Authentication provider	<p>Specifies how the user is authenticated in the Privileged Account Management system. Permitted values are:</p> <ul style="list-style-type: none"> • Certificate: (Only for local identity providers) Authentication is performed using a certificate. • Local: (Only for local identity providers) The user is authenticated by a user name and password. • <Directory name>: (Only for local identity providers) The identity object's domain. Authentication takes place through a user account of the relevant directory service, for example Active Directory user account or LDAP user account. <p>This variant is only available if the Active Directory domain or the LDAP domain is imported into the One Identity Manager.</p> <ul style="list-style-type: none"> • <External federation>: Name of an external organization. The

Property	Description
	<p>given email address or the name claim used for authentication.</p> <ul style="list-style-type: none"> • <RADIUS server>: Name of the RADIUS server. Authentication through the login name on the RADIUS server.
User name	User name of the PAM user account.
Login name	PAM user account login name.
Password	<p>Password for the user account. The employee's central password can be mapped to the user account password. For more information about an employee's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created.</p> <p>The password is deleted from the database after publishing to the target system.</p> <p>NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.</p>
Confirmation	Reconfirm password.
Password never expires	Specifies whether the password expires. This option is usually used for service accounts.
Change password at next login	Specifies whether the user must change their password the next time they log in.
Domain	User account's domain.
Require certificate authentication	Specifies whether the user can log in only with a domain-issued user certificate or SmartCard.
Certificate thumbprint (SHA-1)	Unique hash value (40 hexadecimal numbers) of the hash certificate.
Email address or name claim	Email address or name claim of the external organization's user account.
Display name	Display name of the PAM user account.
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	Maximum risk index value of all assigned groups. The property is only

Property	Description
(calculated)	visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
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: <ul style="list-style-type: none"> • 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 permissions, used by one employee. • Sponsored identity: User account to use for a specific purpose. Training, for example. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • Service identity: Service account.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. <ul style="list-style-type: none"> • 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.
System object	Identifies the user as a part of the system.
User account is disabled	Specifies whether the user account is disabled. If a user account is not required for a period of time, you can temporarily disable the user account by using the <User account is deactivated> option.
Account locked	Specifies whether the user account is locked. Depending on the configuration, the user account in the Privileged Account Management

Property	Description
	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 52
- [Account definitions for PAM user accounts](#) on page 53
- [Assigning employees automatically to PAM user accounts](#) on page 73
- [PAM user group inheritance based on categories](#) on page 99
- [Prerequisites for indirect assignment of PAM groups to PAM user accounts](#) on page 88
- [Disabling PAM user accounts](#) on page 135
- [Supported user account types](#) on page 80

Contact information for PAM user accounts

On the **Contact information** tab, enter the following main data. You can only enter contact data that uses a local identity provider.

Table 23: 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 out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Phone	Telephone number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Mobile phone	Mobile number. If you have assigned an account definition, the input field is automatically filled out with respect to 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	Text field for additional explanation.

Secondary authentication for PAM user accounts

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

Table 24: Secondary authentication of a user account

Property	Description
Secondary authentication	Second authentication provider for requesting multi-factor authentication by the user. All authentication providers that are allowed as secondary authentication providers (PAGAuthProvider table, AllowSecondaryAuth column).
Secondary authentication object	<p>(Only for directory users) Character string for identifying the second authentication object for multi-factor authentication. The input depends on the selected secondary authentication provider.</p> <p>If the secondary authentication of a user is performed using an Active Directory user account or an LDAP user account, you can select the user account.</p> <p>To select a user account</p> <ol style="list-style-type: none">To do this, click  next to the input field and enter the following information:<ul style="list-style-type: none">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.Secondary authentication object: Select a user account.Click OK.
Login name	Login name of the PAM user account for secondary authentication.

Administrative entitlements for PAM user accounts

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

Table 25: 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	Allows the user to create and approve passwords for non-administrative users.
Appliance	Allows the user to edit, update, and configure the appliance.
Operations	Allows the user to restart the appliance and to monitor the appliance.
Auditor	Allows the user read-only access.
Asset	Allows the user to add, edit, and delete partitions, assets, and accounts.
Directory	Allows the user to add, edit, and delete directories.
Security policy	Allows the user to add, edit, and delete entitlements and policies that control access to accounts and assets.
Personal password vault	Allows the user to add, edit, delete, share, and access a vault for personal passwords.

Related topics

- [Administrative entitlements for PAM user groups](#) on page 139

Assigning extended properties to PAM user accounts

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

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

To specify extended properties for a user account

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

TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

Disabling PAM user accounts

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

Scenario: User accounts are linked to employees and are 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 **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 when 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 the Manager, select the **Privileged Account Management > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Scenario: The user accounts are not linked to employees.

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

1. In the Manager, select the **Privileged Account Management > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

For more information about deactivating 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 53
- [Creating manage levels](#) on page 58
- [Deleting and restoring PAM user accounts](#) on page 136

Deleting and restoring PAM user accounts

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 account definition assignment is removed, the user account that was created from this account definition, is deleted.

You can delete a user account that was not created using an account definition through the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

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

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

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

To restore a user account

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

Related topics

- [Disabling PAM user accounts](#) on page 135
- [Specifying deferred deletion for PAM user accounts](#) on page 86

Displaying the PAM user account overview

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 the Manager, select the **Privileged Account Management > User accounts** category.
2. Select the user account in the result list.
3. Select the **PAM user account overview** task.

PAM user groups

Through 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 main data of PAM user groups](#) on page 138
- [General main data of PAM user accounts](#) on page 138
- [Administrative entitlements for PAM user groups](#) on page 139
- [Assigning extended properties to PAM user groups](#) on page 140

- [Displaying the PAM user group overview](#) on page 141
- [Managing assignments of PAM user groups](#) on page 87
- [Synchronizing single objects](#) on page 44

Editing main data of PAM user groups

To edit group main data

1. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Related topics

- [General main data of PAM user accounts](#) on page 138
- [Administrative entitlements for PAM user groups](#) on page 139

General main data of PAM user accounts

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

Table 26: General main data of 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 not permitted.

Property	Description
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range 0 to 1 . This input field is only visible if the QER CalculateRiskIndex configuration parameter is activated. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
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	Text field for additional explanation.
Authentication provider	Directory name (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

- [PAM user group inheritance based on categories on page 99](#)
- [Prerequisites for indirect assignment of PAM groups to PAM user accounts on page 88](#)
- [Adding PAM user groups to the IT Shop on page 93](#)
- [Adding local PAM user groups to the IT Shop automatically on page 94](#)

Administrative entitlements for PAM user groups

If necessary, on the **Permissions** tab, select the user group's administrative permissions. The permissions apply to users in the user group.

Administrative permissions for PAM user groups are supported as from One Identity Safeguard 7.0. For more information about administrative entitlements in One Identity Safeguard, see the *One Identity Safeguard Administration Guide*.

Table 27: Administrative permissions for a user group

Administrative role	Description
Authorizer	Allows group users to share permissions with other users.
Users	Allows group users to create new users, and to unlock and reset passwords of non-administrative users.
Help Desk	Allows group users to unlock and reset passwords of non-administrative users.
Appliance	Allows group users to edit, update, and configure the appliance.
Operations	Allows group users to restart and monitor the appliance.
Auditor	Allows group users read-only access.
Asset	Allows group users to add, edit, and delete partitions, assets, and accounts.
Directory	Allows group users to add, edit, and delete directories.
Security policy	Allows group users to add, edit, and delete permissions and policies that control access to accounts and assets.
Personal password vault	Allows group users to add, edit, delete, share, and access a vault for personal passwords.

Related topics

- [Administrative entitlements for PAM user accounts](#) on page 133

Assigning extended properties to PAM user groups

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

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

To specify extended properties for a group

1. In the Manager, select the **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

Displaying the PAM user group overview

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 **Privileged Account Management > User groups** category.
2. Select the group in the result list.
3. Select the **PAM user group overview** task.

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 by single object synchronization.

To display the properties of an asset

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Assets** category.
2. Select the asset in the result list.
3. Select the **Change main data** task.

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 the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Assets** category.
2. Select the asset in the result list.
3. Select the **PAM asset overview** task.

Related topics

- [Synchronizing single objects](#) on page 44
- [PAM object owners](#) on page 153

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 by single object synchronization.

To display the properties of an asset group

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Asset groups** category.
2. Select the asset group in the result list.
3. Select the **Change main data** task.

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 the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Asset groups** category.
2. Select the asset group in the result list.
3. Select the **PAM asset group overview** task.

Related topics

- [Synchronizing single objects](#) on page 44
- [PAM object owners](#) on page 153

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 by single object synchronization.

To view an overview of an asset account:

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

To display the properties of an asset account:

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Asset accounts** category.
2. Select the asset account in the result list.
3. Select the **Change main data** task.

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

To define a risk index for an asset account

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Asset accounts** category.
2. Select the asset account in the result list.
3. Select the **Change main data** task.
4. Set a value for the **Risk index** between **0** and **1**.

This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.

5. Save the changes.

Related topics

- [Synchronizing single objects](#) on page 44
- [PAM object owners](#) on page 153

PAM directory accounts

Directory accounts are privileged user accounts in a directory, such as Active Directory or LDAP, for which you can request a password.

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 by single object synchronization.

To view an overview of a directory account:

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

To display the properties of a directory account

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Directory accounts** category.
2. Select the directory account in the result list.
3. Select the **Change main data** task.

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 define a risk index for a directory account

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Privileged Objects > Directory accounts** category.
2. Select the directory account in the result list.
3. Select the **Change main data** task.
4. Set a value for the **Risk index** between **0** and **1**.

This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.

5. Save the changes.

Related topics

- [Synchronizing single objects](#) on page 44
- [PAM object owners](#) on page 153

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 by single object synchronization.

To display the properties of an account group

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

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

Related topics

- [Synchronizing single objects](#) on page 44
- [PAM object owners](#) on page 153

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 by single object synchronization.

To display the properties of a directory

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Directories** category.
2. Select the directory in the result list.
3. Select the **Change main data** task.

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 the Manager, select the **Privileged Account Management > Appliances > <appliance> > Directories** category.
2. Select the directory in the result list.
3. Select the **PAM directory overview** task.

Related topics

- [Synchronizing single objects](#) on page 44

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 by single object synchronization.

To display the properties of an entitlement

1. In the Manager, select the **Privileged Account Management > Appliances > <appliance> > Entitlements** category.
2. Select the entitlement in the result list.
3. Select the **Change main data** task.

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 the Manager, select the **Privileged Account Management > Appliances > <appliance> > Entitlements** category.
2. Select the entitlement in the result list.
3. Select the **PAM entitlement overview** task.

Related topics

- [Synchronizing single objects](#) on page 44

PAM access request policies

An access request policy defines:

- The scope (meaning, which assets, asset groups, asset accounts, directory accounts, or account groups).
- The access type (password, SSH, SSH key, remote desktop, remote desktop application, Telnet)
- 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 by single object synchronization.

To display the properties of an access request policy

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

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

Related topics

- [Synchronizing single objects](#) on page 44
- [Configuring PAM access request policies](#) on page 156

Reports about PAM objects

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 28: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	User group	This report finds all roles containing employees who have the selected system entitlement.
Show overview	User group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	User group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	User group	This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Show entitlement drifts	Appliance	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Appliance	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average number of system entitlements	Appliance	This report contains all user accounts with an above average number of system entitlements.

Report	Published for	Description
Show employees with multiple user accounts	Appliance	This report shows all the employees that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Appliance	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Appliance	This report finds all roles containing employees with at least one user account in the selected target system.
Show unused user accounts	Appliance	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Appliance	This report shows all user accounts to which no employee is assigned.

Table 29: Additional reports for the target system

Report	Description
PAM user account and group administration	This report contains a summary of user account and group distribution in all PAM appliances. You can find the report in the My One Identity Manager > Target system overviews category.
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 My One Identity Manager > Data quality analysis category.
Overview of employee's privileged access.	The report contains detailed information about personal and organizational data as well as the employee's current privileged access. The report is displayed for employees.

PAM access requests

In One Identity Manager, you can request access requests for assets, asset accounts, directory accounts, asset groups, and account groups in 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 key request:** To requests SSH keys 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.
- **Telnet session request:** To request Telnet sessions for assets in a PAM system.

The access requests are requested in the 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 information about configuring the IT Shop, see the *One Identity Manager IT Shop Administration Guide*. For more information about requesting access requests in Web Portal, please refer to the *One Identity Manager Web Designer Web Portal User Guide*.

Detailed information about this topic

- [System requirements for requesting PAM access requests](#) on page 150
- [Requesting PAM access requests](#) on page 151
- [PAM object owners](#) on page 153
- [Configuring PAM access request policies](#) on page 156

System requirements for requesting PAM access requests

The access requests 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 generate valid access requests whenever possible, do not set time restrictions on the entitlements and access request policies.

For more 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 17
- [Setting up the One Identity Safeguard synchronization server](#) on page 18

Requesting PAM access requests

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

Table 30: Default objects for requesting access requests

Products	<p>Password release request: To request passwords for accounts in a PAM system.</p> <p>SSH key request: To requests SSH keys for accounts in a PAM system.</p> <p>SSH session request: To request SSH sessions for assets in a PAM system.</p> <p>Remote Desktop session request: To request remote desktop sessions for assets in a PAM system.</p>
----------	--

Telnet session request: To request Telnet sessions for assets in a PAM system.

Service category:	Privileged access requests
Shelf	Identity & Access Lifecycle Privileged access
Approval procedures:	PG - owners of the requested privileged access request
Approval policies/approval workflows	Approval of privileged access requests

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. This allows you to request access requests for assets, asset accounts, directory accounts, asset groups, and account groups that are within the request access policy's scope.
- An application role under **Privileged Account Governance | Assets and account owners** is assigned to the requestable assets, asset accounts, directory accounts, asset groups, and account groups as the owner.
- Employees are assigned to the application roles.
- The **Read status of privileged access requests** schedule is enabled. Adjust the schedule in the 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 PAM System from the Web Portal and retrieve the password or start a session.

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

Related topics

- [PAM object owners](#) on page 153
- [Configuring PAM access request policies](#) on page 156
- [PAM entitlements](#) on page 146
- [General main data of PAM appliances](#) on page 120
- [Known issues about connecting One Identity Safeguard appliances](#) on page 175

PAM object owners

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

Users with this application role:

- Make decisions about requesting access requests for privileged objects.
- Attest the possible user access to these privileged objects.

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

For more information about approval processes, see the *One Identity Manager IT Shop Administration Guide* and the *One Identity Manager Attestation Administration Guide*.

Detailed information about this topic

- [Automatically determining the owners](#) on page 153
- [Manually specifying employees as PAM object owners](#) on page 154
- [Manually specifying application roles for PAM object owners](#) on page 155

Automatically determining the owners

Initially, approvers of access request policies automatically become owners of PAM assets, PAM asset accounts, PAM directory accounts, PAM asset groups and PAM account groups. This assignment only takes place if an access request policy can be determined for a PAM object.

- For each access request policy, a new application role is created for the owner under the **Privileged Account Governance | Asset and account owners** application

role.

- The role approvers of an access request policy are added to the application role.
- The application is assigned to the PAM asserts, PAM asset accounts, PAM directory accounts, PAM asset groups, and PAM account groups within the policy's scope.
- If there are several access policies defined for a PAM object, the valid application roles are determined through the access request policy's entitlements. The PAM object owners are determined by the following order:
 1. Application roles of access request policies with low priority entitlements
 2. Application roles of access request policies with the lowest priority

NOTE:

- An application role for owners is only assigned automatically to a PAM object if an application role is not already assigned to the PAM object. Any existing assignment is not changed.
- Owner are only determined initially. Changes to the role approver of an access request policy are not automatically added to the associated application role. Change the employee assigned to the application manually, if required.
- Owners cannot be determined for access request policies that are automatically approved in One Identity Safeguard. In this case, assign employees manually to the application role.

Related topics

- [Manually specifying employees as PAM object owners](#) on page 154
- [Manually specifying application roles for PAM object owners](#) on page 155

Manually specifying employees as PAM object owners

In addition to automatically determining the owners, you can specify the owners manually.

To manually specify employees as owners

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

TIP: In the **Remove assignments** pane, you can remove assigned employees.

To remove an assignment

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

Related topics

- [Automatically determining the owners](#) on page 153
- [Manually specifying application roles for PAM object owners](#) on page 155

Manually specifying application roles for PAM object owners

Application roles are created when owner are determined automatically. You can specify further application roles manually.

To specify an application role for a PAM object owner

1. In the Manager, select one of the following filters in the **Privileged Account Management > Appliances > <appliance> > Privileged objects** category.
 - To specify an application role for an asset, select **Assets**.
 - To specify an application role for an asset group. select **Asset group**.
 - To specify an application role for an asset account, select **Asset account**.
 - To specify an application role for a directory account, select **Directory account**.
 - To specify an application role for an account group, select **Account group**.
2. In the result list, select the PAM object.
3. Select the **Change main data** task.
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.
5. Assign employees, who are owners, to the application role.

Related topics

- [Manually specifying employees as PAM object owners](#) on page 154
- [Automatically determining the owners](#) on page 153
- [PAM object owners](#) on page 153

Configuring PAM access request policies

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

To configure the access request policy

1. In the Manager, select the **Privileged Account Management > Appliances > <Appliance> > Entitlements > <Entitlement>** category.
2. Select the access request policy in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, check the **One Identity Manager enabled** option.
 - If this option is set, access requests can be requested for assets, asset accounts, directory accounts, asset groups, and account groups that are within the access request policy's scope.
 - If this option is not set, is not possible to request access requests for assets, asset accounts, directory accounts, asset groups, and account groups that are within the access request policy's scope.

Related topics

- [PAM access request policies](#) on page 147
- [Requesting PAM access requests](#) on page 151

Handling of PAM objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and employees

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

- Managing 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 the Web Portal. The request undergoes a defined approval process. The group is not assigned until it has been approved by an authorized person.

In the 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

Through the **Identity & Access Lifecycle > Privileged access** IT Shop shelf, you can request password and session requests for the privileged objects of a PAM system. The request undergoes a defined approval process. 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 the Manager. The attestors 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 the 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 the Manager. Supervisors use the Web Portal to check policy violations 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. 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 52, [Assigning PAM user groups to PAM user accounts in One Identity Manager](#) on page 87, [PAM access requests](#) on page 150 and refer to the following guides:

- *One Identity Manager Web Designer 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*

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. 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 53.

- 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 policies 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 use or customize if required. You can also define your own password policies.

For more information, see [Password policies for PAM users](#) on page 104.

- Target system types

Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

For more information, see [Post-processing outstanding objects](#) on page 46.

- Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all appliances in One Identity Manager.

Define additional application roles if you want to limit the 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 160.

- Servers

In order to handle target system specific processes in One Identity Manager, the synchronization server and its server functionality must be declared.

For more information, see [Job server for PAM-specific process handling](#) on page 162.

- 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 [PAM object owners](#) on page 153.

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 have permission to edit all appliances in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual appliances. The application roles must be added under the default application role.

For more 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 allocates employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.

Target system managers with the default application role are authorized to edit all the 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 31: Default application roles for target system managers

User	Tasks
Target system managers	<p>Target system managers must be assigned to the Target systems Privileged account management application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects.• Edit password policies for the target system.• Prepare groups to add to the IT Shop.• Can add employees who have another identity than the Primary identity.• Configure synchronization in the Synchronization Editor and define 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.

To initially specify employees to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)
2. Select the **One Identity Manager Administration > Target systems > Administrators** category.
3. Select the **Assign employees** task.
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 in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > Privileged Account Management** category.
3. Select the **Assign employees** task.
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. Log in to the Manager as a target system manager.
2. Select the application role in the **Privileged Account Management > Basic configuration data > Target system managers** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To specify target system managers for individual Privileged Account Management systems

1. Log in to the Manager as a target system manager.
2. Select the **Privileged Account Management > Appliances** category.
3. Select the appliance in the result list.
4. Select the **Change main data** task.
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 Privileged Account Management](#) on page 11
- [General main data of PAM appliances](#) on page 120

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 functionality must be declared. You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **Privileged Account Management > Basic configuration data > Server** category and edit the Job server's main 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 19
- [Editing PAM Job servers](#) on page 163

Editing PAM Job servers

To edit a Job server and its functions

1. In the Manager, select the **Privileged Account Management > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.
4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- [General main data of Job servers](#) on page 163
- [Specifying server functions](#) on page 166
- [Installing One Identity Manager Service with a One Identity Safeguard connector](#) on page 20

General main data of Job servers

NOTE: All editing options are also available in the Designer under **Base Data > Installation > Job server**.

NOTE: More properties may be available depending on which modules are installed.

Table 32: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: <Name of server>.<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.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The Server is cluster and Server belongs to cluster properties 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 implementing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the

Property	Meaning
	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. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
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 QBM_PJobQueueLoad procedure 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 Job Queue Info program. For more information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> .
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i> .
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 running.

Property	Meaning
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- [Specifying server functions](#) on page 166

Specifying server functions

NOTE: All editing options are also available in the 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 with respect to the server function.

NOTE: More server functions may be available depending on which modules are installed.

Table 33: Permitted server functions

Server function	Remark
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on. 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	This 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	Server on which reports are generated.

Server function	Remark
report server	
One Identity Safeguard connector	Server on which the One Identity Safeguard connector is installed. This server synchronizes the One Identity Safeguard target system.

Related topics

- [General main data of Job servers](#) on page 163

Configuration parameters for managing a Privileged Account Management system

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 34: Configuration parameters for synchronizing a Privileged Account Management system

Configuration parameters	Meaning if Set
TargetSystem PAG	<p>Preprocessor relevant configuration parameters for controlling model components for Privileged Account Management system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p>
TargetSystem PAG Accounts	Allows configuration of PAM user account data.
TargetSystem PAG Accounts InitialRandomPassword	Specifies whether a random password is generated 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	Employee to receive an email with the random generated password (manager cost center/department/location/business 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

Configuration parameters	Meaning if Set
	parameter.
TargetSystem PAG Accounts InitialRandomPassword SendTo MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The Employee - new user account created mail template is used.
TargetSystem PAG Accounts InitialRandomPassword SendTo MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The Employee - initial password for new user account mail template is used.
TargetSystem PAG Accounts MailTemplateDefaultValues	Mail template used to send notifications about whether 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	Allows configuration of privileged user account settings.
TargetSystem PAG Accounts TransferJPegPhoto	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	Default email address of the recipient for notifications about actions in the target system.
TargetSystem PAG PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem PAG PersonAutoDisabledAccounts	Specifies whether employees are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem PAG PersonAutoFullsync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem PAG PersonExcludeList	Listing of all user account without automatic employee assignment. Names are listed in a pipe () delimited list that is handled as a regular search pattern. Example: ADMINISTRATOR GUEST KRBTGT TSINTERNETUSER IUSR_.* IWAM_.*

Configuration parameters	Meaning if Set
	SUPPORT_.* . * \$
TargetSystem PAG UserObjectAccessThreshold	Threshold for the number of privileged access permissions per user, above which a user's risk index is increased. Default is 20 .
TargetSystem PAG HighRiskIndexThreshold	Risk index values higher than this threshold are considered high . Default is 0.5 .
QER ITShop AutoPublish PAGUsrGroup	<p>Preprocessor relevant configuration parameter for automatically adding PAM user groups to the IT Shop. If the parameter is set, all user groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p>
QER ITShop AutoPublish PAGUsrGroup ExcludeList	<p>List of all PAM user groups that are not to be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.</p> <p>Example: .*Administrator.* . *Admins . *Operators</p>

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 project template uses mappings for the following schema types.

Table 35: 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
AuthenticationProvider	PAGAuthProvider
User	PAGUser
UserGroup	PAGUsrGroup
Entitlement	PAGEntl
AccessRequestPolicy	PAGReqPolicy
AccountGroup	PAGAccGroup
Asset	PAGAsset
AssetAccount	PAGAstAccount
AssetGroup	PAGAstGroup
Directory	PAGDirectory
DirectoryAccount	PAGDirAccount

Editing One Identity Safeguard system objects

The following table describes permitted editing methods for One Identity Safeguard schema types and the necessary restrictions for processing the system objects.

Table 36: 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
Authentication provider (AuthenticationProvider)	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

One Identity Safeguard connector settings

The following settings are configured for the system connection with the One Identity Safeguard connector.

Table 37: One Identity Safeguard connector settings

Setting	Description
Appliance display name	Display name of the appliance. Variable: CP_ApplianceDisplay
System identifier	Unique identifier for identifying the appliance. Variable: CP_ApplianceID ⚠ CAUTION: The system identifier must describe the appliance uniquely. Appliances are differentiated on the basis of the system identifier. If you use an identifier more than once for different appliances, it can cause errors and loss of data.
Always connect to the primary cluster node	This option is automatically set if a One Identity Safeguard cluster is detected when the connection is tested. If you use a cluster of multiple One Identity Safeguard appliances, this option should be enabled. Variable: CP_ConnectPrimaryNode
Appliance host name or IP	Host name or IP address of the appliance. If you use a cluster of multiple One Identity Safeguard appliances, enter the primary appliance here. Variable: CP_ApplianceHost
Trusted certificate thumbprint	Thumbprint of the trusted certificate that is used by the synchronization user and the user account of the One Identity Manager Service. Variable: CP_CertificateThumbprint
Ignore SSL connection	You should only activate this option for test purposes, because this may lead to potential trusting of insecure connections.

Setting	Description
errors	Variable: CP_IgnoreSSLErrors Default: False
Cluster IPv4 addresses	Semicolon delimited list of IPv4 addresses of an environment consisting of several appliances (clusters). Variable: CP_ClusterIPv4Addresses
Cluster IPv6 addresses	Semicolon delimited list of IPv6 addresses of an environment consisting of several appliances (clusters). Variable: CP_ClusterIPv6Addresses
Customize connector definition	You can use this setting to adjust the definition used by the 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.

Known issues about connecting One Identity Safeguard appliances

Issue

The following error message is displayed while setting up a synchronization project for One Identity Safeguard:

```
404: Not Found -- 0:
```

Cause

An older version of One Identity Safeguard is in use that is not supported by One Identity Manager.

Solution

Ensure you are using One Identity Safeguard version 6.0 or later. For more information, see [Synchronizing a Privileged Account Management system](#) on page 15.

Issue

The following error occurs in One Identity Safeguard if you request access to an asset from the access request policy section and it is configured for asset-based session access of type **User Supplied**:

```
400: Bad Request -- 60639: A valid account must be identified in the request.
```

The request is denied in One Identity Manager and the error in the request is displayed as the reason.

Solution

The problem is resolved with One Identity Safeguard version 2.6.

Issue

The One Identity Safeguard connector connection to a One Identity Safeguard appliance quits with following errors:

The version <Appliance version> of the connected One Identity Safeguard appliance is not supported by this version of the One Identity Manager Safeguard connector. Error-free operation cannot be guaranteed. The connection is terminated.

The version <safeguard-ps version> of the PowerShell module 'safeguard-ps' does not match the version <Appliance version> of the One Identity Safeguard appliance. The connection is terminated

Cause

The implemented version of this One Identity Safeguard Appliance does not match the version of the safeguard-ps Windows PowerShell module in use.

Solution

Ensure that you use the matching version. Ensure that the major and the minor version of the Windows PowerShell module match the major and the minor version of your One Identity Safeguard appliance.

For more information, see [Installing the safeguard-ps Windows PowerShell module](#) on page 19.

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

Contacting us

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

Technical support resources

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

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

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

A

- account definition 53
 - add to IT Shop 68
 - assign automatically 66
 - assign to all employees 66
 - assign to appliance 70
 - assign to business role 66
 - assign to cost center 65
 - assign to department 65
 - assign to employee 64, 67
 - assign to location 65
 - assign to system roles 67
 - assign to user account 78
 - create 54
 - delete 70
 - edit 54
 - IT operating data 60, 62
 - manage level 57-58
- application role
 - asset and account owners 11, 153
 - Privileged Account Governance 11, 153
- application roles for Privileged Account Management 11

B

- base object 34, 39

C

- calculation schedule 42
 - deactivate 44

- category 121
- configuration parameter 13, 168
- convert connection parameter 34

D

- default user accounts 81
- direction of synchronization
 - direction target system 26, 32
 - in the Manager 26
- directory 145

E

- email notification 116
- employee
 - assign PAM user account 79
- employee assignment
 - manual 76
 - remove 76
 - search criteria 75
- exclusion definition 97
- extended property
 - PAM user account 134
 - PAM user group 140

I

- identity
 - group identity 80, 83
 - organizational identity 80
 - personalized admin identity 80, 82

- primary identity 80
- service identity 80
- sponsored identity 80
- inheritance
 - category 99
- IT operating data
 - change 63
 - log 62
- IT Shop shelf
 - assign account definition 68

J

- Job server 162
 - edit 20, 163
 - load balancing 40
 - properties 163

L

- load balancing 40
- log file 49
- login data 116

M

- membership
 - modify provisioning 38

N

- NLog 49

O

- object
 - delete immediately 46
 - outstanding 46

- publish 46
- offline mode 50
- outstanding object 46

P

- PAM access request policy 147
 - configure 156
- PAM access requests 150
 - approval policies 151
 - approval workflow 151
 - password request 151
 - remote desktop session requests 151
 - request 151
 - service category 151
 - shelf 151
 - SSH key request 151
 - SSH session request 151
 - system requirements 150
 - telnet session requirement 151
- PAM account group 144
 - owner 153, 155
- PAM appliance
 - account definition (initial) 70, 120
 - category 99, 119
 - create 119
 - employee assignment 75
 - overview 122
 - report 147
 - specify category 121
 - target system managers 120, 160
- PAM asset 141
 - owner 153, 155
- PAM asset account 142
 - owner 153, 155
 - risk index 142

- PAM asset group 142
 - owner 153, 155
- PAM authentication provider
 - certificate 125
 - directory 125
 - local 124
- PAM directory account 143
 - owner 153, 155
- PAM entitlement 146
- PAM owners 153, 155
- PAM user account 123
 - assign employee 73
 - assign extended properties 134
 - assign user groups 96
 - assigned employee 127
 - certificate based 125
 - create 124-125
 - data quality 147
 - deferred deletion 86, 136
 - delete 136
 - directory user 125
 - edit 127
 - local 124
 - lock 135-136
 - overview 137
 - PAM appliance 127
 - password 116
 - notification 116
 - restore 136
 - risk index 127
- PAM user group 137
 - about IT Shop requests 138
 - add to IT Shop 93
 - add to IT Shop (automatic) 94
 - add to system role 92
 - assign category 138
 - assign extended properties 140
 - assign to business role 91
 - assign to cost center 89
 - assign to department 89
 - assign to location 89
 - assign user account 87, 96
 - category 99
 - edit 138
 - effective 97
 - exclusion 97
 - inheriting through categories 121
 - inheriting through roles 87
 - overview 141
 - overview of all assignments 102
 - product owners 94
 - risk index 138
 - service item 94
 - shelf 94
- password
 - initial 116
- password policy 104
 - assign 106
 - character sets 110
 - check password 115
 - conversion script 112-113
 - default policy 106, 108
 - display name 108
 - edit 107-108
 - error message 108
 - excluded list 115
 - failed logins 109
 - generate password 115
 - initial password 109
 - name components 109

- password age 109
 - password cycle 109
 - password length 109
 - password strength 109
 - predefined 105
 - test script 112
 - Privileged Account Management
 - owner 11
 - target system manager 11
 - project template 171
 - provisioning
 - accelerate 40
 - members list 38
- R**
- reset revision 49
 - reset start up data 49
 - revision filter 38
 - risk assessment
 - PAM user account 127
 - PAM user group 138
- S**
- schema
 - changes 36
 - shrink 36
 - update 36
 - server 162
 - server function 166
 - single object synchronization 39, 44
 - accelerate 40
 - start up configuration 34
 - synchronization
 - accelerate 38
 - authorizations 17
 - base object
 - create 33
 - calculation schedule 42
 - configure 26, 31
 - connection parameter 26, 31, 33
 - different appliances 33
 - extended schema 33
 - prerequisite 15
 - prevent 44
 - scope 31
 - simulate 49
 - start 26, 42
 - synchronization project
 - create 26
 - target system schema 33
 - user 17
 - variable 31
 - variable set 33
 - workflow 26, 32
 - synchronization analysis report 49
 - synchronization configuration
 - customize 31-33
 - synchronization log 43, 49
 - contents 30
 - create 30
 - synchronization project
 - create 26
 - deactivate 44
 - edit 122
 - project template 171
 - synchronization server 18, 162
 - configure 19
 - edit 163
 - install 20

- Job server 20
 - server function 166
 - system requirements 19
- synchronization workflow
 - create 26, 32
- synchronize single object 44
- system connection
 - change 33
 - enabled variable set 35

T

- target system
 - not available 50
- target system synchronization 46
- template
 - IT operating data, modify 63

U

- user account
 - administrative user account 82-83
 - apply template 63
 - category 99
 - connected 78
 - default user accounts 81
 - group identity 83
 - identity 80
 - manage level 78
 - personalized admin identity 82
 - privileged user account 80, 84
 - type 80-84

V

- variable set 34
 - active 35