



One Identity Manager 9.1.3

Target System Base Module Administration Guide

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 Target System Base Module Administration Guide
Updated - 29 April 2024, 14:21

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

Contents

Basic mechanisms for employee and user account administration	5
Employee and user account administration	5
Handling employees and user accounts	7
Using account definitions to create user accounts	10
Account definitions and manage levels	10
Assigning account definitions to employees	12
Determining valid IT operating data for the target systems	12
IT operating data for the One Identity Manager default configuration	14
Employee's central user account	16
Employee's default email address	17
Changing employee main data	17
Templates and processes for implementing account definitions	18
Examples for implementing several account definitions within a target system type	19
Assigning employees automatically to user accounts	21
Configuring automatic employee assignment	22
Editing search criteria for automatic employee assignment	24
Define search criteria for employee assignment	25
Finding employees and directly assigning them to user accounts	27
Modifying scripts for automatic employee assignment	29
Deactivating and deleting employees and user accounts	31
Temporarily deactivating employees	32
Permanently deactivating employees	33
Deferred deletion of employees	34
Disabling and deleting using account definitions	36
Handling group memberships	38
The Unified Namespace	41
Mapping target system objects in Unified Namespace	41
Special features for mapping object properties	47
One Identity Manager users for managing target systems in Unified Namespace	47
Displaying Unified Namespace objects	49
Reports about a target system in the Unified Namespace	49

Reports about all target systems in the Unified Namespace	51
About us	53
Contacting us	53
Technical support resources	53
Index	54

Basic mechanisms for employee and user account administration

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 method for linking employees and their user accounts.

- Employees can automatically obtain their user accounts through One Identity Manager account definitions.
- When user accounts are inserted in One Identity Manager, they can be automatically assigned to an existing employee or a new employee can be created if necessary.
- Employee and user account data in One Identity Manager can be manually entered and assigned to each other.

Employee and user account administration

The requirements of a company's user administration are often different not only in the existing target system types, but also in the individual target systems of a target system type.

Requirements for user account administration might be, for example:

Target system type Active Directory with Microsoft Exchange

- In domain A, a user account should be automatically created for each internal employee. The information for the container and home server are based on the department and the location of the person. Each user account in the domain is automatically allocated a Microsoft Exchange mailbox.
- In domain B, the user accounts are administrated independently of the employee data. Microsoft Exchange mailboxes can only be allocated by requesting them in the IT shop.

Target system type HCL Domino

- All members of the sales department are automatically allocated an HCL Domino mailbox. Members of other departments can request an HCL Domino mailbox. The attributes of the HCL Domino mailbox are determined depending on the member's department.

Target system type SAP R/3

- All members of the personnel department are automatically allocated a user account in an SAP Client 101.
- The members of the purchasing department are automatically allocated a user account in the SAP Client 102 the moment they are assigned the appropriate role.
- The user accounts for the SAP Client 103 are allocated exclusively through a request process.

One Identity Manager uses different mechanisms to assign user accounts to employees.

Initial assignment of user accounts

The user accounts are initially read into One Identity Manager from a target system through synchronization. In doing so, the existing employees can automatically be assigned to the user accounts. New employees can be created and assigned to user accounts if necessary. The criteria for these automatic assignments are defined on a company-specific basis. The extent of the attributes an employee inherits on their user account through account definitions can be changed after checking the user accounts. The loss of user accounts through system changes can therefore be avoided. User account verification can be carried out manually or by using scripts.

Assigning user accounts during work hours

One Identity Manager uses special account definitions for allocating user accounts to employees during working hours. Account definitions can be created for each target system of the appointed target system type, for example, the different domains of an Active Directory environment or the individual clients of an SAP R/3 system. A priority is applied to the account definitions in order to ensure that a Microsoft Exchange mailbox, for instance, is only created when an Active Directory user account is available.

An employee can obtain a user account through the integrated inheritance mechanism by either direct assignment of account definitions to an employee, or by assignment of account definitions to departments, cost centers, locations, or business roles. All company employees can be allocated special account definitions independent of their affiliation to the departments, cost centers, locations, or business roles. It is possible to assign account

definitions to the One Identity Manager as requestable items in the IT Shop. A department manager can then request user accounts from the Web Portal for his staff.

Treatment of user accounts and personal data during disabling

The handling of personal data, particularly during long-term or temporary absence of an employee, is dealt with differently in each company. Some companies never delete personal data, but just disabled it when the person leaves the company. Other companies delete the personal data but only after they are sure that all the user accounts have been deleted.

Handling employees and user accounts

The requirements of a company's user administration are often different not only in the existing target system types, but also in the individual target systems of a target system type. Even within a target system, there may be different rules for different user groups. For example, different rules for allocating user accounts can apply in the individual domains within an Active Directory environment.

A requirement could look like the following, for example:

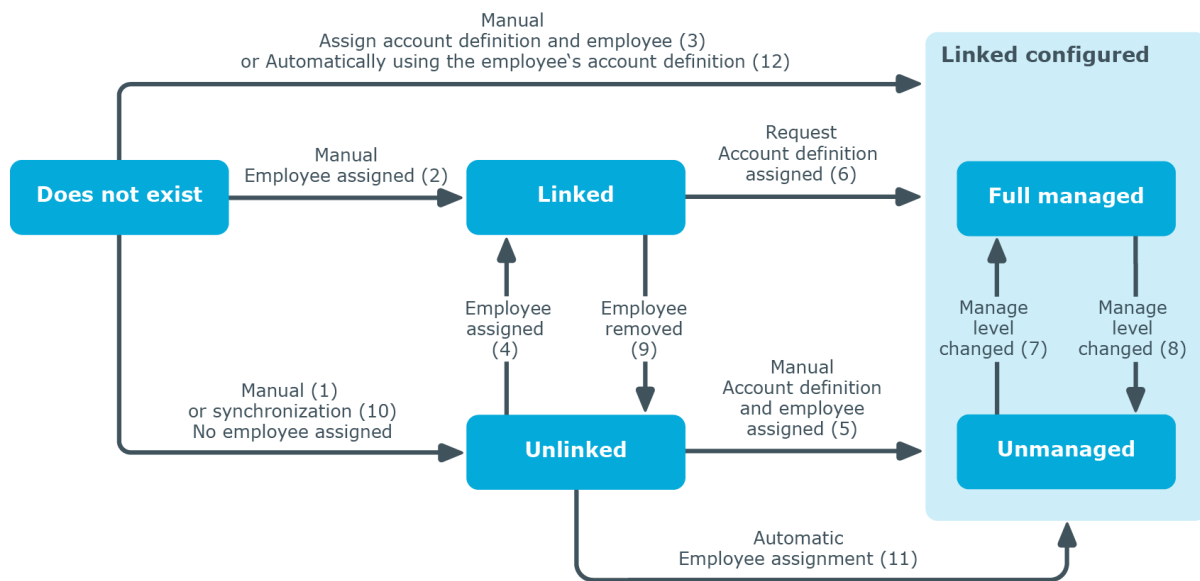
- In domain A, user accounts are administrated independently of employee data.
- In domain B, user accounts are linked to an employee. However, employee main data should not be transferred to the user accounts.
- In domain C, a user account is automatically created for each internal employee. The information for the container, home server, and profile server are based on the employee's department and location.

In order to fulfill the individual requirements of user administration, users can be divided into categories:

- **Unlinked:** The user account is not linked to an employee.
- **Linked:** The user account is linked to an employee.
- **Linked configured** (linked with configuration of the connection): 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.
- One Identity Manager supplies a default configuration with the manage levels:
 - **Unmanaged:** The user accounts are assigned to the employee, but do not have any further properties of that employee.
 - **Full managed:** The user accounts have an assignment to the employee and inherit the properties of the employees.

The following visual is designed to make user account transitions clearer. It shows the standard mechanisms for managing employees and user accounts integrated in One Identity Manager.

Figure 1: Transition states for a user account



Manually adding a user account

- Case 1: In order to manage a user account independently from employee data, the user account is added manually and is not assigned to an employee. The user account is not linked to an employee and therefore has the **Unlinked** state.
- Case 2: If the user account is already linked to an employee when inserted manually, the user account changes its state to **Linked**.
- Case 3: If an employee is already assigned when the user account is added and an account definition is assigned at the same time, the user account changes its state to **Linked configured**. Depending on the manage level used, the state becomes **Linked configured: Unmanaged** or **Linked configured: Full managed**.

Editing an existing user account

- Case 4: If an existing user account is manually assigned to an employee, the user account changes its state from **Unlinked** to **Linked**.
- Case 5: If an existing user account is manually assigned to an employee and an account definition is assigned at the same time, the user account changes its state from **Unlinked** to **Linked configured**. Depending on the manage level used, the state becomes **Linked configured: Unmanaged** or **Linked configured: Full managed**.
- Case 6: When One Identity Manager goes live, you can create IT Shop requests for existing user accounts, which are linked with employees (**Linked** state). This assigns an account definition and the user account changes its state to **Linked configured**. Depending on the manage level used, the state becomes **Linked configured: Unmanaged** or **Linked configured: Full managed**.

Changing the manage level

- Cases 7 and 8: By changing the manage level, an existing user account can change its state from **Linked configured: Unmanaged** to **Linked configured: Full managed** and vice versa. The manage level can only be changed for user accounts that are associated with an employee.

Removing employee assignments

- Case 9: By deleting the employee entry in a linked user account (**Linked**), the user account changes its state to **Unlinked**.

NOTE: The employee entry cannot be removed from user accounts with a state of **Linked configured** as long as the employee owns an account definition.

Handling user accounts during synchronization

- Case 10: When a database is synchronized with a target system, the user accounts are always added without an associated employee and therefore, have an initial state of **Unlinked**. An employee can be assigned afterwards. This can be done manually or through automated employee assignment using process handling.

Assigning employees automatically to existing user accounts

- Case 11: One Identity Manager can automatically assign employees to user accounts in an **Unlinked** state. If the target system is assigned an account definition, this account definition is automatically assigned to the employees. Depending on the manage level used, the state becomes **Linked configured: Unmanaged** or **Linked configured: Full managed**. Automatic employee assignment can follow on from adding or updating user accounts through synchronization or through manually adding a user account. For more information, see [Assigning employees automatically to user accounts](#) on page 21.

Automatically creating user account through account definitions

- Case 12: Account definitions are implemented to automatically assign user accounts to employees during normal working hours. If an employee does not have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling. The manage level is modified to suit the default manage level and the user account has the **Linked configured** state. Depending on the manage level used, the state becomes **Linked configured: Unmanaged** or **Linked configured: Full managed**. For more information, see [Account definitions and manage levels](#) on page 10.

Removing user accounts

- When an account definition assignment is removed from an employee, the associated user account is deleted.
- 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).

Using account definitions to create 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.

Account definitions and manage levels

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.

Account definitions can be created for each target system of the appointed target system type, for example, the different domains of an Active Directory environment or the individual clients of an SAP R/3 system. An account definition is always valid for a target system. You can, however, define several account definitions for one target system. Which account definition will be used is decided when creating an employee's user account. To ensure that a Microsoft Exchange mailbox, for example, is not created until an Active Directory user account exists, you can define dependencies between account definitions.

The manage levels that may be used are specified in the account definition. You can create more than one manage level. The manage level determines the scope of the properties that an employee's user account can inherit. 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.

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.

A default manage level is defined for every account definition. This manage level is used to determine the valid IT operating data when a user account is created automatically. In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

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

The effects on account definition inheritance of temporary disabling, permanent disabling, deletion, and security risk to employees is specified for each account definition.

- As long as an account definition applies to an employee, this employee keeps its linked user accounts. You may want employees that are disabled or marked for deletion to inherit account definitions to ensure that all necessary permissions are made immediately available when the employee is reactivated at a later time.
- If the account definition assignment no longer applies or is removed from the employee, the user account created through this account definition, is deleted.

In addition, you can 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.

- 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.

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.

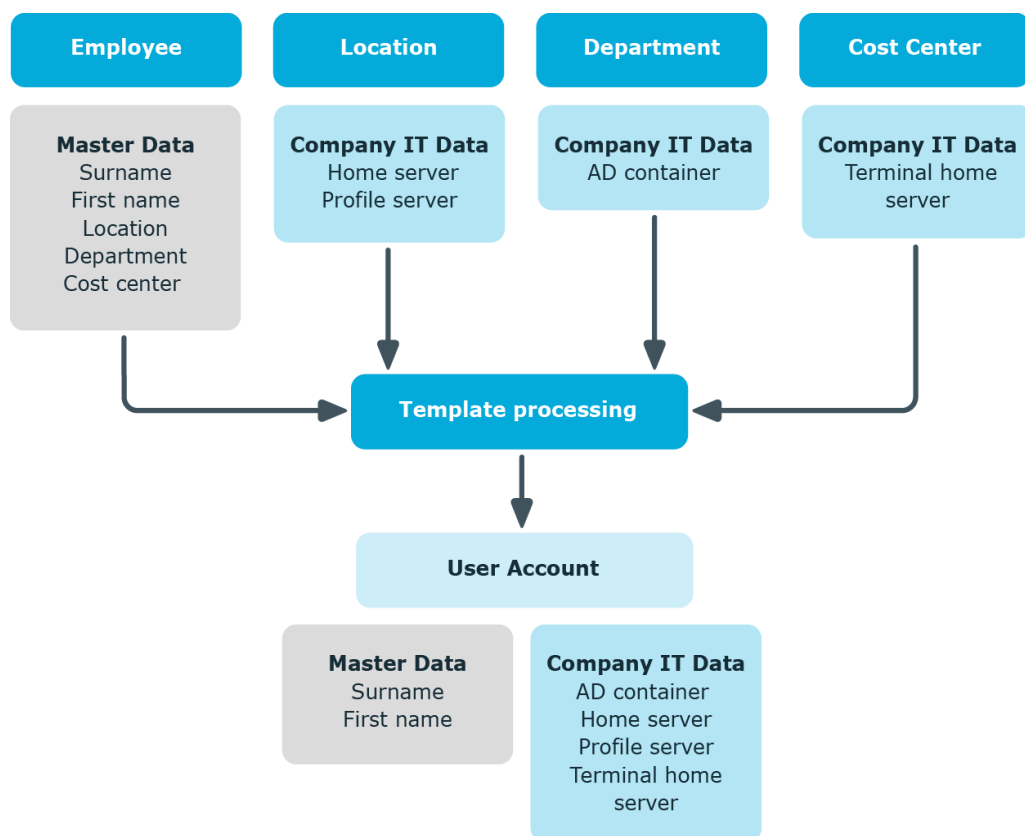
You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. Department managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions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

Determining valid IT operating data for the target systems

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.

The process sequence for automatically assigning IT operating data to the employee's user account within the One Identity Manager should be made clearer with the help of the following diagram.

Figure 2: Mapping IT operating data to a user account



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 domain A. In addition, certain employees in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain 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 domain 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.

IT operating data for the One Identity Manager default configuration

The IT operating data necessary in the One Identity Manager default configuration for automatically creating or changing employee user accounts and mailboxes in the target system is itemized in the following table.

NOTE: IT operating data is dependent on the target system and is contained in One Identity Manager modules. The data is not available until the modules are installed.

Table 1: Target system dependent IT operating data

Target system type	IT operating data
Active Directory	Container Home server Profile server Terminal home server Terminal profile server Groups can be inherited Identity Privileged user account
Microsoft Exchange	Mailbox database
LDAP	Container Groups can be inherited Identity Privileged user account
Domino	Server Certificate Template for mail file Identity
SharePoint	Authentication mode Groups can be inherited Roles can be inherited Identity Privileged user account
SharePoint Online	Groups can be inherited Roles can be inherited

Target system type	IT operating data
	Privileged user account. Authentication mode
Custom target systems	Container (per target system) Groups can be inherited Identity Privileged user account
Azure Active Directory	Groups can be inherited Administrator roles can be inherited Subscriptions can be inherited Disabled service plans can be inherited Identity Privileged user account Change password at next login
Cloud target system	Container (per target system) Groups can be inherited Identity Privileged user account
Unix-based target system	Login shell Groups can be inherited Identity Privileged user account
Oracle E-Business Suite	Identity Groups can be inherited Privileged user account.
SAP R/3	Identity Groups can be inherited Roles can be inherited Profiles can be inherited Structural profiles can be inherited Privileged user account.
Exchange Online	Groups can be inherited
Privileged Account Management	Authentication provider

Target system type	IT operating data
	Groups can be inherited Identity Privileged user account
Google Workspace	Organization Groups can be inherited Products and SKUs can be inherited Admin roles assignments can be inherited Identity Privileged user account. Change password at next login
OneLogin	Roles can be inherited Identity Privileged user account. Licensing state OneLogin group

Employee's central user account

Table 2: Configuration parameter for forming the central user accounts

Configuration parameter	Meaning
QER Person CentralAccountGlobalUnique	Specifies how the central user account is mapped. If this configuration parameter is set, the central user account for an employee is formed uniquely in relation to the central user accounts of all employees and the user account names of all permitted target systems. If the configuration parameter is not set, it is only formed uniquely related to the central user accounts of all employees.

The employee's central user account is used to form the user account login name in the active system. The central user account is still used for logging into the One Identity Manager tools. In One Identity Manager default installation, the central user account is made up of the first and the last name of the employee. If only one of these is known, then it is used for the central user account. One Identity Manager checks to see if a central user account with that value already exists. If this is the case, an incremental number is added to the end of the value.

Table 3: Example of forming of central user accounts

First name	Last name	Central user account
Jo		JO
	User1	J
Jo	User1	JOJ
Jo	User2	JOJ2

Related topics

- [Employee's default email address](#) on page 17
- [Changing employee main data](#) on page 17

Employee's default email address

The employee's default email address is displayed on the mailboxes in the activated target system. In the One Identity Manager default installation, the default email address is formed from the employee's central user account and the default mail domain of the active target system.

The default mail domain is determined using the **QER | Person | DefaultMailDomain** configuration parameter.

- In the Designer, set the configuration parameter and enter the default mail domain name as a value.

Related topics

- [Employee's central user account](#) on page 16
- [Changing employee main data](#) on page 17

Changing employee main data

The following covers only the employee main data that affects the user account of an employee with the **Full managed** manage level if it is changed in the One Identity Manager default installation.

General changes

General changes refer to data changes relating to an employee's telephone number, fax number, mobile telephone, street, postal, or ZIP code. This process changes the data in the target system to which the employees are assigned, assuming this data is mapped in the respective target systems.

Changing an employee's name

Changes to an employee's name influence how an employee's central user account is set up. The central user account is made up of the employee's first and last names according to the formatting rules. The central user account is used as a template for formatting user account login names in some target systems. When a user account is added, other overriding formatting rules control how, for example, the home and profile directories are formatted up from the central user account.

Employee job rotation inhouse

Job rotation is affected by changes to the company data location or department. In One Identity Manager, the administrative tasks for changing the target system specific IT operating data, for example, domains, home servers, or profile servers, are automated. There are other sub-processes for each target system due to system-dependent differences in the actions necessary for changing departments.

Related topics

- [Employee's central user account](#) on page 16
- [Employee's default email address](#) on page 17

Templates and processes for implementing account definitions

Only user account properties used in the script template `TSB_ITDataFromOrg` are available. Create custom templates using this script if you want to use different or additional properties than those in the default installation.

In the One Identity Manager default installation there is one process per target system type for creating user accounts through account definitions. These can be used as templates for the company-specific implementation of the method.

NOTE: Processes are defined in the One Identity Manager modules and are not available until the modules are installed.

The name of the process is formatted as follows:

```
<MMM>_PersonHasTSBAccountDef_Autocreate_<user account table>
```

where:

`<MMM>` = module ID

`<user account table>` = Table, in which the user account of the target system type is mapped.

Examples for implementing several account definitions within a target system type

If several target systems are managed using account definitions in a target system type, a separate account definition must be set up for each target system. When the employee is assigned both account definitions, subsequent script and process handling ensure that the employee obtains the user accounts in both target systems.

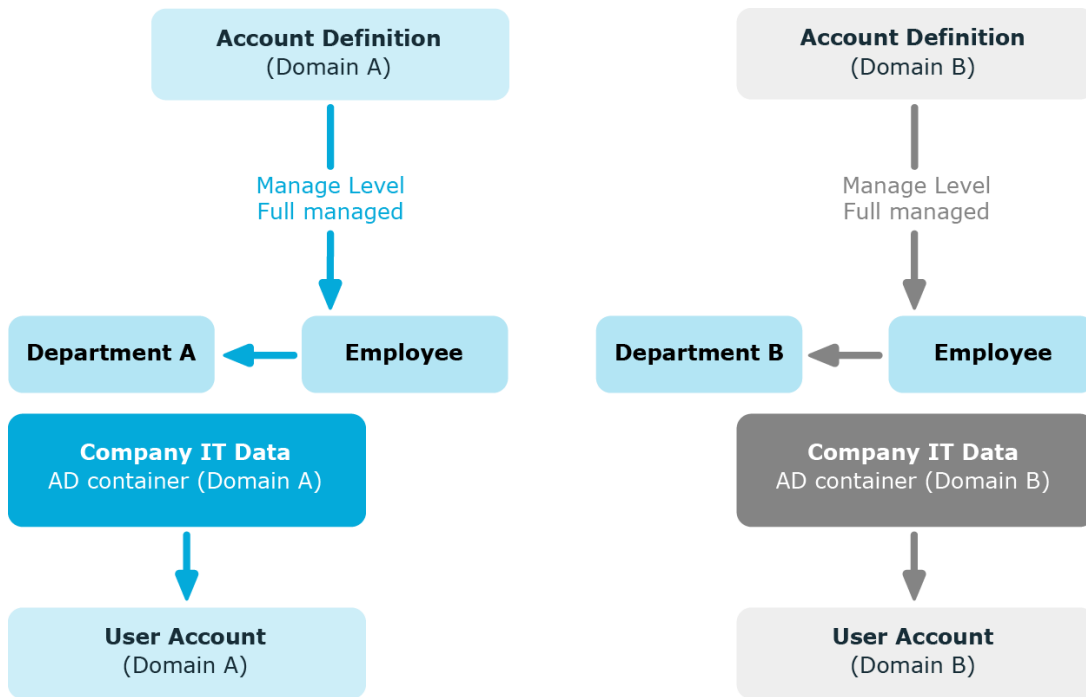
Example: Employees can have a user account only in one domain

There are two domains in an Active Directory environment. The employees can only have a user account in one of the domains. The department operational data is used to determine whether the user account is created in domain A or domain B.

Create an account definition A for domain A and an account definition B for domain B and assign them the **Full managed** manage level. This manage level uses the One Identity Manager default templates to determine the IT operating data. In the IT operating data mapping rule, specify the **department** property for both account definitions for finding the valid IT operating data.

If the employee belongs to department A, they receive (for example by dynamic assignment) the account definition A and as a result, a user account in domain A. If the employee belongs to department B, they are assigned the account definition B and they receive a user account in domain B.

Figure 3: Creating user accounts based on account definitions

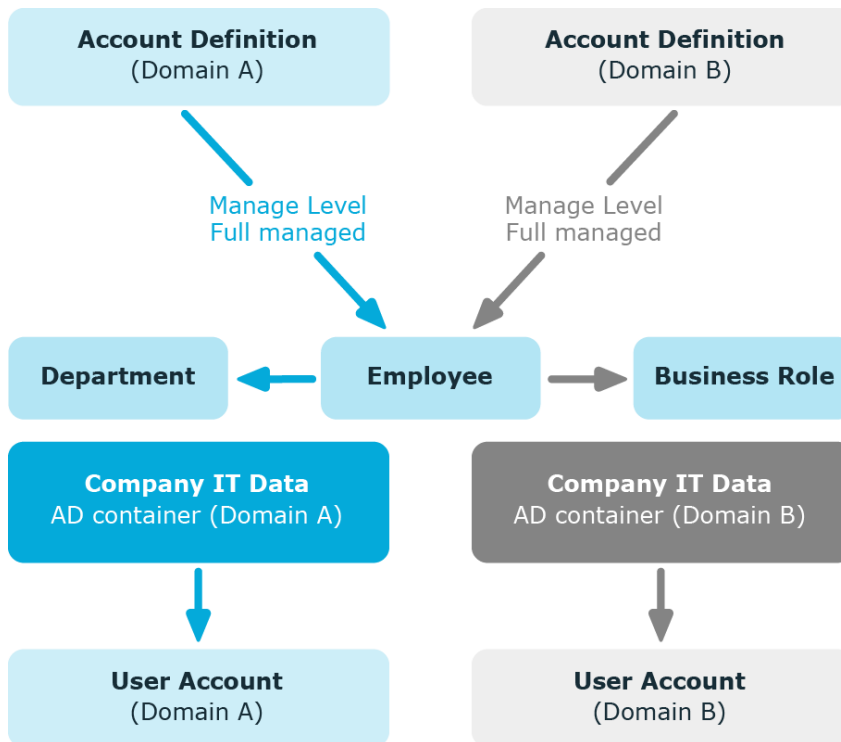


Example: Employees can have a user account in both domains

There are two domains in an Active Directory environment. The employees can have a user account in both of the domains. The user account in domain A is allocated IT operating data through the employee's department. The user account in domain B is allocated IT operating data through the employee's primary business role.

Create an account definition A for domain A and an account definition B for domain B and assign them the **Full managed** manage level. The **Full managed** manage level uses One Identity Manager default templates to determine the IT operating data. Specify the **department** property for account definition A in the IT operating data mapping rule for finding the valid IT operating data. Specify the property **business role** for account definition B in the IT operating data mapping rule for finding the valid IT operating data.

Figure 4: Creating user accounts based on account definitions



Assigning employees automatically to user accounts

Automatic employee assignment is used to:

- Assign existing employees to user accounts
- Create employee main data based on existing user accounts

Through synchronization user accounts are initially loaded from the target system into One Identity Manager. Automatic assignment of user accounts to existing employees can take place by subsequently modifying scripts and processes. If necessary, new employees can be created based on existing user accounts to which they are then assigned. However, this is not the One Identity Manager default method. You can also use this procedure to create employee data from existing target system user accounts during synchronization.

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

The criterion for automatically assigning employees to user accounts can be customized to meet the company's needs. Employees can be directly assigned to existing user accounts as required, based on a suggestion list.

Run the following tasks to assign employees automatically.

- In the Designer, set the configuration parameter for automatic assignment of employees to user accounts and select the required mode.
- Define search criteria for the employee assignment.
- If managed user accounts should arise through automatic employee assignment (**Linked configured** state), assign an account definition to the target system. Ensure that the manage level to be used is entered as the default manage level.

If no account definition is provided in the target system, the user accounts are only linked to the employee (**Linked** state). This is the case on initial synchronization, for example.

Related topics

- [Handling employees and user accounts](#) on page 7
- [Configuring automatic employee assignment](#) on page 22
- [Editing search criteria for automatic employee assignment](#) on page 24
- [Modifying scripts for automatic employee assignment](#) on page 29

Configuring automatic employee assignment

In the One Identity Manager default installation, the automatic assignment of employees to user accounts is controlled by configuration parameters and therefore globally effective for a target system type. A distinction is made here between the synchronization and the default methods.

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: The configuration parameters are included in the One Identity Manager modules and are available once the modules are installed.

Configuration parameters for automatic employee assignment:

- **TargetSystem | <Target system type> | PersonAutoDefault**
- **TargetSystem | <Target system type> | PersonAutoFullSync**

Each configuration parameter has one of the permitted modes:

- **NO:** There is no automatic assignment of a person to the user account. This is the default value that is also displayed when the configuration parameter is not active.
- **SEARCH:** If no employee is assigned to the user account, the system searches for the appropriate employee based on defined criteria and assigns the employees found to the user account. If an employee is not found, no new employee is added.
- **CREATE:** If no employee is assigned to the user account, a new employee is always created, some properties are initialized, and the employee is assigned to the user account.

| **NOTE:** This mode is not available for all target system types.

- **SEARCH AND CREATE:** If no employee is assigned to the user account, the system searches for the appropriate employee based on defined criteria and assigns the employees found to the user account. If no employee is found, a new one is added, some of the properties are initialized, and the employee is assigned to the user account.

| **NOTE:** This mode is not available for all target system types.

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 change this manage level later.

NOTE:

In the default installation, after synchronizing, employees are automatically created for the user accounts. If an account definition for the target system is not 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.

To manage user accounts through account definitions

1. Create an account definition.
2. 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 **<target system type> > User accounts > Linked but not configured > <target system>** 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.

In the target system-dependent Insert/Update processes of the One Identity Manager default installation, the configuration parameters are evaluated and the implementation mode is determined. The names of the corresponding process steps are Search and Create Person for Account and Search and Create Person for Account (Fullsync). Process steps can be used as templates to put into effect the automatic employee assignment in different areas of a target system, such as, the separate domains of an Active Directory environment.

Editing search criteria for automatic employee assignment

The criteria for employee assignments are defined for the target system. 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 target system 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.

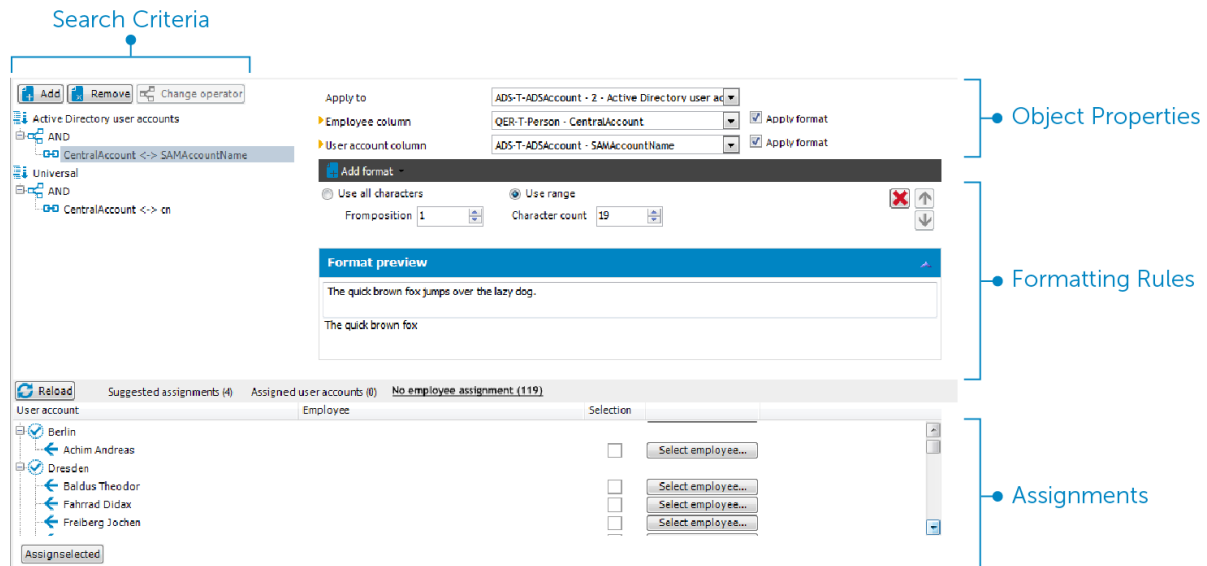
NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One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

Detailed information about this topic

- [Define search criteria for employee assignment](#) on page 25
- [Finding employees and directly assigning them to user accounts](#) on page 27

Define search criteria for employee assignment

Figure 5: Search criteria for 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.

To define search criteria for employee assignment

1. In the Manager, select the **Target system type > <target system>** category.
2. Select the target system in the result list and run the **Define search criteria for employee assignment** task.
3. Select the object definition for the mapping.

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*.

- a. To add a new object definition, click **Add > Criteria**. Use the **Apply to** menu item to select the object definition that the search criteria was defined for.
The search criteria is applied to all user accounts if no object definition is selected.
- b. To change the object definition of an existing search criterion, select the search criterion in the **Search criteria** view. Use the **Apply to** menu item to select the object definition that the search criteria was defined for.

If the existing selection is deleted, the search criterion is applied to all user accounts.

4. Select the object properties to map.

- **Column for employee:** Select the column in the Employee table on which the search is carried out.
- **Column for user account:** Select the column in the user account table that supplies the value for searching for a person.

5. Define the formatting rule to limit the search criteria.

In the **Add format** menu, select a format template. Define the formatting rule to apply to the search string. You can combine different format templates.

Table 4: Format templates

Format template	Meaning
Character range	Characters in the character string to be used as the search criterion.
Crop to fixed length	Defines the length of the character string to search for. Use fill characters at the beginning or end of the string to ensure it reaches the fixed length.
Remove leading or trailing characters	Characters that are to be removed at the start or end of the character string. The remaining string forms the search criteria.
Split value	Characters for which the character string should be split and for which the remaining parts should be used as a search criterion.

6. Test the format rules.

In the **Format preview** view, enter a character string to which the formatting is applied. Use this to test the effects of your search criteria formatting.

7. Apply the formatting rules.

Enable **Use format** on the columns on which to limit the search criteria.

8. Save the changes.

Different object properties can be joined for search criteria. Both AND and OR operators can be used.

Example: AND operator

To assign employees to Notes user accounts, the surname as well as first name must be the same for the employee and the user account. The following table columns are

mapped:

AND

Person.Firstname - NotesUser.Firstname

Person.LastName - NotesUser.LastName

Example: OR operator

To assign employees to Active Directory user accounts, either the employee's central user account and the user account's login name must be identical or the employee's full name and the user account's display name. The following table columns are mapped:

OR

Person.CentralAccount - ADSAccount.SAMAccountName

Person.InternalName - ADSAccount.DisplayName

To link object properties in search criteria

1. In the **Search criteria** view, select the operator to which you want to add another object property. Click **Change operator** to select the operator for the link.
2. Click **Add > Criteria**.
3. Select the object properties to map.
4. Select the object properties to be mapped.
5. If you want to nest links, click **Add > AND operator** or **Add > OR operator** and rerun steps 2 to 4.
6. Save the changes.

To delete search criteria

1. Mark the search criteria and click **Delete**.
2. Save the changes.

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 5: 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

- At the bottom of the **Define search criteria for employee assignment** 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.

Modifying scripts for automatic employee assignment

Automatic employee assignments are controlled through scripts. In **SEARCH** mode, these scripts assign existing employees to the user accounts based on the defined search criteria. The scripts for **CREATE** mode also define the properties that are initialized when a new person is generated. These scripts are implemented in a default One Identity Manager installation for each target system type. The name of this script is:

`<target system type>_PersonAuto_Mapping_<account type>`

where:

`<target system type>` = short name of the addressed target system type

`<account type>` = Table containing the user accounts

TIP: You can customize scripts to extend search criteria for automatic employee assignment or the properties of new employees. The scripts can be overwritten. To do this, create a copy of the existing script and customize the copy.

In automatic employee assignment in **CREATE** mode, some properties of the user account are transferred to the new employee object. Initializing the employee properties is done using the script. Initializing the properties when an employee is being created for a user account is done by evaluating the entry in the table `DialogNotification`. In this table the connected properties are mapped as a bidirectional pair through the formatting rules. Evaluation of entries in `DialogNotification` are exemplified in the following by showing initialization of an employee's surname:

Example:

The last name of an Active Directory user account is made up of the surname of the employee.

Value template for `ADSAccount.Surname`:

```
Value = $FK(UID_Person).Lastname$
```

If the employee's surname changes, the last name of the Active Directory user also changes. The column `Person.Lastname` is therefore the sender and the column `ADSAccount.Surname` is the receiver.

Relationship as in the table `DialogNotification`:

```
Person.Lastname -- > ADSAccount.Surname
```

The table `DialogNotification` can be used to help with the initialization of the properties for a new employee in that the relationships can be removed in reverse. The surname of an employee can be replaced with the surname of the Active Directory user. Thus, certain presets for the employee object can be automatically generated. However, only explicit relationships can be removed.

Example:

The display name of an Active Directory user account should be made up of the surname and the first name of an employee.

Relationships as in the table `DialogNotification`:

```
Person.Lastname -- > ADSAccount.Displayname
```

```
Person.Firstname -- > ADSAccount.Displayname
```

The `Person.Firstname` and `Person.Lastname` cannot be determined from the `ADSAccount.Displayname`, since this is a compound value.

You can use the script `TSB_PersonAuto_GetPropMappings` to make it easier to map employee properties to user account properties. This script evaluates the relationship of the properties as used in the table `DialogNotification`. The script creates a VB.Net script code and the possible assignments, when it is run by the System Debugger. This code can subsequently be inserted into the script `<target system type>_PersonAuto_Mapping_<account type>`.

Example: Generated TSB_PersonAuto_GetPropMappings script

```
' PROPERTY MAPPINGS ADSAccount - Person
' ADSAccount.Initials -- > Person.Initials
' ADSAccount.Locality-- > Person.City
...
Try
    myPers.PutValue("Initials", myAcc.GetValue("Initials").String)
Catch ex As Exception
End Try
Try
    myPers.PutValue("City", myAcc.GetValue("Locality").String)
Catch ex As Exception
End Try
...
```

Deactivating and deleting employees and user accounts

How employees are handled, particularly in the case of permanent or partial withdrawal of an employee, varies between individual companies. There are companies that never delete employees, and only deactivate them when they leave the company. Other firms delete the employee, but only after they have ensured that all the user accounts are removed. Different requirements could also apply to user account group memberships.

The handling of user accounts and their group memberships when employees are deactivated or deleted depends on how the user accounts are managed.

The following scenarios apply:

- User accounts are linked to employees and managed through account definitions.
- User accounts are linked to employees. No account definition is applied.

Detailed information about this topic

- [Temporarily deactivating employees](#) on page 32
- [Permanently deactivating employees](#) on page 33
- [Deferred deletion of employees](#) on page 34

- [Disabling and deleting using account definitions](#) on page 36
- [Handling group memberships](#) on page 38

Temporarily deactivating employees

The employee has temporarily left the company and is expected to return at a predefined date. The desired course of action could be to disable the user account and remove all group memberships. Or the user accounts could be deleted and reestablished with the employee's return, even if it is with a new system identification number (SID).

Temporary disabling of an employee is triggered by:

- The **Temporary disabled** option
- The start and end date for deactivation (**Temporary disabled from** and **Temporary disabled until**)

NOTE:

- Configure the **Lock accounts of employees that have left the company** schedule in the Designer. This schedule checks the start date for disabling and sets the **Temporarily disabled** option when it is reached.
- In the Designer, configure the **Enable temporarily disabled accounts** schedule. This schedule monitors the end date of the disabled period and enables the employee with their user accounts when the date expires. Employee's user accounts that were disabled before the period of temporary absence are also re-enabled once the period has expired.

Scenario: user accounts are linked to employees and are managed through account definitions.

- Specify in the account definitions, how temporary deactivating employees affects the user account. In each manage level you can use the **Lock user accounts if temporarily disabled** option to define whether the user accounts remain enabled or are locked while they are disabled.
- Specify in the account definitions, how temporary deactivation employees affects their user accounts' group memberships. In each manage level you can use the **Retain groups if temporarily disabled** option to define whether the user accounts' group memberships are retained or removed when employees are deactivated.

Scenario: user accounts are linked to employees. No account definition is applied.

- Specify the desired behavior using the **QER | Person | TemporaryDeactivation** configuration parameter. If the configuration parameter is set, the employee's user accounts are locked while the employee is deactivated. If the configuration

parameter is not set, the employee's properties do not have any effect on the associated user accounts.

- The user accounts keep their group memberships. Implement company-specific processes to remove group memberships as required.

Related topics

- [Permanently deactivating employees](#) on page 33
- [Deferred deletion of employees](#) on page 34
- [Disabling and deleting using account definitions](#) on page 36
- [Handling group memberships](#) on page 38

Permanently deactivating employees

Employees can be deactivated permanently when, for example, they leave the company. It might be necessary, to remove access to this employee's entitlements in connected target systems and their company resources.

Effects of permanent deactivating an identity are:

- The employee cannot be assigned to employees as a manager.
- The employee cannot be assigned to roles as a supervisor.
- The employee cannot be assigned to attestation policies as an owner.
- There is no inheritance of company resources through roles, if the additional **No inheritance** option is set for an employee.
- Employee user accounts are locked or deleted and then removed from group memberships.

Trigger permanent deactivation through:

- The **Deactivate employee permanently** task

This task ensures that the **Permanently deactivates** option is enabled and the leaving date and last working day are set to the current date.

- The leaving date is reached

NOTE:

- In the Designer, check the **Lock accounts of employees that have left the company** schedule. This schedule regularly checks the leaving date and sets the **Permanently deactivated** option on reaching the date.
 - The **Re-enable employee** task ensures that the employee is re-enabled.
- The **Denied** certification status

If an employee's certification status is set to **Denied** manually or as a result of attestation, the employee is immediately permanently deactivated. When the

employee's certification status is changed to **Certified**, the employee is activated again.

| **NOTE:** This function is only available if the Attestation Module is installed.

Scenario: user accounts are linked to employees and are managed through account definitions.

- Specify in the account definitions, how permanently deactivating an employee affects the user account. In each manage level you can use the **Lock user accounts if permanently disabled** option to define whether the user accounts remain enabled or are locked while they are disabled.
- Specify in the account definitions, how permanent deactivation of an employee affects their user accounts' group memberships. In each manage level you can use the **Retain groups if permanently disabled** option to define whether the user accounts' group memberships are retained or removed when an employee is deleted.

Scenario: user accounts are linked to employees. No account definition is applied.

- Specify the desired behavior using the **QER | Person | TemporaryDeactivation** configuration parameter. If the configuration parameter is set, the identity's user accounts are locked while the employee is deactivated. If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.
- The user accounts keep their group memberships. Implement company-specific processes to remove group memberships as required.

Related topics

- [Temporarily deactivating employees](#) on page 32
- [Deferred deletion of employees](#) on page 34
- [Disabling and deleting using account definitions](#) on page 36
- [Handling group memberships](#) on page 38

Deferred deletion of employees

When an employee is deleted, the system checks whether user accounts and company resources are still assigned to the employee or whether requests are open in the IT Shop. The employee is marked for deletion and therefore locked out of further processing.

By default, employees are finally deleted from the database after 30 days. During this period it is possible to re-enable the employee. A restore is not possible once deferred deletion has expired.

Before an employee can finally be deleted from the One Identity Manager database, you need to delete all company resource assignments and close all requests. You can do this manually or implement custom processes to do it.

All the user accounts linked to an employee can be deleted by default by One Identity Manager once this employee has been deleted. If no more company resources are assigned, the employee is finally deleted.

Scenario: user accounts are linked to employees and are managed through account definitions.

- Specify in the account definitions, how deleting employees affects the user accounts. In each manage level you can use the **Lock user accounts if deletion is deferred** option to define whether the user accounts remain enabled or are locked while they are deferred for deletion. In any case, the user accounts are deleted from the One Identity Manager database once the deferred deletion period has expired.
- Specify in the account definitions, how deleting employees affects the user accounts' group memberships. In each manage level you can use the **Retain groups if permanently disabled** option to define whether the user accounts' group memberships are retained or removed when an employee is deleted.

Scenario: user accounts are linked to employees. No account definition is applied.

- Implement custom processes to delete linked user accounts. The employee stays marked for deletion until all user accounts are deleted and assignments to company resources have been removed. The user accounts remain enabled with deferred deletion until they are physically deleted.
- Use the **QER | Person | User | KeepMembershipsOfLinkedAccount** configuration parameter to specify how user account group memberships are handled. Permitted values are:
 - **NONE**: All memberships are withdrawn. This is the default.
 - **ALL**: All memberships remain.
 - **DIRECT**: Direct memberships remain, inherited ones are withdrawn.

IMPORTANT: If special inheritance handling is defined for a group, then the configuration parameter settings may be overridden.

Related topics

- [Temporarily deactivating employees](#) on page 32
- [Permanently deactivating employees](#) on page 33
- [Disabling and deleting using account definitions](#) on page 36
- [Handling group memberships](#) on page 38

Disabling and deleting using account definitions

If user accounts are managed through account definitions, you can specify the desired behavior for handling user accounts and group memberships through account definitions and manage levels for temporary disabling, permanent disabling, deletion, and security risk to employees.

You can define special handling for each target system belonging to a target system type, through the relationship between the target system and account definition. For more information, see [Using account definitions to create user accounts](#) on page 10.

Assigning account definitions to employees

The effects on account definition inheritance of temporary disabling, permanent disabling, deletion, and security risk to employees is specified for each account definition. The settings of previous account definitions are overwritten.

You may want employees that are disabled or marked for deletion to inherit account definitions to ensure that all necessary permissions are made immediately available when the employee is reactivated at a later time.

IMPORTANT: As long as an account definition applies to an employee, this employee keeps its linked user accounts. If the account definition assignment no longer applies, the user account created through this account definition is deleted.

The following user account definition options are available for mapping behavior.

Table 6: Main data of an account definition for the assignment behavior of the account

Property	Description
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 stays the same.</p> <p>Option not set: 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 stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on deferred deletion	<p>Specifies the account definition assignment on deferred deletion of employees.</p>

Property	Description
	Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.

Handling user accounts and employees

The effects on user accounts of temporary disabling, permanent deactivating, deletion, and security risk of an employee is specified for each manage level.

In order to remove permissions from an employee when they are being deactivated or deleted, the employee's user accounts can be locked. If the employee is reinstated at a later date, the user accounts are also reactivated.

The following options are available for each manage level on an account definition for handling user accounts.

Table 7: Main data for a manage level for handling user accounts

Property	Description
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated employees are locked.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated employees are locked.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.

Inheritance of group memberships by the employee's user accounts

The effects on user accounts of temporary deactivation, permanent deactivation, deletion, and security risk of an employee is specified for each manage level.

If an employee is deactivated or marked for deletion, inheritance of groups memberships can be suppressed for the account definition target system. You might want this behavior if an employee's user accounts and mailboxes are locked and therefore cannot be included in distribution lists. During this deactivation period, no inheritance processes should be calculated for this employee. Existing group memberships are deleted.

The following options are available for each manage level on an account definition for handling group memberships.

Table 8: Master data of a manage level for handling group memberships

Property	Description
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees inherit group memberships.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

NOTE: Inheritance settings can be overridden for individual groups. For more information, see [Handling group memberships](#) on page 38.

Related topics

- [Temporarily deactivating employees](#) on page 32
- [Permanently deactivating employees](#) on page 33
- [Deferred deletion of employees](#) on page 34

Handling group memberships

How group memberships are handled when user accounts are disabled or deleted depends on how you manage the user accounts.

Scenario: user accounts are linked to employees and are managed through account definitions.

- You use the manage level of account definitions to specify how group memberships of user accounts are handled when employees are temporarily deactivated, permanently deactivated, deleted, or pose a security risk.

Scenario: user accounts are linked to employees. No account definition is applied.

- If an employee is temporarily or permanently deactivated, the group memberships of the user accounts are retained.
- Use the **QER | Person | User | KeepMembershipsOfLinkedAccount** configuration parameter to specify deferred deletion behavior.

Overriding inheritance settings for individual groups

Sometimes it may be necessary to define different behavior for individual group. For example, it is possible to define never to automatically remove a group from user accounts or never to override the account definition settings.

You can specify behavior different from the default for the following group inheritance settings.

- Retain groups if temporarily disabled
- Retain groups if permanently disabled
- Retain groups on deferred deletion
- Retain groups on security risk
- Retain groups if user account disabled

Permitted values are:

- **According to manage level:** The manage level settings apply to the group memberships. You use the manage level of account definitions to specify how group memberships are handled when employees are temporarily deactivated, permanently deactivated, deleted, or pose a security risk.

The setting takes effect for user accounts linked to employees and managed via account definitions.

- **Never:** The group is never inherited. Existing group memberships are removed. The group assignment is maintained but the assignment has no effect.

The setting is effective for user accounts linked to employees. The setting takes effect regardless of whether the user accounts are managed via account definitions or not.

IMPORTANT: If the **Never** value is applied to the **Retain groups if user account disabled** setting, the group memberships of user accounts that are not linked to an employee also become invalid.



NOTE: This overrides the settings in the **QER | Person | User | KeepMembershipsOfLinkedAccount** configuration parameter.

- **Always:** The group is always inherited. Existing group memberships are remain intact.

The setting is effective for user accounts linked to employees. The setting takes effect regardless of whether the user accounts are managed via account definitions or not.

NOTE: This overrides the settings in the **QER | Person | User | KeepMembershipsOfLinkedAccount** configuration parameter.

To override inheritance settings

1. In the Manager, select the **<target system type> > Groups > Override inheritance settings** category.
2. To add a new group, in the result list, click 
 - a. Next to the **Group** field, click .
 - b. Under **Table**, select the table that maps the group.
 - c. Under **Group**, select the group.
 - d. Click **OK**.
- OR -
3. To change the values for an existing group, select the group in the result list.
4. Enter the values for the inheritance settings.
5. Save the changes.

NOTE: Depending on the target system type, the inheritance settings of other permissions types may be overridden.

Related topics

- [Temporarily deactivating employees](#) on page 32
- [Permanently deactivating employees](#) on page 33
- [Disabling and deleting using account definitions](#) on page 36
- [Deferred deletion of employees](#) on page 34

The Unified Namespace

The Unified Namespace is a virtual system in which different target systems can be mapped with their structures, user accounts, system entitlements and memberships. The Unified Namespace allows a general, cross-target system mapping of all connected target systems. This means that target systems like Active Directory domains can be mapped just the same as custom target systems.

You can use other Unified Namespace core functionality across target systems by mapping target systems in the One Identity Manager, such as identity audit, attestation, or report functions. You are supplied with several reports by default.

Detailed information about this topic

- [Mapping target system objects in Unified Namespace](#) on page 41
- [Special features for mapping object properties](#) on page 47
- [One Identity Manager users for managing target systems in Unified Namespace](#) on page 47
- [Displaying Unified Namespace objects](#) on page 49
- [Reports about a target system in the Unified Namespace](#) on page 49
- [Reports about all target systems in the Unified Namespace](#) on page 51

Mapping target system objects in Unified Namespace

Each Unified Namespace object type joins the various tables of the One Identity Manager schema required for mapping connected target systems. The various target system tables are joined in database layers. This allows different object properties to be mapped uniformly.

Use the following database views to run compliance checks or attestation across target systems and also to create reports across target systems.

Target systems (UNSRoot)

The UNSRoot view maps the base objects of target system synchronization.

Target system type	Table
Active Directory	ADSDomain
Microsoft Exchange	EX0Organization
SharePoint	SPSSite
SharePoint Online	O3SSite
HCL Domino	NotesDomain
SAP R/3	SAPMandant
LDAP	LDPDomain
Custom target systems	UNSRotB
Unix	UNXHost
Azure Active Directory	AADOrganization
Google Workspace	GAPCustomer
Cloud target systems	CSMRoot
Oracle E-Business Suite	EBSSystem
Privileged Account Management	PAGAppliance

Container (UNSContainer)

The UNSContainer view maps the target system's container structures.

Target system type	Table
Active Directory	ADSContainer
SharePoint	SPSWeb
SharePoint Online	O3SWeb
LDAP	LDAPContainer
Custom target systems	UNSContainerB
Cloud target systems	CSMContainer
Google Workspace	GAPOrgUnit

User accounts (UNSAccount)

The UNSAccount view maps the user accounts of target system.

Target system type	Table
Active Directory	ADSAccount, ADSContact
Microsoft Exchange	EX0MailUser, EX0MailContact, EX0Mailbox
SharePoint	SPSUser
SharePoint Online	O3SUser
HCL Domino	NotesUser
SAP R/3	SAPUser, SAPBWUser, SAPUserMandant
LDAP	LDAPAccount
Custom target systems	UNSAccountB
Unix	UNXAccount
Azure Active Directory	AADUser
Exchange Online	O3EMailbox, O3EMailContact, O3EMailUser
Google Workspace	GAPUser
Cloud target systems	CSMUser
Oracle E-Business Suite	EBSUser
Privileged Account Management	PAGUser

System entitlements (UNSGroup)

The UNSGroup view maps the target system's system entitlements, such as groups, role, or profiles.

Target system type	Table
Active Directory	ADSGroup
Microsoft Exchange	EX0DL
SharePoint	SPSGroup, SPSRLAsgn
SharePoint Online	O3SGroup, O3SRLAsgn
HCL Domino	NotesGroup
SAP R/3	SAPGrp, SAPProfile, SAPRole, SAPHRP, SAPBWP
LDAP	LDAPGroup
Custom target systems	UNSGroupB, UNSGroupB1, UNSGroupB2, UNSGroupB3
Unix	UNXGroup
Azure Active Directory	AADGroup, AADDeniedServicePlan, AADDirectoryRole,

Target system type	Table
	AADSubSku
Exchange Online	O3EDL, O3EUnifiedGroup
Google Workspace	GAPGroup, GAPPaSku, GAPOrgAdminRole
Cloud target systems	CSMGroup, CSMGroup1, CSMGroup2, CSMGroup3
Oracle E-Business Suite	EBSResp
Privileged Account Management	PAGUsrGroup

Permissions controls (UNSIItem)

The UNSIItem view maps the target system's additional permissions controls.

Target system type	Table
Custom target systems	UNSIItemB
Cloud target systems	CSMItem

Assignment system entitlements (UNSAccountInUNSGroup)

The UNSAccountInUNSGroup view maps system entitlement assignments to the target system's user accounts.

Target system type	Table
Active Directory	ADSAccountInADSGroup, ADSContactInADSGroup
SharePoint	SPSUserInSPSGroup, SPSUserHASSPSRLAsgn
HCL Domino	NotesUserInGroup
SAP R/3	SAPUserInSAPGrp, HelperSAPUserInSAPRole, SAPUserInSAPProfile, HelperSAPUserInSAPHRP, SAPBWUserInSAPBWP
LDAP	LDAPAccountInLDAPGroup
Custom target systems	UNSAccounBInUNSGroupB, UNSAccounBInUNSGroupB1, UNSAccounBInUNSGroupB2, UNSAccounBInUNSGroupB3, UNSAccounBHasUNSGroupB, UNSAccounBHasUNSGroupB1, UNSAccounBHasUNSGroupB2, UNSAccounBHasUNSGroupB3
Unix	UNIXAccountInUNIXGroup
Azure Active Directory	AADUserHasDeniedService, AADUserInDirectoryRole, AADUserInAADGroup

Target system type	Table
Exchange Online	O3EAADUserInUnifiedGroup, O3EMailboxInDL, O3EMailContactInDL, O3EMailUserInDL
Google Workspace	GAPUserInGroup, GAPUserInPaSku, GAPUserInOrgAdminRole
Cloud target systems	CSMUserInGroup, CSMUserInGroup1, CSMUserInGroup2, CSMUserInGroup3, CSMUserHasGroup, CSMUserHasGroup1, CSMUserHasGroup2, CSMUserHasGroup3
Oracle E-Business Suite	EBSUserInRespCompressed
Privileged Account Management	PAGUserInUsrGroup

Assignment permissions controls (UNSAccountHasUNSItem)

The UNSAccountHasUNSItem view maps assignments of additional permissions controls to the target system's user accounts.

Target system type	Table
Custom target systems	UNSAccountBHasUNSItemB
Cloud target systems	CSMUserHasItem

Assignment system entitlements (UNSGroupInUNSGroup)

The UNSGroupInUNSGroup view maps system entitlement assignments to the target system's system entitlements.

Target system type	Table
Active Directory	ADSGroupInADSGroup
SharePoint	SPSGroupHasSPSRLAsgn
HCL Domino	NotesGroupInGroup
SAP R/3	SAPProfileInSAPProfile, SAPRoleInSAPRole, SAPProfileInSAPRole
LDAP	LDAPGroupInLDAPGroup
Custom target systems	UNSGroupBInUNSGroupB, UNSGroupBInUNSGroupB1, UNSGroupBInUNSGroupB2, UNSGroupBInUNSGroupB3
Azure Active Directory	AADGroupInGroup
Exchange Online	O3EDLInDL

Target system type	Table
Google Workspace	GAPGroupInGroup
Cloud target systems	CSMGroupInGroup, CSMGroupInGroup1, CSMGroupInGroup2, CSMGroupInGroup3

Assignment permissions controls (UNSGroupHasUNSItem)

The UNSGroupHasUNSItem view maps assignments of additional permissions controls to the target system's system entitlements.

Target system type	Table
Custom target systems	UNSGroupBHasUnsItemB
Cloud target systems	CSMGroupHasItem

Inheritance exclusion (UNSGroupExclusion)

The UNSGroupExclusion view maps system entitlement definitions that are mutually exclusive.

Target system type	Table
Active Directory	ADSGroupExclusion
SharePoint	SPSGroupExclusion, SPSRLAsgnExclusion
HCL Domino	NotesGroupExclusion
SAP R/3	SAPGrpExclusion, SAPProfileExclusion, SAPRoleExclusion
LDAP	LDAPGroupExclusion
Custom target systems	UNSGroupBExclusion, UNSGroupB1Exclusion, UNSGroupB2Exclusion, UNSGroupB3Exclusion
Unix	UNIXGroupExclusion
Azure Active Directory	AADGroupExclusion, AADSubSkuExclusion
Google Workspace	GAPGroupExclusion
Cloud target systems	CSMGroupExclusion, CSMGroup1Exclusion, CSMGroup2Exclusion, CSMGroup3Exclusion
Oracle E-Business Suite	EBSRespExclusion
Privileged Account Management	PAGUsrGroupExclusion

System entitlement hierarchy (UNSGroupCollection)

The UNSGroupCollection view maps hierarchies of system entitlements.

Target system type	Table
Active Directory	ADSGroupCollection
SharePoint	SPSGroupCollection, SPSRLAsgn
HCL Domino	NotesGroupCollection
SAP R/3	SAPCollectionRPG
LDAP	LDAPGroupCollection
Custom target systems	UNSGroupBCollection, UNSGroupB1Collection, UNSGroupB2Collection, UNSGroupB3Collection
Unix-based target system	UNXGroupExclusion
Azure Active Directory	AADGroupCollection
Exchange Online	O3EDLCollection
Google Workspace	GAPGroupCollection
Cloud target systems	CSMGroupCollection, CSMGroup1Collection, CSMGroup2Collection, CSMGroup3Collection

Special features for mapping object properties

In certain target systems, assignments of system entitlements to user accounts can have a limited duration.

- The validity period is not mapped in the Unified Namespace.
- The **Marked for deletion** (UNSAccountInUNSGroup.XMarkedForDeletion) identifier cannot be set for these assignments. Therefore, in the Unified Namespace, you cannot tell whether an assignment was marked as outstanding by synchronization.

One Identity Manager users for managing target systems in Unified Namespace

The following users are used for managing target systems in the Unified Namespace.

Table 9: 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 Unified Namespace application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Obtain view of the objects in the connected target systems across all target systems. • Can create reports across all target systems. <p>If the users are also target system managers of the basic underlying target systems, you can manage these target systems through the Unified Namespace.</p>
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.

Displaying Unified Namespace objects

NOTE: The object properties and assignments cannot be edited in the Unified Namespace. Use the **Show base object** task to change to the connected target system object. As target system administrator, you can edit the objects of your target system as usual.

To display Unified Namespace objects

- In the Manager, select the **Unified Namespace** category.

User accounts, system entitlements and structure elements of all the connected target systems are displayed hierarchically in the navigation view. This shows the main data and existing assignments of all objects. The object properties and assignments cannot be edited.

Reports about a target system in the Unified Namespace

One Identity Manager supplies various reports with information about a target system mapped in the Unified Namespace.

Table 10: 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	<p>This report shows an overview of the user accounts including its history.</p> <p>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.</p>
Show user accounts overview (incl. history)	Container	<p>This report shows all the container's user accounts with their permissions including a history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments</p>

Report	Published for	Description
		that were removed before this date, are not shown in the report.
Show system entitlements overview (incl. history)	Container	<p>This report shows the container's system entitlements with the assigned user accounts including a history.</p> <p>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.</p>
Overview of all assignments	Container	This report finds all roles containing employees with at least one user account in the selected container.
Overview of all assignments	System entitlement	This report finds all roles containing employees who have the selected system entitlement.
Show overview	System entitlement	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	System entitlement	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	System entitlement	<p>This report shows an overview of the system entitlement and including its history.</p> <p>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.</p>
Show historical memberships	System entitlement	<p>This report shows all employees that are assigned a user account from this system entitlement including the duration of the membership.</p> <p>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.</p>
Show entitlement drifts	Target system	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	Target	This report returns all the user accounts with

Report	Published for	Description
overview (incl. history)	system	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	Target system	This report contains all user accounts with an above average number of system entitlements.
Show employees with multiple user accounts	Target system	This report shows all the employees that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Target system	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	Target system	This report finds all roles containing employees with at least one user account in the selected target system.
Show unused user accounts	Target system	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Target system	This report shows all user accounts to which no employee is assigned.
Show user account operations	Target system	This report shows modified user accounts from all target systems for a specific time period.

Reports about all target systems in the Unified Namespace

One Identity Manager supplies various report with information about all the target systems mapped in the Unified Namespace. The data is combined and grouped by target system type.

Table 11: Data quality analysis report

Report	Description
Orphaned user accounts in all target systems	This report shows all user accounts to which no employee is assigned. You can find the report in the My One Identity Manager > Data quality analysis category.
Unused user accounts in all target systems	This report contains all user accounts, which have not been used in the last few months. You can find the report in the My One Identity Manager > Data quality analysis category.
System entitlement drifts in all target systems	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager. You can find the report in the My One Identity Manager > Data quality analysis category.
User accounts with an above average number of system entitlements	This report contains all user accounts with an above average number of system entitlements. You can find the report in the My One Identity Manager > Data quality analysis category.
Unified Namespace user account system entitlements distribution	The report shows an overview of the distribution of user accounts and system authorizations in Unified Namespace. You can find the report in the My One Identity Manager > Target system overviews category.
User account operations across all systems	This report shows modified user accounts from all target systems for a specific time period. You can find the report in the My One Identity Manager > Target system overviews category.

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 10, 18
 - IT operating data 10, 12, 14
 - manage level 10
- assignment
 - deletion flag 47
 - outstanding 47
 - validity period 47

E

- employee
 - account definition 10
 - assign automatically 21
 - central user account 16
 - change 17
 - default email address 17
 - delete 34, 36
 - general changes 17
 - job rotation 17
 - name change 17
 - permanently deactivate 33
 - temporarily deactivate 32
- employee assignment
 - automatic 21
 - change mapping 29
 - configure 22
 - criteria 24
 - custom script 29
 - manual 27
 - mode "CREATE" 22
 - mode "NO" 22

- mode "SEARCH AND CREATE" 22
- mode "SEARCH" 22
- remove 27
- search criteria 24
 - formatting 25
 - object type 25
 - table column 25

I

- IT operating data
 - account definition 10, 12, 14

S

- search criteria
 - employee assignment 24
- system entitlement
 - limited assignment 47

U

- Unified Namespace 41
 - objects
 - display 49
 - mapping 41
 - report 51
 - target system administrator 47
 - target system manager 47
- user account
 - account definition 10
 - assign employee (automatic) 21

- central 16
- full managed 7
- limited assignment 47
- linked 7
 - configured 7
- manage level 7
- state 7
- unlinked 7
- unmanaged 7