One Identity Manager 8.0.4

Target System Base Module Administration Guide

Legend

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

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

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

One Identity Manager Target System Base Module Administration Guide
Updated - September 2019
Version - 8.0.4

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 11
Determining valid IT Operating Data for the Target System 12
One Identity Manager Default Configuration IT Operating Data 13
Employee's Central User Account 15
Employee's Default Email Address 16
Changing Employee Master Data 16
Templates and Processes for Implementing Account Definitions 17
Example for Implementing Several Account Definitions with a Target System Type 18
Automatic Assignment of Employees to User Accounts 20
Configuring Automatic Employee Assignment 21
Editing Search Criteria for Automatic Employee Assignment 23
Modifying Scripts for Automatic Employee Assignment 28
Disabling and Deleting Employees and User Accounts 29
Temporarily Deactivating Employees 30
Permanently Deactivating Employees 31
Deferred Deletion of an Employee 32
Disabling and Deleting Account Definitions 32

The Unified Namespace **36**
Mapping Target System Objects in Unified Namespace 36
Special Features for Mapping Object Properties 42
One Identity Manager Users for Managing Target Systems in Unified Namespace 42
Displaying Unified Namespace Objects 43
Reports about the Unified Namespace 43

About us **45**
Contacting us 45
Technical support resources 45

Index **46**

1

Basic Mechanisms for Employee and User Account Administration

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

Because requirements vary between companies, the 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 the 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 the 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 IBM Notes

- All members of the sales department are automatically allocated an IBM Notes mailbox. Members of other departments can request an IBM Notes mailbox. The attributes of the IBM Notes 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 their 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 though 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, the user accounts are administrated independently of employee data.
- In domain B, the user accounts are linked to an employee. However, employee master data should not be transferred to the user accounts.
- In domain C, a user account should be 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

  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

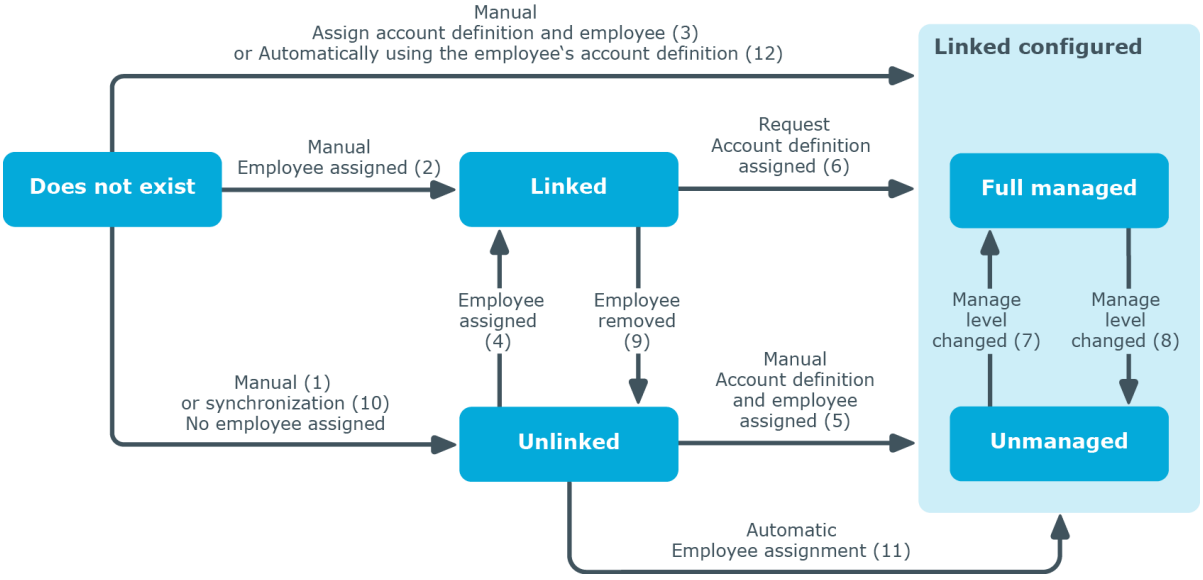
    The user accounts are assigned to an employee but do not inherit other properties from the employee.

- Full managed

  The user accounts are assigned to an employee and inherit the employee's properties.

The following visual is designed to make user account transitions clearer. The default mechanisms integrated in One Identity Manager about employee and user account administration are shown.

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, therefore, not linked to an employee and has the state "Unlinked".
- Case 2: If the user account is already manually linked to an employee , the user account goes into a "Linked" state.
- 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 enters the "Linked configured" state. The state "Linked configured: Unmanaged" or "Linked configured: Full managed" is attained depending on the manage level in use.

Editing an Existing User Account

- Case 4: If an existing user account is manually assigned to an employee, the state of the user account changes 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 state of the user account changes from "Unlinked" to "Linked configured". The state "Linked configured: Unmanaged"

or "Linked configured: Full managed" is attained depending on the manage level in use.

- Case 6: When the One Identity Manager goes live, you can create IT Shop requests for existing user accounts, which are linked with employees (state "linked"). This assigns an account definition and the user account enter the "Linked configured" state. The state "Linked configured: Unmanaged" or "Linked configured: Full managed" is attained depending on the manage level in use.

Changing the Manage Level

- Cases 7 and 8: By changing the manage level an existing user account can change from the state "Linked configured: Unmanaged" to the state "Linked configured: Full managed" and the reverse. 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, the state of the user accounts becomes "Unlinked".

NOTE: The employee entry cannot be removed from user accounts in the "Linked configured" state as long as the employee owns an account definition. Removing an employee's account definition results immediately in deleting the user accounts.

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 the "Unlinked" state. If the target system is assigned an account definition, this account definition is automatically assigned to the employees. The state "Linked configured: Unmanaged" or "Linked configured: Full managed" is attained depending on the manage level in use. 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 Automatic Assignment of Employees to User Accounts on page 20.

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 state "Linked configured". The state "Linked configured: Unmanaged" or "Linked configured: Full managed" is attained depending on the manage level in use. For more information, see Account Definitions and Manage Levels on page 10.

Using Account Definitions to Create User Accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not 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 data for the user accounts in the respective target system comes from the basic employee data. 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 (template processing). 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.

The One Identity Manager supplies a default configuration for manage levels:

- Unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other 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 a manage level of "Full managed" inherit specific properties from the assigned employee.

NOTE: The manage levels "Full managed" and "Unmanaged" are evaluated in the 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 determined 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 afterwards 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.

Assigning Account Definitions to Employees

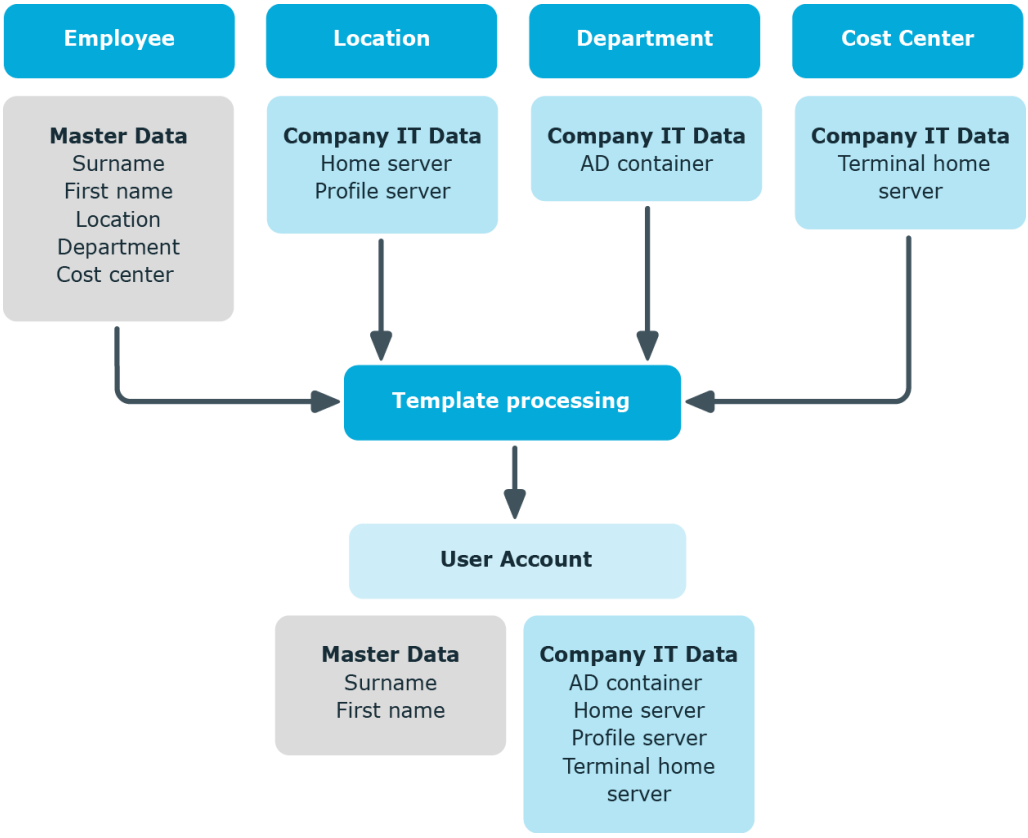
Account definitions are assigned to company employees. Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations or roles. The employees are categorized into these departments, cost centers, locations or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees. You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

Determining valid IT Operating Data for the Target System

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

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: Displaying IT Operating Data on Top of 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. Specify the property "Department" in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

One Identity Manager Default Configuration IT Operating Data

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

Target system type	IT Operating Data
LDAP	Container
	Groups can be inherited
	Identity
	Privileged user account
IBM Notes	Server
	Certificate
	Template for mail file
	Identity
SharePoint	Authentication mode
	Groups can be inherited
	Identity
	Privileged user account
SharePoint Online	Groups can be inherited
	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
	Identity
	Privileged user account
	Change password the next time you log in
Cloud target system	Container (per target system)
	Groups can be inherited
	Identity
	Privileged user account

Target system type	IT Operating Data
Unix-based target system	Login shell
	Groups can be inherited
	Identity
	Privileged user account
Exchange Online	Groups can be inherited
G Suite	Organizational unit
	Groups can be inherited
	Privileged user account
	Change password the next time you log in

Employee's Central User Account

Table 2: Configuration Parameter for Forming the Central User Accounts

Configuration Parameter	Meaning
QER\Person\CentralAccountGlobalUnique	This configuration parameter 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 the 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. The 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
Clara		CLARA
	Harris	HARRIS
Clara	Harris	CLARAH
Clara	Harrison	CLARAH1

Related Topics

- Employee's Default Email Address on page 16
- Changing Employee Master Data on page 16

Employee's Default Email Address

Table 4: Configuration parameter for the Default Email Address

Configuration parameter	Description
QER\Person\DefaultMailDomain	This configuration parameter contains the default mail domain. The value is used to establish an employee's email address.

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

The default mail domain is found in the configuration parameter "QER\Person\DefaultMailDomain".

- Set the configuration parameter in the Designer and enter the default mail domain name as a value.

Related Topics

- Employee's Central User Account on page 15
- Changing Employee Master Data on page 16

Changing Employee Master Data

In the following sections, we only examine the employee master data that affects the user account of an employee with the manage level "Full managed" when 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. With this, the company operations are automated in the One Identity Manager, with respect to the administrative tasks for alterations to the target system dependent IT operating data (for example, domains, home server or profile server). 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 15
- Employee's Default Email Address on page 16

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:

TSB_PersonHasTSBAccountDef_Autocreate_<user account table>

where:

<user account table> = table, in which user accounts are mapped;

for example:

ADSAccount (Active Directory user accounts)

ADSContact (Active Directory contacts)

EBSUser (Oracle E-Business Suite user accounts)

EX0Mailbox (Microsoft Exchange mailboxes)

EX0MailUser (Microsoft Exchange email address for user accounts)

EX0MailContact (Microsoft Exchange email address for contacts)

LDAPAccount (LDAP user accounts)

NotesUser (IBM Notes user accounts)

SAPUser (SAP R/3 user accounts)

SPSUser (SharePoint user accounts)

UNSAccountB (user accounts for custom target systems)

Example for Implementing Several Account Definitions with 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.

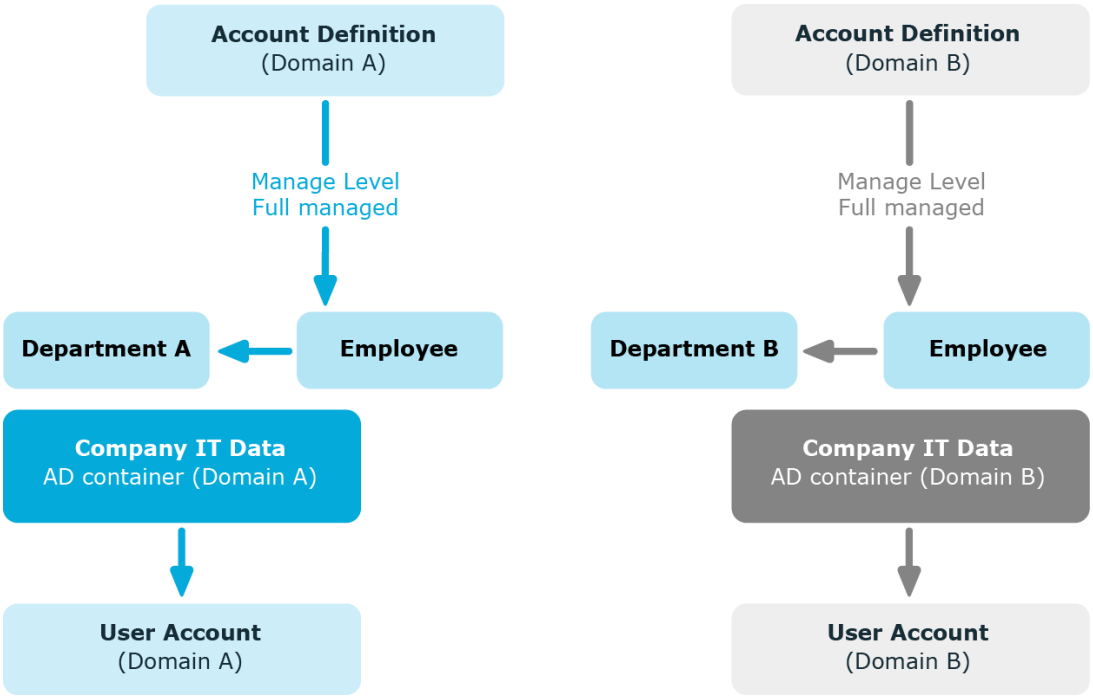
Example 1

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 manage level "Full managed". This manage level uses the One Identity Manager default templates to determine the IT operating data. Specify the property "department" for both account definitions in the IT operating data formatting rule for finding the valid IT operating data.

If the employee belongs to department A, they obtain (by dynamic assignment, for example) the account definition A and the resulting user account is in domain A. If the employee belongs to department B, they are issued the account definition B and a user account in domain B.

Figure 3: Creating User Accounts based on Account Definitions

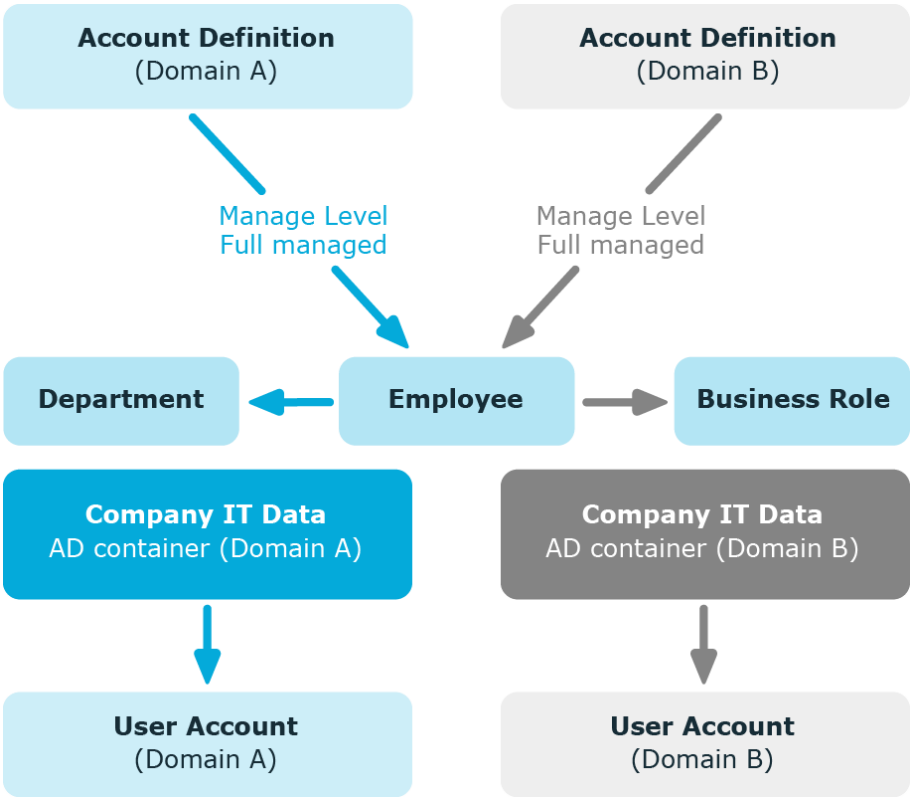


Example 2

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 manage level "Full managed". The manage level "Full Managed" uses One Identity Manager default templates to determine the IT operating data. Specify the property "department" for account definition A in the IT operating data formatting rule for finding the valid IT operating data. Specify the property "business role" for account definition B in the IT operating data formatting rule for finding the valid IT operating data.

Figure 4: Creating User Accounts based on Account Definitions



Automatic Assignment of Employees to User Accounts

Automatic employee assignment is used to:

- Assign existing employees to user accounts
- Create employee master 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. This method, however, 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.

- Set the configuration parameter for automatic assignment of employees to user accounts in the Designer and select the desired mode.
- Define search criteria for the employee assignment.
- If managed user accounts should arise through automatic employee assignment, assign an account definition to the target system. Ensure the manage level to be used is entered as default automation level.

  User accounts are only linked to the employee (state "Linked") if no account definition is given in the target system. 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 21
- Editing Search Criteria for Automatic Employee Assignment on page 23
- Modifying Scripts for Automatic Employee Assignment on page 28

Configuring Automatic Employee Assignment

In the One Identity Manager default installation, the automatic assignment of employees to user accounts is controlled by the configuration parameters shown below and is 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.

Table 5: Configuration Parameter for Automatic Employee Assignment

Target system type	Configuration parameter
Active Directory	TargetSystem\ADS\PersonAutoDefault
	TargetSystem\ADS\PersonAutoFullSync
LDAP	TargetSystem\LDAP\PersonAutoDefault
	TargetSystem\LDAP\PersonAutoFullSync
IBM Notes	TargetSystem\NDO\PersonAutoDefault
	TargetSystem\NDO\PersonAutoFullSsync
SAP R/3	TargetSystem\SAPR3\PersonAutoDefault
	TargetSystem\SAPR3\PersonAutoFullSync
SharePoint	TargetSystem\SharePoint\PersonAutoDefault
	TargetSystem\SharePoint\PersonAutoFullSync
Unix-Based Target Systems	TargetSystem\Unix\PersonAutoDefault
	TargetSystem\Unix\PersonAutoFullSync
Azure Active Directory	TargetSystem\AzureAD\PersonAutoDefault
	TargetSystem\AzureAD\PersonAutoFullsync

Each configuration parameter has one of the permitted modes:

- NO

  No automatic assignment of employees to user accounts takes place. This is the default value that is also displayed when the configuration parameter is not active.

- SEARCH

  If an employee is not assigned, the matching employee is searched for based on defined criteria, and the employee found is assigned to the user accounts. If an employee is not found, no new employee is added.

- CREATE

  If the user account is not assigned to an employee, a new employee is always added, some of the properties initialized, and the employee is assigned to the user account.

  NOTE: This mode is not available for the target system type SharePoint and Unix-based target systems.

- SEARCH AND CREATE

  If the user account does not have an employee assigned to it, a matching employee is searched for based on defined criteria and the employee that is found is assigned 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 the target system type SharePoint and Unix-based target systems.

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: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the target system at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the target system.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
    a. Select the category **Custom target systems | <target system> | User accounts | Linked but not configured | <target system>**.
    b. Select the task **Assign account definition to linked accounts**.

The configuration parameters are evaluated in the One Identity Manager default installation insert and update processes. These are target system dependent and thus determine the execution mode. The names of the corresponding processes 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

Criteria for employee assignment are defined in the target systems. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criteria are written in XML notation in the column "Search criteria for automatic employee assignment" (`AccountToPersonMatchingRule`) of 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: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

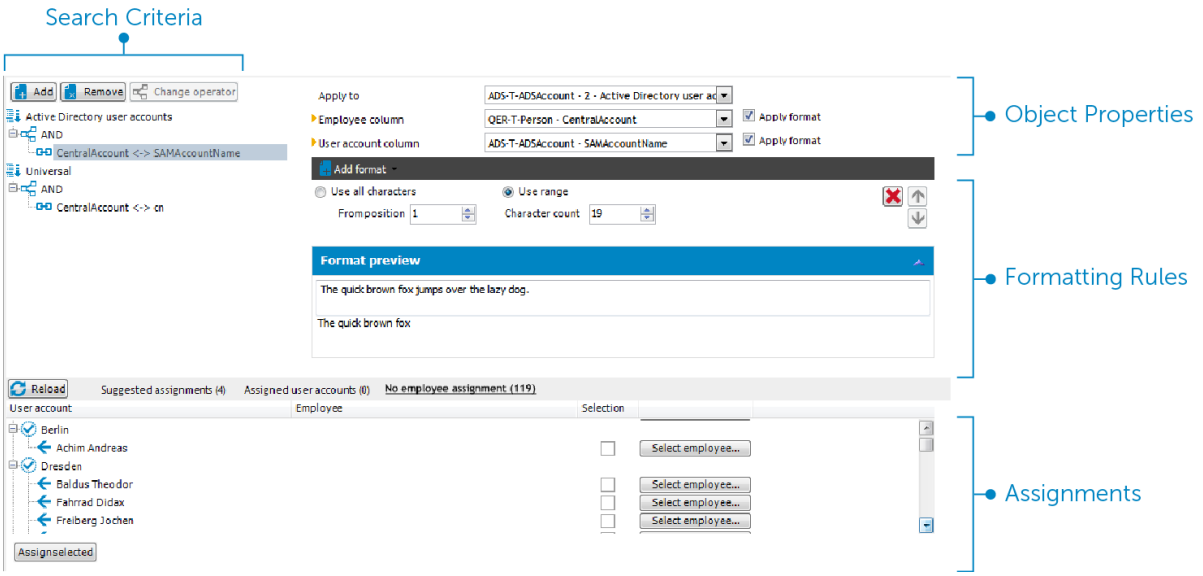
It is not recommended to make assignment to administrative user accounts based on search criteria. Use the task **Change master data** to assign employees to administrative user account for the respective user account.

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

To open the employee assignment form

1. Open the category **Target system type | <target system>**.
2. Select the target system in the result list.
3. Click **Define search criteria for employee assignment**.

Figure 5: Define Search Criteria for Employee Assignment



To define search criteria for employee assignment

1. Select the object type for the mapping.

   Object types are user accounts with certain properties, for example "Active Directory contacts" or "Disabled Notes user accounts".

   a. To add a new object type, click **Add | Criteria**. Select the object type for which to define the search criteria using the **Apply to** menu.

      The search criteria is applied to all user accounts if no object type is selected.

b. To change the object type on an existing search criteria, mark the search criteria in "Search criteria". Select the object type for which to define the search criteria using the **Apply to** menu.

   If the existing selection is removed, the search criteria is applied to all user accounts.

2. Select the object properties to map.
   - Employee column

     Select the column in the Person table on which to run the search.
   - User account column

     Select the column in the user account table which return the value for the employee search.
3. Define the formatting rule to limit the search criteria.

   Select a formatting rule in the **Add format** menu. Define the formatting rule to apply to the search string. You can combine different format templates.

   Table 6: Format Templates

Format template	Meaning
Character range	Characters in the search string to be used in the search criteria.
Crop to fixed length	Length of the search string. Use fill characters at the beginning or end of the string to ensure it reaches the fixed length.
Remove leading or trailing characters	Characters to be removed at the beginning or the end of the string. The remaining string forms the search criteria.
Split value	Characters defining the place to split the string and which part of string should be used as search criteria.

4. Test the format rules.

   Enter a string "Format preview" to which to apply the search. Use this to test the effects of your search criteria formatting.
5. Apply the formatting rules.

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

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

Example for AND

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 for an OR operation.

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. Mark the operator to which to add another object property in "Search criteria". 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.

Direct Assignment of Employees to User Accounts Based on a Suggestion List

You can create a suggestion list in the "Assignments" view for assignments of employees to user accounts based on the search criteria. User accounts are grouped in different views for this.

Table 7: 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.

View	Description
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.

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

To apply search criteria to user accounts

- 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.

To assign employees directly over a suggestion list

1. Click **Suggested assignments**.
   a. Click **Select** for all user accounts to be assigned to the suggested employee. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

      The selected user accounts are assigned to the employees found using the search criteria.

   – OR –
2. Click **No employee assignment**.
   a. Click **Select employee...** for the user account to which you want to assign the employee. Select an employee from the menu.
   b. Click **Select** for all user accounts to which you want to assign the selected employees. Multi-select is possible.
   c. Click **Assign selected**.
   d. Confirm the security prompt with **Yes**.

      This assigns the selected user accounts to the employees shown in the "Employee" column.

To remove assignments

1. Click **Assigned user accounts**.
   a. Click **Select** for all user accounts whose employee assignment you want to remove. Multi-select is possible.
   b. Click **Delete selected**.
   c. Confirm the security prompt with **Yes**.

      The assigned employees are deleted from the selected user accounts.

Modifying Scripts for Automatic Employee Assignment

Automatic employee assignments are controlled through scripts. These scripts, in 'SEARCH' mode, assign existing employees to user accounts depending on defined search criteria. Furthermore, the scripts, in 'CREATE' mode, define properties which are initialized when a new employee is created. 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.

When automatic employee assignment is carried out in "CREATE" mode, some of the properties of the user account are passed on to the new employee object. Initializing the employee properties is done using the script "VI_PersonAuto_<targetsystem>". 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 changes, too. 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 Version of the 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
...
```

Disabling 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 disable them when they leave the company. Other firms delete the employee, but only after they have ensured that all the user accounts are removed.

How employees are handled when they are disabled or deleted depends on the type of user account management. The following scenarios apply:

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

The following methods are available in the One Identity Manager standard version:

- Temporarily Deactivating Employees
- Permanently Deactivating Employees
- Deferred Deletion of an Employee
- Disabling and Deleting Account Definitions

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

NOTE: Configure and enable the schedule "Lock accounts of employees that have left the company" in the Designer. This schedule checks the start date for disabling and sets the option **Temporarily disabled** when it is reached.

NOTE: Configure and enable the schedule "Enable temporarily disabled accounts" in the Designer. 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 disabling of an employee affects the user account.

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

- Specify which behavior you require with configuration parameter "QER\Person\TemporaryDeactivation". If the configuration parameter is set, the employee's user accounts are locked if the employee is permanently or temporarily disabled. If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

Related Topics

- Disabling and Deleting Account Definitions on page 32

Permanently Deactivating Employees

Employees can be disabled 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 disabling of an employee 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 option **No inheritance** is set for an employee.
- Employee user accounts are locked or deleted and then removed from group memberships.

Trigger permanent deactivation through:

- The task **Disable employee permanently**

  This task ensures that the option **Permanently disabled** is set and leaving date and the last day of work are set to the current date.

- Leave date reached

  NOTE: : Configure and enable the schedule "Lock accounts of employees that have left the company" in the Designer. This schedule regularly checks the leaving date and sets the option **Permanently disabled** on reaching the date.

  NOTE: The task **Re-enable employee** ensures that the employee is re-enabled.

- Certification status "Denied"

  An employee is permanently deactivated when their certification status is set to "Denied" either through attestation or manually. If the employee's certification status is changed to "certified", the employee is activated again.

  NOTE: This function is 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 temporary disabling of an employee affects the user account.

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

- Specify which behavior you require with configuration parameter "QER\Person\TemporaryDeactivation". If the configuration parameter is set, the employee's user accounts are locked if the employee is permanently or temporarily disabled. If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

Related Topics

- Disabling and Deleting Account Definitions on page 32

Deferred Deletion of an Employee

When an employee is deleted, they are tested to see if user accounts and company resources are still assigned, or if there are still pending requests in the IT Shop. The employee is marked for deletion and therefore locked out of further processing. 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 one employee could be deleted by default by the 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 deletion of an employee affects their user accounts. The user accounts can be locked or enabled for the period that deletion is deferred. In any case, the user accounts are deleted from the One Identity Manager database once the deferred deletion period has expired.

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.

Related Topics

- Disabling and Deleting Account Definitions on page 32

Disabling and Deleting 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.

You can configure the following behavior:

1. How employees inherit account definitions

   The effects on account definition assignment 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: An employee keeps its linked user accounts as long as an account definition applies to the employee. 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 8: Account Definition Master Data for Account Definition Assignment Behavior

Property	Description
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.

Property	Description
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.

2. Handling employee user accounts

   The effects on user accounts of temporary disabling, permanent disabling, 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 disabled 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 9: Manage Level Master Data for Handling User Accounts

Property	Description
Lock user accounts if temporarily disabled	Specifies whether user accounts of permanently disabled employees are locked.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled 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.

3. Inheritance of group memberships by the employee's user accounts

   The effects on user account group memberships of temporary disabling, permanent disabling, 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 10: Manage Level Master Data for Handling Group Memberships

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

2

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

Mapping Target System Objects in Unified Namespace

Each Unified Namespace object type joins the various tables of the One Identity Manager data model 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 execute 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

Target system type	Table
IBM Notes	NotesDomain
SAP R/3	SAPMandant
LDAP	LDPDomain
Custom target systems	UNSRootB
Unix	UNXHost
Azure Active Directory	AADOrganization
G Suite	GAPCustomer
Cloud Target Systems	CSMRoot
Oracle E-Business Suite	EBSSystem

Container (`UNSContainer`)

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

Target system type	Table
Active Directory	ADSContainer
SharePoint	SPSWeb
LDAP	LDAPContainer
Custom target systems	UNSContainerB
Cloud Target Systems	CSMContainer
G Suite	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
IBM Notes	NotesUser
SAP R/3	SAPUser, SAPBWUser

Target system type	Table
LDAP	LDAPAccount
Custom target systems	UNSAccounB
Unix	UNXAccount
Azure Active Directory	AADUser
Exchange Online	O3EMailbox, O3EMailContact, O3EMailUser
G Suite	GAPUser
Cloud Target Systems	CSMUser
Oracle E-Business Suite	EBSUser

System entitlements (UNSGroup)

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

Target system type	Table
Active Directory	ADSGroup
Microsoft Exchange	EX0DL
SharePoint	SPSGroup, SPSRLAsgn
IBM Notes	NotesGroup
SAP R/3	SAPGrp, SAPProfile, SAPRole, SAPHRP, SAPBWP
LDAP	LDAPGroup
Custom target systems	UNSGroupB
Unix	UNXGroup
Azure Active Directory	AADGroup, AADDeniedServicePlan, AADDirectoryRole, AADSubSku
Exchange Online	O3EDL, O3EUnifiedGroup
G Suite	GAPGroup, GAPPaSku
Cloud Target Systems	CSMGroup
Oracle E-Business Suite	EBSResp

Permissions controls (UNSItem)

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

Target system type	Table
Custom target systems	UNSItemB
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
IBM Notes	NotesUserInGroup
SAP R/3	SAPUserInSAPGrp, HelperSAPUserInSAPRole, SAPUserInSAPProfile, SAPUserInSAPHRP, SAPBWUserInSAPBWP
LDAP	LDAPAccountInLDAPGroup
Custom target systems	UNSAccounBInUNSGroupB
Unix	UNXAccountInUNXGroup
Azure Active Directory	AADUserHasDeniedService, AADUserInDirectoryRole, AADUserInAADGroup
Exchange Online	O3EAADUserInUnifiedGroup, O3EMailboxInDL, O3EMailContactInDL, O3EMailUserInDL
G Suite	GAPUserInGroup, GAPUserInPaSku
Cloud Target Systems	CSMUserInGroup
Oracle E-Business Suite	EBSUserInRespCompressed

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
IBM Notes	NotesGroupInGroup
SAP R/3	SAPProfileInSAPProfile, SAPRoleInSAPRole, SAPProfileInSAPRole
LDAP	LDAPGroupInLDAPGroup
Custom target systems	UNSGroupBInUNSGroupB
Azure Active Directory	AADGroupInGroup,
Exchange Online	O3EDLInDL
G Suite	GAPGroupInGroup
Cloud Target Systems	CSMGroupInGroup

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
IBM Notes	NotesGroupExclusion
SAP R/3	SAPGrpExclusion, SAPProfileExclusion, SAPRoleExclusion
LDAP	LDAPGroupExclusion
Custom target systems	UNSGroupBExclusion
Unix	UNXGroupExclusion
Azure Active Directory	AADGroupExclusion, AADSubSkuExclusion
G Suite	GAPGroupExclusion
Cloud Target Systems	CSMGroupExclusion
Oracle E-Business Suite	EBSRespExclusion

System entitlement hierarchy (`UNSGroupCollection`)

The `UNSGroupCollection` view maps hierarchies of system entitlements.

Target system type	Table
Active Directory	ADSGroupCollection
SharePoint	SPSGroupCollection,SPSRLAsgn
IBM Notes	NotesGroupCollection
SAP R/3	SAPCollectionRPG
LDAP	LDAPGroupCollection
Custom target systems	UNSGroupBCollection
Unix based target system	UNXGroupExclusion
Azure Active Directory	AADGroupCollection
Exchange Online	O3EDLCollection
G Suite	GAPGroupCollection
Cloud Target Systems	CSMGroupCollection

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" option (`UNSAccountInUNSGroup.XMarkedForDeletion`) cannot be set for this assignment. 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 11: Users

User	Task
Target system administrators	Target system administrators must be assigned to the application role **Target system | Administrators**. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the application role **Target systems | Unified Namespace** or a sub application role. Users with this application role: • Obtain view of the objects in the connected target systems across

User	Task
	all target systems. • Can create reports across all target systems. If the users are also target system managers of the basic underlying target systems, you can manage these target systems through the Unified Namespace.
One Identity Manager administrators	• 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, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.

Displaying Unified Namespace Objects

To display Unified Namespace objects

- Select the category **Unified Namespace**.

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

  NOTE: The object properties and assignments cannot be edited in the Unified Namespace.

  Use the task **Show base object** to change to the connected target system object. As target system administrator, you can edit the objects in your target system as usual.

Reports about the Unified Namespace

The 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 12: 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 category **My One Identity Manager | Data quality analysis**.
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 category **My One Identity Manager | Data quality analysis**.
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 using the One Identity Manager provisioning engine. You can find the report in the category **My One Identity Manager | Data quality analysis**.
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 category **My One Identity Manager | Data quality analysis**.
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 category **My One Identity Manager | Target system overviews**.
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 category **My One Identity Manager | Target system overviews**.

About us

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

Contacting us

For sales or other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

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

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

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

Index

A

account definition 10, 17
- IT operating data 10, 12-13
- manage level 10

assignment
- deletion flag 42
- outstanding 42
- validity period 42

E

employee
- account definition 10
- assign automatically 20
- central user account 15
- change 16
- default email address 16
- delete 32
- general changes 16
- job rotation 16
- name change 16
- permanently disabled 31
- reenable 31
- temporarily disabled 30

employee assignment
- automatic 20
- change mapping 28
- configure 21
- criteria 23
- custom script 28
- manual 26
- mode "CREATE" 21
- mode "NO" 21
- mode "SEARCH AND CREATE" 21
- mode "SEARCH" 21
- remove 26
- search criteria 23
  - formatting 23
  - object type 23
  - table column 23

I

IT operating data
- account definition 10, 12-13

S

search criteria
- employee assignment 23

system entitlement
- limited assignment 42

U

Unified Namespace 36
- objects
  - display 43
  - mapping 36
- report 43
- target system administrator 42
- target system manager 42

user account
- account definition 10

assign employee (automatic) 20
central 15
full managed 7
limited assignment 42
linked 7
    configured 7
manage level 7
state 7
unlinked 7
unmanaged 7