



One Identity Manager 8.0.2

Administration Guide for Connecting to LDAP

Copyright 2018 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. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

One Identity Manager Administration Guide for Connecting to LDAP
Updated - September 2018
Version - 8.0.2

Contents

Managing LDAP Environments	7
Architecture Overview	7
One Identity Manager Users for Managing an LDAP	8
Setting up LDAP Directory Synchronization	11
Users and Permissions for Synchronizing with LDAP	12
Special Cases for synchronizing Active Directory Lightweight Directory Services	13
Setting Up the Synchronization Server	14
Creating a Synchronization Project for initial Synchronization of an LDAP Domain	18
Show Synchronization Results	29
Customizing Synchronization Configuration	30
Configuring Synchronization in LDAP Domains	31
Configuring Synchronization of Several LDAP Domains	31
Updating Schemas	32
Speeding Up Synchronization with Revision Filtering	33
Post-Processing Outstanding Objects	34
Configuring Memberships Provisioning	36
Help for Analyzing Synchronization Issues	37
Deactivating Synchronization	37
Basic Configuration Data	39
Setting Up Account Definitions	40
Creating an Account Definition	41
Master Data for an Account Definition	41
Setting Up Manage Levels	43
Master Data for a Manage Level	45
Creating a Formatting Rule for IT Operating Data	46
Determining IT Operating Data	47
Modifying IT Operating Data	49
Assigning Account Definitions to Employees	50
Assigning Account Definitions to Departments, Cost Centers and Locations	51
Assigning Account Definitions to Business Roles	51
Assigning Account Definitions to all Employees	52

Assigning Account Definitions Directly to Employees	53
Assigning Account Definitions to System Roles	53
Adding Account Definitions in the IT Shop	54
Assigning Account Definitions to a Target System	55
Deleting an Account Definition	56
Password Policies	57
Predefined Password Policies	58
Editing Password Policies	59
General Master Data for a Password Policy	59
Policy Settings	60
Character Sets for Passwords	60
Custom Scripts for Password Requirements	61
Script for Checking a Password	61
Script for Generating a Password	63
Restricted Passwords	64
Testing a Password	64
Testing Generating a Password	64
Assigning a Password Policy	65
Initial Password for New LDAP User Accounts	66
Email Notifications about Login Data	68
Target System Managers	70
LDAP Domains	73
General Master Data for an LDAP Domain	73
LDAP Specific Master Data for an LDAP Domain	75
Specifying Categories for Inheriting LDAP Groups	76
How to Edit a Synchronization Project	76
LDAP User Accounts	78
Linking User Accounts to Employees	78
Supported User Account Types	79
Entering Master Data for LDAP User Accounts	82
General Master Data for an LDAP User Account	83
Contact Data for an LDAP User Account	87
Address Information for an LDAP User Account	87
Organizational Data for an LDAP User Account	88

Miscellaneous Data for an LDAP User Account	89
Additional Tasks for Managing LDAP User Accounts	89
Overview of LDAP User Accounts	90
Changing the Manage Level of an LDAP User Account	90
Assigning LDAP Groups Directly to LDAP User Accounts	90
Assign Extended Properties to an LDAP User Account	91
Automatic Assignment of Employees to LDAP User Accounts	92
Editing Search Criteria for Automatic Employee Assignment	94
Disabling LDAP User Accounts	96
Deleting and Restoring LDAP User Accounts	97
LDAP Groups	99
LDAP Group Master Data	99
Assigning LDAP Groups to LDAP User Accounts and LDAP Computers	101
Assigning LDAP Groups to Departments, Cost Centers and Locations	102
Assigning LDAP Groups to Business Roles	103
Assigning LDAP User Accounts directly to an LDAP Group	104
Assigning LDAP Computers Directly to an LDAP Group	105
Adding LDAP Groups to System Roles	105
Adding LDAP Groups to the IT Shop	106
Additional Tasks for Managing LDAP Groups	108
Overview of LDAP Groups	108
Effectiveness of Group Memberships	108
LDAP Group Inheritance Based on Categories	110
Assigning Extended Properties to an LDAP Group	113
Deleting LDAP Groups	113
LDAP Container Structures	114
General Master Data for LDAP Containers	114
Contact Data for LDAP Containers	116
Address Information for LDAP Containers	116
LDAP Computers	118
Master Data for an LDAP Computer	118
Assigning LDAP Computers directly to LDAP Groups	119
Reports about LDAP Objects	120
Overview of all Assignments	121

Appendix: Configuration Parameters for Managing LDAP	123
Appendix: Default Project Template for LDAP	127
OpenDJ Basic Template	127
Default Project Template for Active Directory Lightweight Directory Services	128
Appendix: Authentication Modules for Logging into the One Identity Manager	129
About us	133
Contacting us	133
Technical support resources	133
Index	134

Managing LDAP Environments

The One Identity Manager allows administration of objects, such as employees, groups and organizational units that are managed in an LDAP directory. The LDAP structure in the One Identity Manager should be seen as a suggestion and seldom corresponds to the property structure in a customer specific LDAP directory. Whether or how the available properties will be used depends on the respective LDAP schema which is in use and must be custom configured.

The default One Identity Manager installation is concerned with employee administration and their user accounts, user groups and LDAP directory organizational units. The One Identity Manager data model is designed to manage administration of LDAP directory computers and servers.

One Identity Manager supplies templates for synchronizing with several server systems. However, the synchronization connection has to be custom configured in any case.

Company employees are provided with the necessary user accounts in the One Identity Manager. Different mechanisms can be used to link employees to their user accounts. These user accounts can also be managed separately from employees and therefore administrative user accounts can be set up. In order to provide the required permissions, LDAP groups are managed in the One Identity Manager. In One Identity Manager you can also manage organizational units in a hierarchical structure. Organizational units (branches or departments) are used to logically organize the objects in an LDAP directory such as user accounts and groups and thus make administration easier.

Architecture Overview

The following servers are used for managing an LDAP system in One Identity Manager:

- LDAP Server
LDAP server for keeping the LDAP directory. This server is a selected live server with a good network connection to the synchronization server. The synchronization server connects to this server in order to access LDAP objects.
- Synchronization server

The synchronization server for synchronizing the One Identity Manager database with the LDAP system. The One Identity Manager Service is installed on this server with the LDAP connector. The synchronization server connects to the LDAP server.

The LDAP connector is used for synchronization and provisioning LDAP. The LDAP connector communicates directly with an LDAP server.

Figure 1: Architecture for synchronization



One Identity Manager Users for Managing an LDAP

The following users are used for setting up and administration of an LDAP system.

Table 1: User

User	Task
Target system administrators	<p>Target system administrators must be assigned to the application role Target system Administrators.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • 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	Target system managers must be assigned to the application

User	Task
managers	<p>role Target systems LDAP or a sub application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	<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, 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.
Administrators for the IT Shop	<p>Administrators must be assigned to the application role Request & Fulfillment IT Shop Administrators.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to IT Shop structures.
Administrators for organizations	<p>Administrators must be assigned to the application role Identity Management Organizations Administrators.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to departments, cost centers and locations.
Business roles administrators	<p>Administrators must be assigned to the application role Identity Management Business roles Administrators.</p>

User**Task**

Users with this application role:

- Assign groups to business roles.

Setting up LDAP Directory Synchronization

One Identity Manager supports synchronization of LDAP version 3 conform directory servers.

NOTE: Other schema and provisioning process adjustments can be made depending on the schema.

To load LDAP objects into the One Identity Manager database

1. Prepare a user account with sufficient permissions for synchronization.
2. The One Identity Manager parts for managing LDAP systems are available if the configuration parameter "TargetSystem\LDAP" is set.
 - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
 - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Users and Permissions for Synchronizing with LDAP](#) on page 12
- [Setting Up the Synchronization Server](#) on page 14
- [Creating a Synchronization Project for initial Synchronization of an LDAP Domain](#) on page 18
- [Deactivating Synchronization](#) on page 37
- [Customizing Synchronization Configuration](#) on page 30
- [Appendix: Configuration Parameters for Managing LDAP](#) on page 123
- [Appendix: Default Project Template for LDAP](#) on page 127

Users and Permissions for Synchronizing with LDAP

The following users are involved in synchronizing One Identity Manager with LDAP.

Table 2: Users for Synchronization

User	Permissions
User for accessing the LDAP directory	A reasonable minimal configuration for the synchronization user account cannot be recommended because the permissions depend which on the LDAP directory service is implemented. For more information about which permissions are required, see your LDAP directory service documentation.
One Identity Manager Service user account	<p>The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited).</p> <p>The user account must belong to the group "Domain Users".</p> <p>The user account must have the extended access right "Log on as a service".</p> <p>The user account requires access rights to the internal web service.</p> <p>i NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.</p> <p>In the default installation the One Identity Manager is installed under:</p> <ul style="list-style-type: none">• %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)• %ProgramFiles%\One Identity (on 64-bit operating systems)
User for accessing the One Identity Manager database	The default system user "Synchronization" is available to run synchronization over an application server.

Special Cases for synchronizing Active Directory Lightweight Directory Services

There are various special cases to take into account when setting up a synchronization project for Active Directory Lightweight Directory Services (AD LDS).

AD LDS supports different authentication methods. For more detailed information about AD LDS, see the [Microsoft TechNet Library](#).

Different settings arise, which need to be considered when setting up the synchronization project, depending on the authentication method you choose.

Authentication with AD LDS Security Principal

For this authentication method, you use a user account that is in AD LDS.

- The user account must be a member in the group "Administrators" of the AD LDS instance.
- The user account must have a password.

If it does not have a password, authentication is anonymous. This causes the schema to load incorrectly and the synchronization project set up fails.

Take note of the following for setting up your synchronization project.

- Authentication must use SSL encryption.
- "Basic" must be used as authentication method.
- Enter the distinguished LDAP name (DN) with the user account's user name for logging in to AD LDS.

Syntax example: `CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd`

Authentication with Windows Security Principal

Use a user account for authentication which resides on a local computer or in an Active Directory domain.

- The user account must be a member in the group "Administrators" of the AD LDS instance.

Take note of the following for setting up your synchronization project.

- "Negotiate" must be used as authentication method.
- If SSL encoding is not being used, sealing and signing authentication modes must be enabled.
- If SSL encoding is being used, sealing and signing authentication modes should not be enabled.
- Enter the user principal name with the user account's user name for logging in to AD

LDS.

Syntax example: Administrator@Doku.Testlab.dd

Authentication with AD LDS Proxy Object

Use a user account for authentication which exists in AD LDS and serves as binding for a local user account or a user account in an Active Directory domain. The local user account or the Active Directory user account is referenced in AD LDS as security ID (SID).

- The user account (AD LDS proxy object) must be a member in the group "Administrators" of the AD LDS instance.

Take note of the following for setting up your synchronization project.

- Authentication must use SSL encryption.
- "Basic" must be used as authentication method.
- Use the AD LDS proxy object user name for the AD LDS login.
- Enter the distinguished LDAP name (DN) with the user name.
Syntax example: CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd
- The user account password referenced by the AD LDS proxy object is to be used as login password.

Setting Up the Synchronization Server

To set up synchronization with an LDAP environment a server has to be available that has the following software installed on it:

- Windows operating system
Following versions are supported:
 - Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later
 - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 or later
 - ① | **NOTE:** Microsoft .NET Framework version 4.6.0 is not supported.
 - ① | **NOTE:** Take the target system manufacturer's recommendations into account.
- Windows Installer

- One Identity Manager Service, LDAP connector
 - Install One Identity Manager components with the installation wizard.
 1. Select the option **Select installation modules with existing database.**
 2. Select the machine role **Server | Job Server | LDAP directories.**

All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database, are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

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

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

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

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

1. Start the program Server Installer on your administrative workstation.
2. Enter valid data for connecting to One Identity Manager on the **Database connection** page and click **Next**.
3. Specify on which server you want to install the One Identity Manager Service on the **Server properties** page.
 - a. Select a job server in the **Server** menu.
 - OR -
 - Click **Add** to add a new job server.

- b. Enter the following data for the Job server.

Table 3: Job Servers Properties

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

NOTE: Use the **Advanced** option to edit other Job server properties. You can use the Designer to change properties at a later date.

- Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.
Select at least the following roles:
 - LDAP directories
- Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.
The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.
Select the following server functions:
 - LDAP connector
- Check the One Identity Manager Service configuration on the **Service settings** page.
 - NOTE:** The initial service configuration is already predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more detailed information about configuring the service, see One Identity Manager Configuration Guide.
- To configure remote installations, click **Next**.
- Confirm the security prompt with **Yes**.
- Select the directory with the install files on the **Select installation source** page.
- Select the file with the private key on the page **Select private key file**.
 - NOTE:** This page is only displayed when the database is encrypted.

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

Table 4: Installation Data

Data	Description
Computer	<p>Server on which to install and start the service from.</p> <p>To select a server</p> <ul style="list-style-type: none"> Enter the server name. - OR - Select a entry from the list.
Service account	<p>One Identity Manager Service user account data.</p> <p>To enter a user account for the One Identity Manager Service</p> <ul style="list-style-type: none"> Set the option Local system account. This starts the One Identity Manager Service under the account "NT AUTHORITY\SYSTEM". - OR - Enter user account, password and password confirmation.
Installation account	<p>Data for the administrative user account to install the service.</p> <p>To enter an administrative user account for installation</p> <ul style="list-style-type: none"> Enable Advanced. Enable the option Current user. This uses the user account of the current user. - OR - Enter user account, password and password confirmation.

- Click **Next** to start installing the service.
Installation of the service occurs automatically and may take some time.
- Click **Finish** on the last page of the Server Installer.

1 | **NOTE:** The is entered with the name "One Identity Manager Service" in the server's service administration.

Creating a Synchronization Project for initial Synchronization of an LDAP Domain

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and LDAP. The following describes the steps for initial configuration of a synchronization project.

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

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

Table 5: Information Required for Setting up a Synchronization Project

Data	Explanation
LDAP server's DNS name	Full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects. Example: <code>Server.Doku.Testlab.dd</code>
Authentication type	You can only connect to a target system if the correct type of authentication is selected. Authentication type "Basic" is taken as default. For more information about authentication types, see the MSDN Library .
Communications port on the domain controller	LDAP default communications port is 389.
User account and password for domain login	User account and password for domain login. This user account is used to access the domain. Make a user account available with sufficient permissions. For more information, see Users and Permissions for Synchronizing with LDAP on page 12.
Synchronization server for LDAP	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database, are processed by the synchronization server. The One Identity Manager Service with the LDAP connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One

Data	Explanation
	Identity Manager. Use the following properties when you set up the Job server.

Table 6: Additional Properties for the Job Server

Property	value
Server Function	LDAP connector
Machine role	Server/Job Server/LDAP directories

For more information, see [Setting Up the Synchronization Server](#) on page 14.

One Identity Manager Database Connection Data	<p>SQL Server:</p> <ul style="list-style-type: none"> • Database server • Database • Database user and password • Specifies whether Windows authentication is used. <p>This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p> <p>Oracle:</p> <ul style="list-style-type: none"> • Species whether access is direct or through the Oracle client Which connection data is required, depends on how this option is set. • Database server • Oracle instance port • Service name • Oracle database user and password • Data source (TNS alias name from <code>TNSNames.ora</code>)
---	--

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

Data

Explanation

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

Remote connection server configuration:

- One Identity Manager Service is started
- RemoteConnectPlugin is installed
- LDAP connector is installed

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

TIP: The remote connection server requires the same configuration (with respect to the installed software) as the synchronization server. Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well.

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

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

- In default mode
- Started from the launchpad

Additional settings can be made if the project wizard is run in expert mode or is started directly from the Synchronization Editor. Follow the project wizard instructions through these steps.

To set up initial synchronization project for an LDAP domain.

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

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

2. Select the entry **LDAP target system type**. Click **Run**.

This starts the Synchronization Editor's project wizard.

3. Specify how the One Identity Manager can access the target system on the **System access** page.

- If you have access from the workstation from which you started the Synchronization Editor, do not set anything.
- If you do not have access from the workstation from which you started the Synchronization Editor, you can set up a remote connection.

In this case, set the option **Connect using remote connection server** and select, under **Job server**, the server you want to use for the connection.

4. Specify settings for the wizard using the option **Expert mode (Configure advanced settings)** on the wizard's start page.
 - If you use a default project template, disable this option. The default templates automatically find which settings to use.
 - Set the option for custom modified LDAP environments. You can set the following options for this case:
 - Definition of virtual classes for RFC non-compliant object mappings
 - Definition of auxiliary classes of type "Auxiliary"
 - Definition of system attributes for object identification, revision attributes and additional functional attributes
 - Definition of other attributes for supporting dynamic groups
5. Enter network settings for connecting to the LDAP server on the **Network** page.
 - Enter the connection to the LDAP server under **Host**.

Table 7: LDAP Server Connection Data

Property	Description
Server	Full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects. Example: Server.Doku.Testlab.dd
Port	Communications port on the Server. LDAP default communications port is 389.

- Click **Test connection**. The system tries to connect to the server.
- Enter additional LDAP server communication settings under **Additional settings**.

Table 8: Additional Connection Settings

Property	Description
Protocol version	Version of the LDAP protocol.
No encryption	Specifies that no encryption is used.
SSL/TLS encryption	Specifies whether a SSL/TLS encrypted connection is established.
Use StartTLS	Specifies whether StartTLS is used.

6. Enter authentication data on the **Authentication** page.
 - Select the authentication type for logging into the system under **Authentication**.
 - Other information may be required depending on the selected authentication method. Enter this information under **Credentials**.

Table 9: Credentials

Property	Description
User name	Name of the user account for logging on to LDAP.
Password	User account password.
Enable sealing	Specifies whether sealing is enabled. Set this option if the selected authentication method supports sealing.
Enable signing	Specifies whether signing is enabled. Set this option if the selected authentication method supports signing.

- You can verify the connection data under **LDAP verify connection**. Click **Test**. The system tries to log on to the server.
7. Information about the LDAP schema are displayed on the **LDAP server information** page.
 8. Defined additional virtual classes on the **Virtual classes** page.

NOTE: This step is only displayed if you have set the option **Expert mode** for the system connection wizard.

Object containing several structural classes can only be created in LDAP systems which are not RFC compliant. They consist of one or more different classes, which are not derived from each other, for example, "OrganisationalUnit" and "inetOrgPerson".

To map these objects

- Enter the virtual class name in **Configured virtual classes**.
 - Select structural classes for mapping the virtual classes in **Select structural classes**.
9. Specify search parameters for finding LDAP objects to be loaded, on the **Search options** page.

Table 10: Search Options

Property	Description
Base DN	Base entry (normally the domain) for synchronization.
Cache LDAP schema locally	Specifies whether LDAP schema is kept in cache. This accelerates synchronization and provisioning of LDAP objects. The cache is on the connected computer under %Appdata%\...\Local\One Identity\One Identity Manager\Cache\GenericLdapConnector\<ConnectionInternalKey>\<Hash>\<Hash>.Cache
Request timeout (seconds)	Timeout for requests in seconds.
Use paged search	Specifies whether LDAP objects are listed a page at a time. If you set this option, you include the page size.
Page size	Maximum number of objects per page.

10. Enter which type of write operations are support by the LDAP server on the **Modification capabilities** page.
 - Set the option **Server supports renaming of entries** if the LDAP server supports renaming of objects.
 - Set the option **Server supports moving of entries** if the LDAP server supports moving of objects.

i **NOTE:** Some servers only support object renaming at leaf level. In this case, renaming other nodes fails with an error message.

11. Assign additional auxiliary classes to structural classes on the **Assign auxiliary classes** page.

i **NOTE:** This step is only displayed if you have set the option **Expert mode** for the system connection wizard.

Auxiliary classes are classes of type "Auxiliary" and contain attributes for extending structural classes. Auxiliary class attributes are offered as optional attributes for structural classes in the schema.

i **NOTE:** You may have to customize the One Identity Manager schema in order to map auxiliary class attributes in One Identity Manager. Use the program Schema Extension to do this.

12. On the **System attributes** page, you specify which LDAP system attribute is used to uniquely identify the objects.

NOTE: This step is only displayed if you have set the option **Expert mode** for the system connection wizard.

- Select the attribute to uniquely identify the objects in the LDAP under **Object identification attributes**. The attribute must be unique and set for all objects LDAP.
- Specify which attribute to use for revision filtering under **Revision properties**.
- Specify which additional attributes to determine for LDAP objects on the **Additional operational attributes** page. Functional attributes are used for managing directories. Attributes are only determined if they are explicitly given.

NOTE: You may have to customize the One Identity Manager schema in order to map functional attributes in One Identity Manager. Use the program Schema Extension to do this.

13. If the LDAP server supports dynamic groups, mark the attribute which contains the URL with the search information for matching members of dynamic groups, on the **Select dynamic group attributes** page, for example memberURL.

NOTE: This step is only displayed if you have set the option **Configure advanced settings (Expert mode)** for the system connection wizard.

14. Specify additional password settings for user accounts on the **Password settings** page.
 - Enter the following settings.

Table 11: Password settings

Property	Description						
Password attribute	Attribute representing a user account's password, for example userPassword.						
Password change method	Method used to modify passwords,						
	<table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>Default method for modifying passwords. The password is written directly to the password attribute.</td> </tr> <tr> <td>ADLDS</td> <td>Password modification method used for systems based on Microsoft Active Directory Lightweight Directory Services (AD LDS).</td> </tr> </tbody> </table>	Value	Description	Default	Default method for modifying passwords. The password is written directly to the password attribute.	ADLDS	Password modification method used for systems based on Microsoft Active Directory Lightweight Directory Services (AD LDS).
Value	Description						
Default	Default method for modifying passwords. The password is written directly to the password attribute.						
ADLDS	Password modification method used for systems based on Microsoft Active Directory Lightweight Directory Services (AD LDS).						

15. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.
 - ① **NOTE:** Reenter all the connection data if you are not working with an encrypted One Identity Manager database and no synchronization project has been saved yet in the database. This page is not shown if a synchronization project already exists.
16. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
17. Select a project template on the **Select project template** page to use for setting up the synchronization configuration.

Table 12: Default project template

Project template	Description
OpenDJ Synchronization	Project template based on OpenDJ. Use this project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.
AD LDS Synchronization	This project template is based on Active Directory Lightweight Directory Services (AD LDS).

- ① **NOTE:** A default project template ensures that all required information is added in the One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself. Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.
18. Specify how system access should work on the page **Restrict target system access**. You have the following options:


Table 13: Specifying Target System Access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow should be set up to initially load the target system into the One Identity Manager database. The synchronization workflow has the following characteristics:


Option	Meaning
Changes are also made to the target system.	<ul style="list-style-type: none"> • Synchronization is in the direction of "One Identity Manager". • Processing methods in the synchronization steps are only defined in synchronization direction "One Identity Manager".
	<p>Specifies whether a provisioning workflow should be set up in addition to the synchronization workflow to initially load the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization in the direction of the "target system" • Processing methods are only defined in the synchronization steps in synchronization direction "target system". • Synchronization steps are only created for such schema classes whose schema types have write access.

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

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

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

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

 **NOTE:** Ensure that this server is set up as the synchronization server after saving the synchronization project.

20. Enter the general setting for the synchronization project on the **General** page.

NOTE: This step is only shown if the selected project template supports several script languages.

Table 14: General Synchronization Project Properties

Property	Description
Display name	Display name for the synchronization project.
Script language	Language in which the scripts for this synchronization project are written. Scripts are implemented at various points in the synchronization configuration. Specify the script language when you set up an empty project. IMPORTANT: The script language cannot be changed after the synchronization project has been saved. If you use a project template, the template's script language is used.
Description	Spare text box for additional explanation.

21. Click **Finish** to complete the project wizard.

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

The synchronization project is created, saved and enabled immediately.

NOTE: If the synchronization project is not going to be executed immediately, disable the option **Activate and save the new synchronization project automatically**.

In this case, save the synchronization project manually before closing the Synchronization Editor.

NOTE: The target system connection data is saved in a variable set, which you can change in the Synchronization Editor under **Configuration | Variables** if necessary.

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the category **Configuration | Target system**.
2. To configure the synchronization log for the database connection, select the category **Configuration | One Identity Manager connection**.
3. Select **General** view and click **Configure....**
4. Select the **Synchronization log** view and set **Create synchronization log**.

5. Enable the data to be logged.

NOTE: Certain content create a lot of log data.

The synchronization log should only contain the data necessary for error analysis and other evaluations.

6. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

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

NOTE: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the domain 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 domain.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
 - a. Select the category **LDAP | User accounts | Linked but not configured | <Domain>**.
 - b. Select the task **Assign account definition to linked accounts**.

Detailed information about this topic

- [One Identity Manager Target System Synchronization Reference Guide](#)

Related Topics


- [Setting Up the Synchronization Server](#) on page 14
- [Users and Permissions for Synchronizing with LDAP](#) on page 12
- [Show Synchronization Results](#) on page 29

- [Customizing Synchronization Configuration](#) on page 30
- [Speeding Up Synchronization with Revision Filtering](#) on page 33
- [OpenDJ Basic Template](#) on page 127
- [Default Project Template for Active Directory Lightweight Directory Services](#) on page 128
- [Setting Up Account Definitions](#) on page 40
- [Automatic Assignment of Employees to LDAP User Accounts](#) on page 92


Show Synchronization Results

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

To display a synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Logs**.
3. Click  in the navigation view toolbar.
Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking on it.
An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log.

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Logs**.
3. Click  in the navigation view toolbar.
Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking on it.
An analysis of the provisioning is show as a report. You can save the report.

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In the Designer, set the "DPR\Journal\LifeTime" configuration parameter and enter the maximum retention time.

Customizing Synchronization Configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization of an LDAP domain. You can use this synchronization project to load LDAP objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the LDAP environment.

You must customize the synchronization configuration in order to compare the LDAP database with the regularly and to synchronize changes.

- Create a workflow with the direction of synchronization "target system" to use One Identity Manager as the master system for synchronization.
- You can use variables to create generally applicable synchronization configurations which contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes or processing methods, for example.
- To specify which LDAP objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Use variables to set up a synchronization project which can be used for several different domains. Store a connection parameter as a variable for logging in to the domain.
- Update the schema in the synchronization project, if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

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

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

Detailed information about this topic

- [Configuring Synchronization in LDAP Domains](#) on page 31
- [Configuring Synchronization of Several LDAP Domains](#) on page 31
- [Updating Schemas](#) on page 32

Configuring Synchronization in LDAP Domains

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

To create a synchronization configuration for synchronizing LDAP domains

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.
This adds a workflow for synchronizing in the direction of the target system.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related Topics

- [Configuring Synchronization of Several LDAP Domains](#) on page 31

Configuring Synchronization of Several LDAP Domains

Prerequisites

- The target system schema of both domains are identical.
- All virtual schema properties used in the mapping must exist in the extended schema of both domains.

To customize a synchronization project for synchronizing another domain

1. Prepare a user account with sufficient permissions for synchronizing in the other domain.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other domain. Use the wizards to attach a base object.
 - Select the LDAP connector in the wizard and enter the connection parameters. The connection parameters are saved in a special variable set.
A start up configuration is created, which uses the new variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related Topics

- [Configuring Synchronization in LDAP Domains](#) on page 31

Updating Schemas

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

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

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

- A schema was changed by:
 - Changes to a target system schema
 - Customizations to the One Identity Manager schema
 - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
 - Activating the synchronization project
 - Synchronization project initial save

- Compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target system**.
- OR -
Select the category **Configuration | One Identity Manager connection**.
3. Select the view **General** and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Mappings**.
3. Select a mapping in the navigation view.
Opens the Mapping Editor. For more detailed information about editing mappings, see One Identity Manager Target System Synchronization Reference Guide.

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

Speeding Up Synchronization with Revision Filtering

When you start synchronization, all synchronization objects are loaded. Some of these objects have not be modified since the last synchronization and, therefore, must not be processed. Synchronization is accelerated by only loading those object pairs that have changed since the last synchronization. One Identity Manager uses revision filtering to accelerate synchronization.

LDAP supports revision filtering. Revision attributes defined when the synchronization project was set up, are used for the revision count. In the default version, the creation date and the date that LDAP objects were last modified is used. Every synchronization saves the last execution date in the One Identity Manager database. (table `DPRRevisionStore`, column `value`). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. The next time synchronization is run, only those objects that have been changed since this date are loaded. This avoids unnecessary updating of objects that have not changed since the last synchronization.

Determining the revision is done when synchronization starts. Objects changed after this point are included with the next synchronization.

Revision filtering can be applied to workflows and start up configuration.

To permit revision filtering on a workflow

- Open the synchronization project in the Synchronization Editor.
- Edit the workflow properties. Select the entry **Use revision filter** from **Revision filtering**.

To permit revision filtering for a start up configuration

- Open the synchronization project in the Synchronization Editor.
- Edit the start up configuration properties. Select the entry **Use revision filter** from **Revision filtering**.

NOTE: Specify whether revision filtering will be applied when you first set up initial synchronization in the project wizard.

For more detailed information about revision filtering, see the One Identity Manager Target System Synchronization Reference Guide.

Post-Processing Outstanding Objects

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

Objects marked as outstanding:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Must be post-processed separately in One Identity Manager.

Start target system synchronization to do this.

To post-process outstanding objects

1. Select the category **LDAP | Target system synchronization: LDAP**.
All tables assigned to the target system type LDAP as synchronization tables are displayed in the navigation view.
2. Select the table whose outstanding objects you want to edit in the navigation view.
This opens the target system synchronization form. All objects are shown here that are marked as outstanding.




TIP:

To display object properties of an outstanding object

- a. Select the object on the target system synchronization form.
- b. Open the context menu and click **Show object**.

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

Table 15: Methods for handling outstanding objects

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

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

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

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

To disable bulk processing

- Deactivate  in the form toolbar.

You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization.

1. Select the category **LDAP | Basic configuration data | Target system types**.
2. Select the target system type LDAP in the result list.
3. Select **Assign synchronization tables** in the task view.
4. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
5. Save the changes.
6. Select **Configure tables for publishing**.

7. Select custom tables whose outstanding objects can be published in the target system and set the option **Publishable**.
8. Save the changes.

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

Configuring Memberships Provisioning

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

- Memberships are saved in the target system as an object property in list form (Example: List of user accounts in the property Member of an LDAP GroupOfNames).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

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

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

To allow separate provisioning of memberships

1. Start the Manager.
2. Select the category **LDAP | Basic configuration data | Target system types**.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
 - The option can only be set for assignment tables whose base table has a XDateSubItem or a CCC_XDateSubItem.
 - Assignment tables, which are grouped together in a virtual schema property in the mapping, must be labeled identically (beispielsweise LDAPAccountInLDAPGroup, LDAPGroupInLDAPGroup and LDAPMachineInLDAPGroup).
5. Click **Enable merging**.
6. Save the changes.

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

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

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

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

Help for Analyzing Synchronization Issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance. The report contains information such as:

- Consistency check results
- Revision filter settings
- Scope applied
- Analysis of the synchronization buffer
- Object access times in the One Identity Manager database and in the target system

To generate a synchronization analysis report

1. Open the synchronization project in the Synchronization Editor.
2. Select the menu **Help | Generate synchronization analysis report** and answer the security prompt with **Yes**.
The report may take a few minutes to generate. It is displayed in a separate window.
3. Print the report or save it in one of the available output formats.

Deactivating Synchronization

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

To prevent regular synchronization

- Select the start up configuration and deactivate the configured schedule.
Now you can only start synchronization manually.

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

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

To deactivate the loaded synchronization project

1. Select **General** on the start page.
2. Click **Deactivate project**.

Detailed information about this topic

- [Creating a Synchronization Project for initial Synchronization of an LDAP Domain](#) on page 18

Basic Configuration Data

To manage an LDAP environment in One Identity Manager, the following data is relevant.

- Configuration parameter

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

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

For more information, see [Appendix: Configuration Parameters for Managing LDAP](#) on page 123.

- Account definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not 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.

For more information, see [Setting Up Account Definitions](#) on page 40.

- Password policies

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

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

For more information, see [Password Policies](#) on page 57.

- Initial Password for New User Accounts

You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used or a randomly generated initial password can be issued.

For more information, see [Initial Password for New LDAP User Accounts](#) on page 66.

- Email notifications about login data

When a new user account is created, the login data are sent to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.

For more information, see [Email Notifications about Login Data](#) on page 68.

- Target System Types

Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.

For more information, see [Post-Processing Outstanding Objects](#) on page 34.

- Target system managers

A default application role exists for the target system manager in the One Identity Manager. Assign this application to employees who are authorized to edit the domains in One Identity Manager.

Define other application roles, if you want to limit target system managers' access permissions to individual domains. The application roles must be added under the default application role.

For more information, see [Target System Managers](#) on page 70.

Setting Up Account Definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not 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.


For more details about the basics, see the One Identity Manager Target System Base Module Administration Guide.

The following steps are necessary to implement an account definition:

- [Creating an Account Definition](#)
- [Setting Up Manage Levels](#)
- [Creating a Formatting Rule for IT Operating Data](#)
- [Determining IT Operating Data](#)
- [Assigning Account Definitions to Employees](#)
- [Assigning Account Definitions to a Target System](#)

Creating an Account Definition

To create a new account definition

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list. Select **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- [Master Data for an Account Definition](#) on page 41

Master Data for an Account Definition

Enter the following data for an account definition:

Table 16: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema which maps user accounts.
Target System	Target system to which the account definition applies.
Required	Required account definitions. Define the dependencies between account

Property	Description
account definition	<p>definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it.</p> <p>Leave empty for LDAP domains.</p>
Description	Spare text box for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	<p>Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set.</p> <p>For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.</p>
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can still be directly assigned to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	<p>Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.</p> <p>i IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.</p> <p>Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</p>
Retain account definition if permanently	<p>Specifies the account definition assignment to permanently disabled employees.</p> <p>Option set: the account definition assignment remains in effect. The user</p>

Property	Description
disabled	<p>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 disabled 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> <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 security risk	<p>Specifies the account definition assignment to employees posing a security risk .</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Setting Up Manage Levels

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

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

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.

Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level. For more detailed information about manage levels, see the One Identity Manager Target System Base Module Administration Guide.

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


To assign manage levels to an account definition

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level** in the task view.
4. Assign manage levels in **Add assignments**.
- OR -
Remove assignments to manage levels in **Remove assignments**.
5. Save the changes.

IMPORTANT: The manage level "Unmanaged" is assigned automatically when an account definition is assigned and cannot be removed.

To edit a manage level

1. Select the category **LDAP | Basic configuration data | Account definitions | Manage levels**.

2. Select the manage level in the result list. Select **Change master data**.
- OR -
Click  in the result list toolbar.
3. Edit the manage level's master data.
4. Save the changes.

Related Topics

- [Master Data for a Manage Level](#) on page 45

Master Data for a Manage Level

Enter the following data for a manage level.

Table 17: Master Data for a Manage Level

Property	Description						
Manage level	Name of the manage level.						
Description	Spare text box for additional explanation.						
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <table border="0" style="margin-left: 20px;"> <tr> <td>Never</td> <td>Data is not updated</td> </tr> <tr> <td>always</td> <td>Data is always updated</td> </tr> <tr> <td>Only initially</td> <td>Data is only initially determined.</td> </tr> </table>	Never	Data is not updated	always	Data is always updated	Only initially	Data is only initially determined.
Never	Data is not updated						
always	Data is always updated						
Only initially	Data is only initially determined.						
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.						
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.						
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.						
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.						
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.						
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.						
Retain groups on	Specifies whether user accounts of employees posing a security						

Property	Description
security risk	risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether locked user accounts retain their group memberships.

Creating a Formatting Rule for IT Operating Data

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

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

- LDAP Container
- Groups can be inherited
- Identity
- Privileged user account

To create a mapping rule for IT operating data

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Edit IT operating data mapping** in the task view and enter the following data.

Table 18: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: <ul style="list-style-type: none"> • Primary department • Primary location

Property Description

	<ul style="list-style-type: none">• Primary cost center• Primary business roles <p>i NOTE: Only use the primary business role if the Business Roles Module is installed.</p> <ul style="list-style-type: none">• Empty <p>If you select a role, you must specify a default value and set the option Always use default value.</p>
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\LDAP\Accounts\MailTemplateDefaultValues".

4. Save the changes.

Related Topics

- [Determining IT Operating Data](#) on page 47

Determining IT Operating Data

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.

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.

To specify IT operating data

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

Table 19: IT Operating Data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.
	<p>To specify an application scope</p> <ol style="list-style-type: none"> a. Click → next to the text box. b. Select the table under Table, which maps the target system or the table TSBAccountDef for an account definition. c. Select the concrete target system or concrete account definition under Effects on. d. Click OK.
Column	User account property for which the value is set. Columns using the script template TSB_ITDataFromOrg in their template are listed. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
Value	Concrete value which is assigned to the user account property.

3. Save the changes.

Related Topics

- [Creating a Formatting Rule for IT Operating Data](#) on page 46

Modifying IT Operating Data

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

Prerequisites

- The IT operating data of a department, cost center, business role or a location was changed.
- OR -
- The default values in the IT operating data template were modified for an account definition.

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

To execute the template

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

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

Old value Current value of the object property.

New value Value applied to the object property after modifying the IT operating data.

Selection Specifies whether the modification is applied to the user account.

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

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

Assigning Account Definitions to Employees

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

Detailed information about this topic

- [Assigning Account Definitions to Departments, Cost Centers and Locations](#) on page 51
- [Assigning Account Definitions to Business Roles](#) on page 51
- [Assigning Account Definitions to all Employees](#) on page 52
- [Assigning Account Definitions Directly to Employees](#) on page 53
- [Assigning Account Definitions to a Target System](#) on page 55

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
 - Assign departments on the **Departments** tab.
 - Assign locations on the **Locations** tab.
 - Assign cost centers on the **Cost center** tab.

- OR -

Remove the organizations from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning Account Definitions to Business Roles](#) on page 51
- [Assigning Account Definitions to all Employees](#) on page 52
- [Assigning Account Definitions Directly to Employees](#) on page 53

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

- OR -

Remove business roles in **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning Account Definitions to Departments, Cost Centers and Locations](#) on page 51
- [Assigning Account Definitions to all Employees](#) on page 52
- [Assigning Account Definitions Directly to Employees](#) on page 53

Assigning Account Definitions to all Employees

To assign an account definition to all employees

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Automatic assignment to employees** on the **General** tab.
 - ❗ **IMPORTANT:** Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.
5. Save the changes.

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

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

Related Topics

- [Assigning Account Definitions to Departments, Cost Centers and Locations](#) on page 51
- [Assigning Account Definitions to Business Roles](#) on page 51
- [Assigning Account Definitions Directly to Employees](#) on page 53

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees** in the task view.
4. Assign employees in **Add assignments**.
- OR -
Remove employees from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning Account Definitions to Departments, Cost Centers and Locations](#) on page 51
- [Assigning Account Definitions to Business Roles](#) on page 51
- [Assigning Account Definitions to all Employees](#) on page 52

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

1. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.
- OR -
Remove assignments to system roles in **Remove assignments**.
5. Save the changes.

Adding Account Definitions in the IT Shop

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

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

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

To add an account definition to the IT Shop

1. Select the category **LDAP | Basic configuration data | Account definitions** (non role-based login).
- OR -
Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the account definition to the IT Shop shelf in **Add assignments**
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. Select the category **LDAP | Basic configuration data | Account definitions** (non role-based login).
- OR -
Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the account definition from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

1. Select the category **LDAP | Basic configuration data | Account definitions** (non role-based login).
- OR -
Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.

3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related Topics

- [Master Data for an Account Definition](#) on page 41
- [Assigning Account Definitions to Departments, Cost Centers and Locations](#) on page 51
- [Assigning Account Definitions to Business Roles](#) on page 51
- [Assigning Account Definitions Directly to Employees](#) on page 53
- [Assigning Account Definitions to System Roles](#) on page 53

Assigning Account Definitions to a Target System

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

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

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

To assign the account definition to a target system

1. Select the domain in the category **LDAP | Domains**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

Detailed information about this topic

- [Automatic Assignment of Employees to LDAP User Accounts](#) on page 92


Deleting an Account Definition

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

NOTE: If an account definition is deleted, the user accounts arising from this account definition are deleted.

To delete an account definition

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

- d. Save the changes.
5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves. For more detailed information, see the One Identity Manager IT Shop Administration Guide.
6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Select **Change master data** in the task view.
 - d. Remove the account definition from the **Required account definition** menu.
 - e. Save the changes.
7. Remove the account definition's assignments to target systems.
 - a. Select the domain in the category **LDAP | Domains**.
 - b. Select **Change master data** in the task view.
 - c. Remove the assigned account definitions on the **General tab**.
 - d. Save the changes.
8. Delete the account definition.
 - a. Select the category **LDAP | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Click , to delete the account definition.

Password Policies

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

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

Detailed information about this topic

- [Predefined Password Policies](#) on page 58
- [Editing Password Policies](#) on page 59
- [Custom Scripts for Password Requirements](#) on page 61

- [Restricted Passwords](#) on page 64
- [Testing a Password](#) on page 64
- [Testing Generating a Password](#) on page 64
- [Assigning a Password Policy](#) on page 65

Predefined Password Policies

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

Password for logging into One Identity Manager

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

The password policy "One Identity Manager password policy" is also labeled as the default and is used when no other password policy is found.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The password policy "Employee central password policy" defines the settings for the central password (Person.CentralPassword).

- ❗ **IMPORTANT:** Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.

Password policies for target systems

A predefined password policy that you can apply to the user account password columns, is provided for every target system.


- ❗ **NOTE:** When you update One Identity Manager version 7.x to One Identity Manager version 8.0.2, the configuration parameter settings for forming passwords are passed on to the target system specific password policies.
- ❗ **IMPORTANT:** If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

The password policy "LDAP password policy" is predefined for LDAP. You can apply this password policy to LDAP user accounts passwords (LDAPAccount.UserPassword) of an LDAP domain or an LDAP container.

If the domains' or containers' password requirements differ, it is recommended that you set up your own password policies for each domain or container.

Editing Password Policies

To edit a password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the LDAP.
2. Select the password policy in the result list and select **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Edit the password policy's master data.
4. Save the changes.




Detailed information about this topic


- [General Master Data for a Password Policy](#) on page 59
- [Policy Settings](#) on page 60
- [Character Sets for Passwords](#) on page 60
- [Custom Scripts for Password Requirements](#) on page 61

General Master Data for a Password Policy

Enter the following master data for a password policy.

Table 20: Master Data for a Password Policy

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.
Description	Spare text box for additional explanation. Translate the given text using the  button.
Error Message	Custom error message outputted if the policy is not fulfilled. Translate the given text using the  button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords.

 **NOTE:** The password policy "One Identity Manager password policy" is marked as the default policy. This password policy is applied if no other password policies can be found.

Policy Settings

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

Table 21: Policy Settings

Property	Meaning
Initial password	Initial password for new user accounts. If no password is given when the user account is added or a random password is generated, the initial password is used.
Password confirmation	Reconfirm password.
Min. Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If the value '5' is entered, for example, the last 5 passwords of the user are saved.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The password strength is not tested if the value is '0'. The values '1', '2', '3' and '4' gauge the required complexity of the password. The value '1' demands the least complex password. The value '4' demands the highest complexity.
Name properties denied	Specifies whether name properties are permitted in the password.

Character Sets for Passwords

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

Table 22: Character Classes for Passwords

Property	Meaning
Min. letters	Specifies the minimum number of alphabetical characters

Property	Meaning
	the password must contain.
Min. number lower case	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted characters.
Denied special characters	List of characters, which are not permitted.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Maximum number of identical character that can be repeated after each other.

Custom Scripts for Password Requirements

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

Detailed information about this topic

- [Script for Checking a Password](#) on page 61
- [Script for Generating a Password](#) on page 63

Script for Checking a Password

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

Syntax for Check Scripts

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

With parameters:

policy = password policy object

spwd = password to test

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

Example for a script for testing a password

A password cannot have '?' or '!' at the beginning. The script checks a given password for validity.

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

To use a custom script for checking a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
 - a. Select the category **Manager | Basic configuration data | Password policies** in the LDAP.
 - b. Select the password policy in the result list.
 - c. Select **Change master data** in the task view.
 - d. Enter the name of the script to test the password in **Check script** on the **Scripts** tab.
 - e. Save the changes.

Related Topics

- [Script for Generating a Password](#) on page 63

Script for Generating a Password

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

Syntax for Generating Script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

The script replaces the invalid characters '?' and '!' in random passwords.

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

```
    Dim pwd = spwd.ToInsecureArray()  
    ' replace invalid characters at first position  
    If pwd.Length>0  
        If pwd(0)="?" Or pwd(0)="!"  
            spwd.SetAt(0, CChar("_"))  
        End If  
    End If
```

```
End Sub
```

To use a custom script for generating a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
 - a. Select the category **Manager | Basic configuration data | Password policies** in the LDAP.
 - b. Select the password policy in the result list.
 - c. Select **Change master data** in the task view.
 - d. Enter the name of the script to generate a password in **Generation script** on the **Scripts** tab.
 - e. Save the changes.

Related Topics

- [Script for Checking a Password](#) on page 61

Restricted Passwords

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

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

To add a term to the restricted list

1. Select the category **Base Data | Security Settings | Restricted passwords** in the Designer.
2. Create a new entry with the menu item **Object | New** and enter the term to be excluded to the list.
3. Save the changes.

Testing a Password

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

To test whether a password conforms to the password policy

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

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

Testing Generating a Password

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

To generate a password that conforms to the password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the LDAP.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
4. Select the **Test** tab.
5. Click **Generate**.

This generates and displays a password.

Assigning a Password Policy

The password policy "LDAP password policy" is predefined for LDAP. You can apply this password policy to LDAP user accounts passwords (LDAPAccount.UserPassword) of an LDAP domain or an LDAP container.

If the domains' or containers' password requirements differ, it is recommended that you set up your own password policies for each domain or container.

- ❗ **IMPORTANT:** If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

To reassign a password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the LDAP.
2. Select the password policy in the result list.
3. Select **Assign objects** in the task view.

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

Table 23: Assigning a Password Policy

Property	Description
Apply to	Application scope of the password policy. To specify an application scope <ol style="list-style-type: none"> Click → next to the text box. Select the table which contains the password column under Table. Select the specific target system under Apply to. Click OK.
Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

- Save the changes.

To change a password policy's assignment

- Select the category **Manager | Basic configuration data | Password policies** in the LDAP.
- Select the password policy in the result list.
- Select **Assign objects** in the task view.
- Select the assignment you want to change in **Assignments**.
- Select the new password policy to apply from the **Password Policies** menu.
- Save the changes.

Initial Password for New LDAP User Accounts

Table 24: Configuration Parameters for Formatting Initial Passwords for User Accounts

Configuration parameter	Meaning
QER\Person\UseCentralPassword	This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central

Configuration parameter	Meaning
	password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated.
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permanently stored. If the parameter is not set, the central password is only used for publishing to existing target system specific user accounts and is subsequently deleted from the One Identity Manager database.
TargetSystem\LDAP\Accounts InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.

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

- User the employee's central password. The employee's central password is mapped to the user account password.
 - Set the configuration parameter "QER\Person\UseCentralPassword" in the Designer.

If the configuration parameter "QER\Person\UseCentralPassword" is set, the employee's central password is automatically mapped to an employee's user account in each of the target systems. This excludes privileged user accounts, which are not updated.
 - Use the configuration parameter "QER\Person\UseCentralPassword\PermanentStore" in the Designer to specify whether an employee's central password is permanently saved in the One Identity Manager database or only until the password has been published in the target system.

The password policy "Employee central password policy" is used to format the central password.

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

- Create user accounts manually and enter a password in their master data.
- Specify an initial password to be used when user accounts are created automatically.
 - Apply the target system specific password policies and enter an initial password in the password policies.
- Assign a randomly generated initial password to enter when you create user accounts.
 - Set the configuration parameter "TargetSystem\LDAP\Accounts\InitialRandomPassword" in the Designer.
 - Apply target system specific password policies and define the character sets that the password must contain.
 - Specify which employee will receive the initial password by email.

Related Topics

- [Password Policies](#) on page 57
- [Email Notifications about Login Data](#) on page 68

Email Notifications about Login Data

Table 25: Configuration Parameters for Notifications about Login Data

Configuration parameter	Meaning
TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\LDAP\DefaultAddress".
TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplateName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".
TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\LDAP\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.

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

To use email notifications about login data

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Configuration Guide.
2. Enable the configuration parameter "Common\MailNotification\DefaultSender" in the Designer and enter the email address for sending the notification.
3. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.
4. Ensure that a language culture can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.

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

To send initial login data by email

1. Set the configuration parameter "TargetSystem\LDAP\Accounts\InitialRandomPassword" in the Designer.
2. Set the configuration parameter "TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo" in the Designer and enter the message recipient as the value.
3. Set the configuration parameter "TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in the Designer.

By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.

4. Set the configuration parameter "TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in the Designer.

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

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

Target System Managers

For more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

Implementing Application Roles for Target System Managers

1. The One Identity Manager administrator assigns employees to be target system managers.
2. These target system managers add employees to the default application role for target system managers.
The default application role target system managers are entitled to edit all domains in One Identity Manager.
3. Target system managers can authorize more employees as target system managers, within their scope of responsibilities and create other child application roles and assign individual domains.

Table 26: Default Application Roles for Target System Managers

User	Task
Target System Managers	<p>Target system managers must be assigned to the application role Target systems LDAP or a sub application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change or delete target system objects, like user accounts or groups.• Edit password policies for the target system.• Prepare groups for adding to the IT Shop.• Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.• Edit the synchronization's target system types and outstanding objects.• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to the Manager as One Identity Manager administrator (application role **Base role | Administrators**)

2. Select the category **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees** in the task view.
4. Assign the employee you want and save the changes.

To add the first employees to the default application as target system managers.

1. Log yourself into the Manager as target system administrator (application role **Target systems | Administrator**).
2. Select the category **One Identity Manager Administration | Target systems | LDAP**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

1. Login to the Manager as target system manager.
2. Select the application role in the category **LDAP | Basic configuration data | Target system managers**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To define target system managers for individual domains.

1. Login to the Manager as target system manager.
2. Select the category **LDAP | Domains**.
3. Select the domain in the result list.
4. Select **Change master data** in the task view.
5. Select the application role on the **General** tab in the **Target system manager** menu.

- OR -

Click  next to the **Target system manager** menu to create a new application role.

- Enter the application role name and assign the parent application role **Target system | LDAP**.
 - Click **OK** to add the new application role.
6. Save the changes.
 7. Assign the application role to employees, who are authorized to edit the domain in One Identity Manager.

NOTE: You can also specify target system managers for individual containers. Target system managers for a container are authorized to edit objects in this container.

Related Topics

- [One Identity Manager Users for Managing an LDAP](#) on page 8
- [General Master Data for an LDAP Domain](#) on page 73
- [LDAP Container Structures](#) on page 114

LDAP Domains

NOTE: The Synchronization Editor sets up the domains in the One Identity Manager database by using a default template.

To edit master data for an LDAP domain

1. Select the category **LDAP | Domains**.
2. Select the domain in the result list and run the task **Change master data**.
3. Edit the domain's master data.
4. Save the changes.

Detailed information about this topic



- [General Master Data for an LDAP Domain](#) on page 73
- [LDAP Specific Master Data for an LDAP Domain](#) on page 75
- [Specifying Categories for Inheriting LDAP Groups](#) on page 76

General Master Data for an LDAP Domain

Enter the following data on the **General** tab:

Table 27: Domain Master Data

Property	Description
Domain	NetBIOS domain name.
Full domain name	Name of the domain confirming to DNS syntax. Name of this domain.name of parent domain.name of default domain Example

Property	Description
	Docu.Testlab.dd
LDAP system type	Type of the LDAP system.
Display name	The display name is used to display the domain in the user interface. This is preset with the domain NetBIOS name; however, the display name can be changed.
Object class	List of classes defining the attributes for this object. The default object class is "DOMAIN". However, you can add object classes and auxiliary classes in the input field that are used by other LDAP and X.500 directory services.
Distinguished name	Distinguished name of the domain. The distinguished name is determined using a template from the full domain name and cannot be edited.
Canonical name	Canonical name of the domain.
Account definition (initial)	<p>Initial account definition for creating user accounts. These account definitions are used if automatic assignment of employees to user account is used for this domain resulting in administered user accounts (state "Linked configured"). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the employee (state "Linked") if no account definition is given. This is the case on initial synchronization, for example.</p>
Target system managers	<p>Application role in which target system managers are specified for the domain. Target system managers only edit the objects from domains that are assigned to them. Therefore, each domain can have a different target system manager assigned to it.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this domain. Use the  button to add a new application role.</p>
Synchronized by	<p> NOTE: You can only specify the synchronization type when adding a new domain. No changes can be made after saving.</p> <p>"One Identity Manager" is used when you create a domain with the Synchronization Editor.</p> <p>Type of synchronization through which the data is synchronized between the domain and One Identity Manager.</p>

Property	Description
Table 28: Permitted Values	
Value	Synchronization by
One Identity Manager	LDAP connector
No synchronization	none
<p>NOTE: If you select "No synchronization" you can define custom processes to exchange data between One Identity Manager and the target system.</p>	
Description	Spare text box for additional explanation.
Structural object class	Structural object class representing the object type.

Related Topics

- [Automatic Assignment of Employees to LDAP User Accounts](#) on page 92
- [Target System Managers](#) on page 70

LDAP Specific Master Data for an LDAP Domain

Enter the following master data on the **LDAP** tab.

Table 29: LDAP Data


Property	Description
Full domain name	Name of the domain confirming to DNS syntax. Name of this domain.name of parent domain.name of default domain Example Docu.Testlab.dd
Distinguished name	Distinguished name of the domain. The distinguished name is determined using a template from the full domain name and cannot be edited.
Structural object class	Structural object class representing the object type.
Object class	List of classes defining the attributes for this object. The default object class is "DOMAIN". However, you can add object classes and auxiliary

Property	Description
	classes in the input field that are used by other LDAP and X.500 directory services.
Search mask	Search mask for another LDAP object.

Specifying Categories for Inheriting LDAP Groups

In One Identity Manager, groups can be selectively inherited by user accounts. For this, groups and user accounts are divided into categories. The categories can be freely selected and are specified by a template. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. Enter your categories for the target system dependent groups, administrative roles, subscriptions and disabled service plans in the . Each table contains the category items "Position1" to "Position31".

To define a category

1. Select the category **LDAP | Domains**.
2. Select the domain in the result list.
3. Select **Change master data** in the task view.
4. Switch to the **Mapping rule category** tab.
5. Expand the respective base node of the user account or group table.
6. Click  to enable category.
7. Enter a name for the user account and group categories in the current language.
8. Save the changes.

Detailed information about this topic

- [LDAP Group Inheritance Based on Categories](#) on page 110

How to Edit a Synchronization Project

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

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

To open an existing synchronization project in the Synchronization Editor

1. Select the category **LDAP | Domains**.
2. Select the domain in the result list. Select **Change master data** in the task view.
3. Select **Edit synchronization project...** from the task view.

Related Topics

- [Customizing Synchronization Configuration](#) on page 30

LDAP User Accounts

You manage user account in One Identity Manager with LDAP. A user can login in to a domain with a user account and receive group memberships and access rights to network resources.

Detailed information about this topic

- [Linking User Accounts to Employees](#) on page 78
- [Supported User Account Types](#) on page 79
- [Entering Master Data for LDAP User Accounts](#) on page 82

Linking User Accounts to Employees

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 and user accounts can be entered manually and assigned to each other.
- Employees can automatically obtain their account definitions using user account resources. If an employee does not have a user account in an LDAP domain, 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.

When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.

NOTE: If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, primary location or a primary cost center.

- An existing employee is automatically assigned when a user account is added or a new employee is created if necessary. In this case, employee master data is created on the basis of the existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. This method, however, is not the One Identity Manager default method. Define criteria for finding employees for automatic employee assignment.

Related Topics

- [Entering Master Data for LDAP User Accounts](#) on page 82
- [Setting Up Account Definitions](#) on page 40
- [Automatic Assignment of Employees to LDAP User Accounts](#) on page 92
- For more detailed information about employee handling and administration, see the One Identity Manager Target System Base Module Administration Guide.

Supported User Account Types

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

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

- Identity (column IdentityType)
The identity describes the type of user account.

Table 30: Identities of User Accounts

Identity	Description	Value of the column "IdentityType"
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for various roles within the organization, f. ex. In sub-agreements with other functional areas.	Organizational

Identity	Description	Value of the column "IdentityType"
Personalized admin identity	User account with administration rights used by one person.	Admin
Sponsored identity	User account used for example for training purposes.	Sponsored
Shared identity	User account with administration rights used by several people.	Shared
Service identity	Service account.	Service

- Privileged user account (column IsPrivilegedAccount)

Use this option to flag user accounts with special, privileged permissions. This includes administrative user accounts or service accounts, for example. This option is not used to flag default user accounts.

Default User Accounts

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

To create default user accounts through account definitions

1. Create an account definition and assign the manage level "Unmanaged" or "Full managed" to it.
2. Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

- Use the default value "1" in the formatting rule for the column IsGroupAccount and set the option **Always use default value**.
- Use the default value "primary" in the formatting rule for the column IdentityType and set the option **Always use default value**.

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

5. Assign the account definition to employees.

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

Administrative User Accounts

An administrative user account must be used for certain administrative tasks.

Administrative user accounts are normally predefined in the target system and have fixed identifiers and login names, for example, "Administrator".

Administrative user accounts are loaded through synchronization into the One Identity Manager. To assign a manager to administrative user accounts, assign an employee to the user account in One Identity Manager.

- NOTE:** You can automatically label administrative user accounts as privileged user accounts. To do this, set the schedule "Mark selected user accounts as privileged" in the Designer.

Privileged User Accounts

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

- NOTE:** The criteria used to label user accounts automatically as privileged, are defined as extensions to the view definition (ViewAddOn) on the table TSBVAccountIsPrivDetectRule (table type "Union"). The evaluation is done in the script TSB_SetIsPrivilegedAccount.

To create privileged users through account definitions

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

An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's

department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

- Use the default value "1" in the formatting rule for the column `IsPrivilegedAccount` and set the option **Always use default value**.
 - You can also specify a formatting rule for the column `IdentityType`. The column owns different permitted values, which represent user accounts.
 - To prevent privileged user accounts inheriting default user groups, define a template for the column `IsGroupAccount` with the default value "0" and set the option **Always use default value**.
5. Enter the effective IT operating data for the target system.
Specify in the departments, cost centers, locations or business roles, which IT operating data should apply when you set up a user account.
 6. Assign the account definition directly to employees who work with privileged user accounts.

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

NOTE: Specify a formatting rule for a naming schema if it is required by the company for privileged user account login names.

To use a prefix with a login name, set the configuration parameter "TargetSystem\LDAP\Accounts\PrivilegedAccount\UserID_Prefix" in the Designer. To use a postfix with a login name, set the configuration parameter "TargetSystem\LDAP\Accounts\PrivilegedAccount\UserID_Postfix" in the Designer.

These configuration parameters are evaluated in the default installation, if a user account is marked with the property **Privileged user account** (`IsPrivilegedAccount`). The user account login names are renamed according to the formatting rules. This also takes place if the user accounts are labeled as privileged by the schedule "Mark selected user accounts as privileged".


Entering Master Data for LDAP User Accounts

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

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

- NOTE:** If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, primary location or a primary cost center.

To edit master data for a user account

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list and run the task **Change master data**.
- OR -
Click  in the result list toolbar.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list and run **Assign LDAP user accounts** from the task view.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic

- [General Master Data for an LDAP User Account](#) on page 83
- [Contact Data for an LDAP User Account](#) on page 87
- [Address Information for an LDAP User Account](#) on page 87
- [Organizational Data for an LDAP User Account](#) on page 88
- [Miscellaneous Data for an LDAP User Account](#) on page 89

Related Topics

- [Supported User Account Types](#) on page 79
- [Setting Up Account Definitions](#) on page 40

General Master Data for an LDAP User Account

Enter the following data on the **General** tab:

Table 31: Additional Master Data for a User Account

Property	Description
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you use automatic employee assignment, an associated employee is created and entered into the user account when the user account is saved.
Account definition	<p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p>i NOTE: The account definition cannot be changed once the user account has been saved.</p>
Manage level	User account's manage level. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Domain	Domain in which the user account is created.
Structural object class	Structural object class representing the object type. By default, user accounts in One Identity Manager are added with the object class "INETORGPERSO".
Container	Container in which to create the user account. If you have assigned an account definition, the container is determined from the company IT data for the assigned employee depending on the manage level of the user account. When the container is selected, the defined name for the user is created using a formatting rule.
Object class	List of classes defining the attributes for this object. By default, user accounts in One Identity Manager are added with the object class "INETORGPERSO". However, you can add object classes and auxiliary classes in the input field that are used by other LDAP and X.500 directory services.
Name	User account identifier. The identifier is made up of the user's first and last names.
Display name	User account display name. The display name is made up of the first and last names.
Distinguished name	User account's distinguished name. The distinguished name is formatted from the user account's identifier and the container and cannot be changed.

Property	Description
Object SID (AD)	The object's security ID (SID) in Active Directory.
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Initials	The user's initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Job description	Job description. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Login name	Login name. If you assigned an account definition, the login name is made up of the employee's central user account depending on the manage level.
Password	<p>Password for the user account. Depending on the configuration parameter "Person\UseCentralPassword" the employee's central password can be mapped to the user account's password. If you use an initial password for the user accounts, it is automatically entered when a user account is created.</p> <p>NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.</p>
Password confirmation	Reconfirm password.
Risk index (calculated)	Maximum risk index values for all assigned groups. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Account expiry date	Account expiry date. Specifying an expiry data for the account has the effect that the logon for this user account is blocked as soon as the given date is exceeded. If you assigned an account definition, the employee's last day of work it is automatically taken as the expiry date depending on the manage level. Any existing account expiry date is overwritten in this case.
Category	Categories for the inheritance of groups by the user account. Select one or more categories from the menu. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories.
Description	Spare text box for additional explanation.
Identity	User account's identity type

Property	Description
----------	-------------

Table 32: Permitted values for the identity.

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

Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	<p>Specifies whether the user account groups can inherit through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests.</p> <ul style="list-style-type: none">• If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.• If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
User account is disabled	Specifies whether the user account is disable. If a user account is not required for a period of time, you can temporarily disable the user account by using the option <User account is deactivated>.



Related Topics

- [Setting Up Account Definitions](#) on page 40
- [Password Policies](#) on page 57
- [Initial Password for New LDAP User Accounts](#) on page 66
- [Linking User Accounts to Employees](#) on page 78
- [Disabling LDAP User Accounts](#) on page 96

Contact Data for an LDAP User Account

Enter the data used by this user account for contacting the employee by telephone on the **Contact data** tab.

Table 33: Contact Data

Property	Description
Picture	Picture to display in a telephone book, for example. <ul style="list-style-type: none">• Load the picture using .• You can delete the picture using .
Email address	Email address. If you assigned an account definition, the email address is made up of the employee's default email address depending on the manage level of the user account.
Phone	Telephone number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Mobile phone	Mobile number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Pager	Pager number.
Fax	Fax number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Phone private	Private telephone number.
Phone, private (2)	Extra telephone number.
Internationale ISDN no.	Internationale ISDN number.
Additional email addresses	Additional email addresses.
X.121 address	Addressing as X.121 address.
X.400 address	Address in X.400 format.

Address Information for an LDAP User Account

Enter the following address data for contacting the employee on the **Address data** tab.

Table 34: Address data

Property	Description
Room	Room. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Registered address	Postal address.
Address	Postal address.
Address (private)	Postal address (private).
Mailbox	Mailbox. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Street	Street or road. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Zip code	Zip code. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
State	State. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.

Organizational Data for an LDAP User Account

Enter the following organizational master data on the **Organizational** tab.

Table 35: Organizational Master Data

Property	Description
Business unit	Business unit to which the employee is assigned.
Department	Employee's department. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Location	Employee's location. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Location ID	Location identifier (country and city) for telegram services.
Employment	Job details.
Employee number	Number for identifying the employee in addition to their ID.
Title	The user's academic title. If you have assigned an account definition, the

Property	Description
	input field is automatically filled out with respect to the manage level.
Organizational position	Details of position in the company, for example, directory or department manager.
Office	Office. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Preferred language	Preferred language. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Account manager	Manager responsible for the user account.
Secretary	Secretary's user account.
Country ID	The country ID.
Company	Employee's company. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Car license plate	Vehicle's license plate.

Miscellaneous Data for an LDAP User Account

Enter the following master data on the **Miscellaneous** tab.

Table 36: Miscellaneous Master Data

Property	Description
See Also	Link to another LDAP object.
Default PC	User's workstation.
User ID	User's Identification number.

Additional Tasks for Managing LDAP User Accounts

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

Overview of LDAP User Accounts

Use this task to obtain an overview of the most important information about a user account.

To obtain an overview of a user account

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Select **LDAP user account overview** in the task view.

Changing the Manage Level of an LDAP User Account

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

To change the manage level for a user account

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Select the manage level in the **Manage level** menu on the tab **General**.
5. Save the changes.

Related Topics

- [Entering Master Data for LDAP User Accounts](#) on page 82

Assigning LDAP Groups Directly to LDAP User Accounts

Groups can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and groups in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has a user account in LDAP, the groups in the role are inherited by this user account.

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

- NOTE:** User accounts cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

To assign groups directly to user accounts

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**.
- OR -
Remove groups from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning LDAP Groups to LDAP User Accounts and LDAP Computers](#) on page 101

Assign Extended Properties to an LDAP User Account

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

To specify extended properties for a user account

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.
- OR -
Remove assignments to extended properties in **Remove assignments**.
5. Save the changes.

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

Automatic Assignment of Employees to LDAP User Accounts

Table 37: Configuration Parameters for Automatic Employee Assignment

Configuration parameter	Meaning
TargetSystem\LDAP\PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\LDAP\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\LDAP\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.

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

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

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

Run the following tasks to assign employees automatically.

- If employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\LDAP\PersonAutoFullsync" in the Designer and select the required mode.
- If employees can be assigned by user accounts outside synchronization, set the parameter "TargetSystem\LDAP\PersonAutoDefault" in the Designer and select the required mode.

- Use the configuration parameter "TargetSystem\LDAP\PersonAutoDisabledAccounts" to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the domain. Ensure the manage level to be used is entered as default automation level.
- Define the search criteria for employees assigned to the domain.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

- NOTE:** Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the domain 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 domain.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
 - a. Select the category **LDAP | User accounts | Linked but not configured | <Domain>**.
 - b. Select the task **Assign account definition to linked accounts**.

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

Related Topics

- [Creating an Account Definition](#) on page 41
- [Assigning Account Definitions to a Target System](#) on page 55
- [Editing Search Criteria for Automatic Employee Assignment](#) on page 94

Editing Search Criteria for Automatic Employee Assignment

Criteria for employee assignment are defined in the domain. 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 LDAPDomain 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.

- 1 **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.

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

To specify criteria for employee assignment

1. Select the category **LDAP | Domains**.
2. Select the domain in the result list.
3. Select **Define search criteria for employee assignment** in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 38: Default Search Criteria for User Accounts

Apply to	Column on Employee	Column on User Account
LDAP user accounts	Central user account (CentralAccount)	Login name (UserID)

5. 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 39: 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.

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.

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

Related Topics

- [Automatic Assignment of Employees to LDAP User Accounts](#) on page 92

Disabling LDAP User Accounts

Table 40: Configuration Parameter for Disabling User Accounts

Configuration parameter	Meaning
QER\Person\TemporaryDeactivation	This configuration parameter specifies whether user accounts for an employee are locked if the employee is temporarily or permanently disabled.

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

Scenario:

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

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. User accounts with the manage level "Full managed" are disabled depending on the account definition settings. For user accounts with another manage level, modify the column template LDAPAccount.AccountDisabled accordingly.

Scenario:

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

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

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

To lock a user account when the configuration parameter is disabled

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To lock a user account, which is not linked to an employee

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

Related Topics

- [Setting Up Account Definitions](#) on page 40
- [Setting Up Manage Levels](#) on page 43
- [Deleting and Restoring LDAP User Accounts](#) on page 97
- For more detailed information about deactivating and deleting employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

Deleting and Restoring LDAP User Accounts

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

To delete a user account

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Delete the user account.
4. Confirm the security prompt with **Yes**.

To restore user account

1. Select the category **LDAP | User accounts**.
2. Select the user account in the result list.
3. Click **Undo delete** in the result list toolbar.

Configuring Deferred Deletion

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

Related Topics


- [Disabling LDAP User Accounts](#) on page 96

LDAP Groups

You can collect user accounts, contacts, computers and groups into groups that can be used to regulate access to resources in the LDAP directory. In One Identity Manager, you can set up new groups or to edit already existing groups.

To add users to groups, you assign the groups directly to users. This can be assignments of groups to departments, cost centers, location, business roles or to the IT Shop.

To edit group master data

1. Select the category **LDAP | Groups**.
2. Select the group in the result list and run **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Edit a group's master data.
4. Save the changes.

Detailed information about this topic

- [LDAP Group Master Data](#) on page 99
- [Assigning LDAP Groups to LDAP User Accounts and LDAP Computers](#) on page 101

LDAP Group Master Data

Enter the following master data:

Table 41: General Master Data

Property	Description
Distinguished name	Distinguished name of the group. The distinguished name is determined by template from the name of the group and the container and cannot be edited.

Property	Description
Name	Group identifier
Display name	The display name is used to display the group in the One Identity Manager tools user interface.
Domain	Domain in which to create the group.
Container	Container in which to create the group.
Administrator	The group administrator.
Service item	Service item data for requesting the group through the IT Shop.
Business unit	Business unit to which the group is assigned.
See Also	Link to another LDAP object.
Structural object class	Structural object class representing the object type. By default, containers in One Identity Manager are added with the object class "GROUPOFNAMES".
Object class	List of classes defining the attributes for this object. By default, containers in One Identity Manager are added with the object class "GROUPOFNAMES". However, you can add object classes and auxiliary classes in the input field that are used by other LDAP and X.500 directory services.
Risk index	<p>Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set.</p> <p>For more detailed information about risk assessment, see the One Identity Manager Risk Assessment Administration Guide.</p>
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Use this menu to allocate one or more categories to the group.
Description	Spare text box for additional explanation.
Condition	LDAP filter for finding memberships in a dynamic groups.
Dynamic group	Specifies whether this is a dynamic group.
IT Shop	Specifies whether the group can be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted through a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted

Property	Description
	through a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.

Related Topics

- [LDAP Group Inheritance Based on Categories](#) on page 110
- For more detailed information about preparing groups for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning LDAP Groups to LDAP User Accounts and LDAP Computers

You can assign groups directly and indirectly to user account, workdesks and devices. Employees (workdesks, devices) and groups are grouped into hierarchical roles in the case of indirect assignment. The number of groups assigned to an employee (workdesk or device) From the position within the hierarchy and is calculated from the position within the hierarchy and inheritance direction.

If you add an employee to roles and that employee owns a user account, the user account is added to the group. Prerequisites for indirect assignment of employees to user accounts are:

- Assignment of employees and groups is permitted for role classes (department, cost center, location or business role).
- The user accounts are marked with the option **Groups can be inherited**.

If you add a device to roles, the computer, which references the device, is added to the group. Prerequisites for indirect assignment to computers are:

- Assignment of devices and groups is permitted for role classes (department, cost center, location or business role).
- The computer is connected to a device labeled as PC or server.
- The configuration parameter "TargetSystem\LDAP\HardwareInGroupFromOrg" is set.

If a device owns a workdesk and you add the workdesk to roles, the computer, which references this device, is also added to all groups of the workdesk's roles. Prerequisites for indirect assignment to computers through workdesks are:

- Assignment of workdesks and groups is permitted for role classes (department, cost center, location or business role).
- The computer is connected to a device labeled as PC or server. This device owns a workdesk.

Furthermore, groups can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that groups can be assigned through IT Shop requests. All groups assigned to this shop can be requested by the customers. Requested groups are assigned to the employees after approval is granted.

Detailed information about this topic

- [Assigning LDAP Groups to Departments, Cost Centers and Locations](#) on page 102
- [Assigning LDAP Groups to Business Roles](#) on page 103
- [Assigning LDAP User Accounts directly to an LDAP Group](#) on page 104
- [Assigning LDAP Computers Directly to an LDAP Group](#) on page 105
- [Adding LDAP Groups to System Roles](#) on page 105
- [Adding LDAP Groups to the IT Shop](#) on page 106
- One Identity Manager Identity Management Base Module Administration Guide

Assigning LDAP Groups to Departments, Cost Centers and Locations

Assign the group to departments, cost centers and locations so that the group can be assigned to user accounts, contacts and computers through these organizations.

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

1. Select the category **LDAP | Groups**.
 2. Select the group in the result list.
 3. Select **Assign organizations**.
 4. Assign organizations in **Add assignments**.
 - Assign departments on the **Departments** tab.
 - Assign locations on the **Locations** tab.
 - Assign cost centers on the **Cost center** tab.
- OR -
- Remove the organizations from **Remove assignments**.
5. Save the changes.

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

1. Select the category **Organizations | Departments**.
- OR -
- Select the category **Organizations | Cost centers**.

- OR -

Select the category **Organizations | Locations**.

2. Select the department, cost center or location in the result list.
3. Select **Assign LDAP groups**.
4. Assign groups in **Add assignments**.

- OR -

Remove assignments to groups in **Remove assignments**.

5. Save the changes.

Related Topics

- [Assigning LDAP Groups to Business Roles](#) on page 103
- [Assigning LDAP User Accounts directly to an LDAP Group](#) on page 104
- [Assigning LDAP Computers Directly to an LDAP Group](#) on page 105
- [Adding LDAP Groups to System Roles](#) on page 105
- [Adding LDAP Groups to the IT Shop](#) on page 106
- [One Identity Manager Users for Managing an LDAP](#) on page 8

Assigning LDAP Groups to Business Roles

Installed Modules: Business Roles Module

Assign the group to business roles so that it is assigned to user accounts, contacts and computers through this business role.

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

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.
- OR -
Remove business roles from **Remove assignments**.
5. Save the changes.

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

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign LDAP groups**.

4. Assign groups in **Add assignments**.
- OR -
Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning LDAP Groups to Departments, Cost Centers and Locations](#) on page 102
- [Assigning LDAP User Accounts directly to an LDAP Group](#) on page 104
- [Assigning LDAP Computers Directly to an LDAP Group](#) on page 105
- [Adding LDAP Groups to System Roles](#) on page 105
- [Adding LDAP Groups to the IT Shop](#) on page 106
- [One Identity Manager Users for Managing an LDAP](#) on page 8

Assigning LDAP User Accounts directly to an LDAP Group

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is carried out by allocating the employee and groups in company structures, like departments, cost centers, locations or business roles. If the employee has a user account in LDAP, the groups in the role are inherited by this user account.

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

NOTE: User accounts cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

To assign a group directly to user accounts

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.
- OR -
Remove user accounts from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning LDAP Groups Directly to LDAP User Accounts](#) on page 90
- [Assigning LDAP Groups to Departments, Cost Centers and Locations](#) on page 102

- [Assigning LDAP Groups to Business Roles](#) on page 103
- [Assigning LDAP Computers Directly to an LDAP Group](#) on page 105
- [Adding LDAP Groups to System Roles](#) on page 105
- [Adding LDAP Groups to the IT Shop](#) on page 106

Assigning LDAP Computers Directly to an LDAP Group

Groups can be assigned directly or indirectly to a computer. Indirect assignment is carried out by allocating the device with which a computer is connected and groups to company structures, like departments, cost centers, locations or business roles.

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

NOTE: Computers cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

To assign a group directly to computers

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select the **Assign computers** in the task view.
4. Assign computers in **Add assignments**.
- OR -
Remove the computers in **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning LDAP Computers directly to LDAP Groups](#) on page 119
- [Assigning LDAP Groups to Departments, Cost Centers and Locations](#) on page 102
- [Assigning LDAP Groups to Business Roles](#) on page 103
- [Assigning LDAP User Accounts directly to an LDAP Group](#) on page 104
- [Adding LDAP Groups to System Roles](#) on page 105
- [Adding LDAP Groups to the IT Shop](#) on page 106

Adding LDAP Groups to System Roles

Installed Modules: System Roles Module

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

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

To assign a group to system roles

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.
- OR -
Remove system roles from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning LDAP Groups to Departments, Cost Centers and Locations](#) on page 102
- [Assigning LDAP Groups to Business Roles](#) on page 103
- [Assigning LDAP User Accounts directly to an LDAP Group](#) on page 104
- [Assigning LDAP Computers Directly to an LDAP Group](#) on page 105
- [Adding LDAP Groups to the IT Shop](#) on page 106

Adding LDAP Groups to the IT Shop

Once a group has been assigned to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- The group must be labeled with the option **IT Shop**.
- The group must be assigned to a service item.
- The group must be labeled with the option **Only use in IT Shop** if the group can only be assigned to employees through IT Shop requests. Direct assignment to hierarchical roles or user accounts is no longer permitted.

- NOTE:** IT Shop administrators can assign groups to IT Shop shelves in the case of role-based login. Target system administrators are not authorized to add groups in the IT Shop.

To add a group to the IT Shop

1. Select the category **LDAP | Groups** (non role-based login).
- OR -
Select the category **Entitlements | LDAP groups** ((role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the group to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove a group from individual IT Shop shelves.

1. Select the category **LDAP | Groups** (non role-based login).
- OR -
Select the category **Entitlements | LDAP groups** ((role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the group from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove a group from all IT Shop shelves.

1. Select the category **LDAP | Groups** (non role-based login).
- OR -
Select the category **Entitlements | LDAP groups** ((role-based login).
2. Select the group in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

This removes the group from all One Identity Manager Service shelves. All requests and assignment requests with this group are canceled in the process.

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related Topics

- [LDAP Group Master Data](#) on page 99
- [Assigning LDAP Groups to Departments, Cost Centers and Locations](#) on page 102
- [Assigning LDAP Groups to Business Roles](#) on page 103
- [Assigning LDAP User Accounts directly to an LDAP Group](#) on page 104

- [Assigning LDAP Computers Directly to an LDAP Group](#) on page 105
- [Adding LDAP Groups to System Roles](#) on page 105

Additional Tasks for Managing LDAP Groups

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

Overview of LDAP Groups

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

To obtain an overview of a group

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **LDAP group overview** in the task view.

Effectiveness of Group Memberships

Table 42: Configuration Parameter for Conditional Inheritance

Configuration parameter	Active Meaning
QER\Structures\Inherit\GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. The database has to be recompiled after changes have been made to the parameter.

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

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

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.
- One Identity Manager does not check whether membership of an excluded group is permitted in another group.

The effect of the assignments is mapped in the tables LDAPAccountInLDAPGroup and BaseTreeHasLDAPGroup through the column XIsInEffect.

Example of the effect of group memberships

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

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

By using suitable controls, you want to prevent an employee from being able to trigger a request and to pay invoices. That means, groups A, B and C are mutually exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 43: Specifying excluded groups (table LDAPGroupExclusion)

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

Table 44: Effective Assignments

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

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

The groups A and C are in effect for Jenny Basset because the groups are not defined as mutually exclusive. That means that the employee is authorized to trigger request and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 45: Excluded groups and effective assignments

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

Prerequisites

- The configuration parameter "QER\Inherite\GroupExclusion" is enabled.
- Mutually exclusive groups belong to the same domain

To exclude a group

1. Select the category **LDAP | Groups**.
2. Select a group in the result list.
3. Select **Exclude groups** in the task view.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.
- OR -
Remove the conflicting groups that are no longer mutually exclusive in **Remove assignments**.
5. Save the changes.

LDAP Group Inheritance Based on Categories

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

roles, subscriptions and disabled service plans in the . Each table contains the category items "Position1" to "Position31".

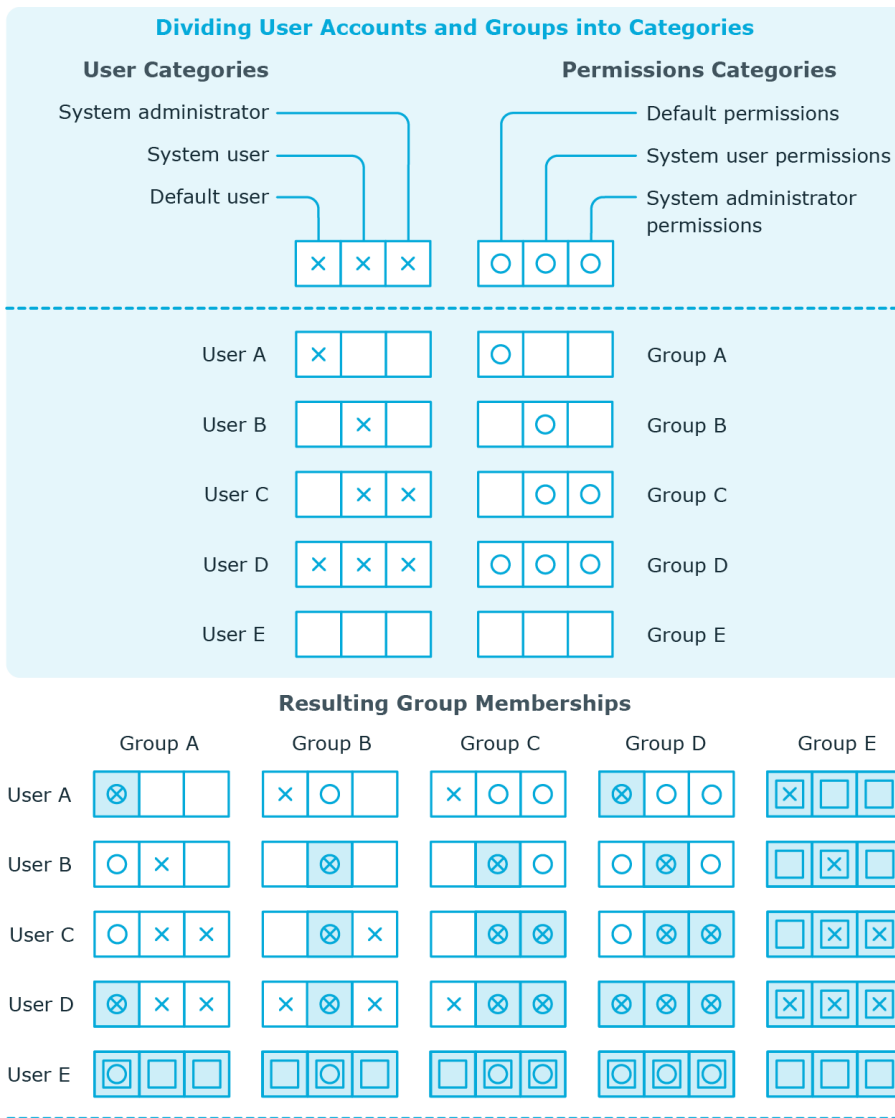
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the user account is not put into categories.

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

Table 46: Category Examples

Category Position	Categories for User Accounts	Categories for Groups
1	Default user	Default permissions
2	System user	System user permissions
3	System administrator	System administrator permissions

Figure 2: Example of inheriting through categories.



Key:

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

To use inheritance through categories

- Define categories in the domain.
- Assign categories to user accounts and contacts through their master data.
- Assign categories to groups through their master data.

Related Topics

- [Specifying Categories for Inheriting LDAP Groups](#) on page 76
- [General Master Data for an LDAP User Account](#) on page 83
- [LDAP Group Master Data](#) on page 99

Assigning Extended Properties to an LDAP Group

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


To specify extended properties for a group

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.
- OR -
Remove extended properties from **Remove assignments**.
5. Save the changes.

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

Deleting LDAP Groups

To delete a group


1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Delete the group using .
4. Confirm the security prompt with **Yes**.

The group is deleted completely from the One Identity Manager database and from LDAP.

LDAP Container Structures

LDAP containers are represented by a hierarchical tree structure. Containers are often used to display organizational units such as branch offices or departments, to organize LDAP directory objects such as users, groups and computers logically and therefore to ease the burden of object administration. LDAP directory containers are loaded by synchronization with the One Identity Manager database.

To edit container master data

1. Select the category **LDAP | Container**.
2. Select the container in the result list and run **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Edit the container's master data.
4. Save the changes.


Detailed information about this topic

- [General Master Data for LDAP Containers](#) on page 114
- [Contact Data for LDAP Containers](#) on page 116
- [Address Information for LDAP Containers](#) on page 116

General Master Data for LDAP Containers

Enter the following data on the **General** tab:

Table 47: Master Data for a Container

Property	Description
Display name	Container's display name.
Domain	Container domain
Parent container	Parent container for mapping a hierarchical container structure. The distinguished name is automatically updated using templates.
Name	Container name.
Distinguished name	Container's distinguished name. The distinguished name for the new container is made up from the container name, the object class, the parent container and the domain and cannot be modified.
Business unit	Business unit to which the container is assigned.
Link (named URI format)	Specifies links in Uniform Resource Identifier (URI) Format; made up of a name and a URL.
Search mask	Search mask for another LDAP object.
See also	Link to another LDAP object.
State	State.
Structural object class	Structural object class representing the object type. By default, containers in One Identity Manager are added with the object class "ORGANIZATIONALUNIT".
Object class	List of classes defining the attributes for this object. By default, containers in One Identity Manager are added with the object class "ORGANIZATIONALUNIT". However, you can add object classes and auxiliary classes in the input field that are used by other LDAP and X.500 directory services.
Description	Spare text box for additional explanation.
Target system manager	<p>Application role in which target system managers are specified for the container. Target system managers only edit container objects that are assigned to them. Each container can have a different target system manager assigned to it.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this container. Use the  button to add a new application role.</p>

Related Topics

- [Target System Managers](#) on page 70

Contact Data for LDAP Containers

Enter data for making contact on the **Contact data** tab.

Table 48: Contact Data

Property	Description
Fax	Fax number.
Internationale ISDN no.	Internationale ISDN number.
Phone	Telephone number.
Teletex ID	Teletex terminal identification.
Telex	Telex number.
Password	Password.
Password confirmation	Reconfirm password.

Address Information for LDAP Containers

Enter the following address data for contacting the employee on the **Address data** tab.

Table 49: Address data

Property	Description
Building name	Name of the building.
Location ID	Location identifier (country and city) for telegram services.
Office	Office.
Address	Postal address.
Zip code	Zip code. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Mailbox	Mailbox. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Preferred delivery	Preferred method of delivery.

Property	Description
-----------------	--------------------

Registered address	Postal address.
--------------------	-----------------


Street	Street or road. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
--------	---

X.121 address	Addressing as X.121 address.
---------------	------------------------------

LDAP Computers

The One Identity Manager data model is designed to manage administration of LDAP directory computers and servers. To synchronize this data with LDAP, customize the synchronization project accordingly.

To edit computer master data

1. Select the category **LDAP | Computers**.
2. Select the computer in the result list and run **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Edit the computer's master data.
4. Save the changes.

Detailed information about this topic

- [Master Data for an LDAP Computer](#) on page 118


Related Topics

- One Identity Manager Target System Synchronization Reference Guide

Master Data for an LDAP Computer

Enter the following data for a computer.

Table 50: Computer Master Data

Property	Description
Device	The computer is connected to this device. Specify a new device using the  button next to the menu.

Property	Description
Name	Computer identifier
Domain	Domain in which to create the computer.
Container	Container in which to create the computer. The distinguished name of the computer is determined by a template when the container is selected.
Structural object class	Structural object class representing the object type.
Object class	List of classes defining the attributes for this object. However, you can add object classes and auxiliary classes in the input field that are used by other LDAP and X.500 directory services.

Related Topics

- [One Identity Manager Identity Management Base Module Administration Guide](#)

Assigning LDAP Computers directly to LDAP Groups

Groups can be assigned directly or indirectly to a computer. Indirect assignment is carried out by allocating the device with which a computer is connected and groups to company structures, like departments, cost centers, locations or business roles.

To react quickly to special requests, you can assign groups directly to a computer.

NOTE: Computers cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

To assign a computer directly to groups

1. Select the category **LDAP | Computers**.
2. Select the computer in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**.
- OR -
Remove groups from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning LDAP Groups to LDAP User Accounts and LDAP Computers](#) on page 101

Reports about LDAP Objects

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

NOTE: Other sections may be available depending on the which modules are installed.

Table 51: Reports for the Target System

Report	Description
Overview of all assignments (domain)	This report finds all roles containing employees with at least one user account in the selected domain.
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 (group)	This report finds all roles containing employees with the selected group.
Show orphaned user accounts	This report shows all user accounts in the domain, which are not assigned to an employee. The report contains group memberships and risk assessment.
Show employees with multiple user accounts	This report shows all employees with more than one user account in the domain. The report is a risk assessment.
Show unused user accounts	This report shows all user accounts in the domain, which have not been used in the last few months. The report contains group memberships and risk assessment.
Show entitlement drifts	This report shows all groups in the domain that are the result of manual operations in the target system rather than using the One Identity Manager.
Show user accounts with an above average number of system entitlements	This report contains all user accounts in the domain with an above average number of group memberships.
LDAP user account and	This report contains a summary of user account and group

Report	Description
group administration	distribution in all domains. You can find this report in the category My One Identity Manager .
Data quality summary for LDAP user accounts	This report contains different evaluations of user account data quality in all domains. You can find this report in the category My One Identity Manager .

Related Topics

- [Overview of all Assignments](#) on page 121


Overview of all Assignments

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

Example

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

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Use the  **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are employees with the selected base object.

All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The

meaning of the report control elements is explained in a separate legend. In the report's toolbar, click **i** to open the legend.

- Double-click a control to show all child roles belonging to the selected role.
- By clicking the **▼** button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to **▼** to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 3: Toolbar for Report "Overview of all assignments"

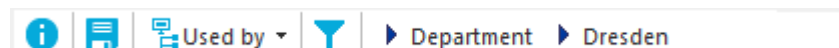


Table 52: Meaning of Icons in the Report Toolbar

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

Appendix: Configuration Parameters for Managing LDAP

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

Table 53: Configuration Parameter for LDAP Directory Synchronization

Configuration Parameter	Description
TargetSystem\LDAP	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system LDAP. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\LDAP\Accounts	This configuration parameter permits configuration of user account data.
TargetSystem\LDAP\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the

Configuration Parameter	Description
	address stored in the configuration parameter "TargetSystem\LDAP\DefaultAddresses".
TargetSystem\LDAP\Accounts InitialRandomPassword\SendTo\ MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".
TargetSystem\LDAP\Accounts InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\LDAP\Accounts MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. Use the mail template "Employee - new user account with default properties created".
TargetSystem\LDAP\Accounts PrivilegedAccount	This configuration parameter allows configuration of settings for privileged LDAP user accounts.
TargetSystem\LDAP\Accounts PrivilegedAccount\UserID_Postfix	This configuration parameter contains the postfix for formatting login names for privileged user accounts.
TargetSystem\LDAP\Accounts PrivilegedAccount\UserID_Prefix	This configuration parameter contains the prefix for formatting login names for privileged user accounts.
TargetSystem\LDAP\Authentication	The configuration parameter allows configuration of the LDAP authentication module.
TargetSystem\LDAP\Authentication\Authentication	The configuration parameter specified the authentication mechanism. Permitted values are "Secure", "Encryption", "SecureSocketsLayer", "ReadOnlyServer", "Anonymous",

Configuration Parameter	Description
	"FastBind", "Signing", "Sealing", "Delegation" and "ServerBind". The value can be combined with commas (,). For more information about authentication types, see the MSDN Library . Default is ServerBind.
TargetSystem\LDAP\Authentication\Port	LDAP server's port. Default is port 389.
TargetSystem\LDAP\Authentication\RootDN	The configuration parameter contains the root domain's distinguished name. Syntax: dc=MyDomain
TargetSystem\LDAP\Authentication\Server	The configuration parameter contains the name of the LDAP server.
TargetSystem\LDAP\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem\LDAP\HardwareInGroupFromOrg	This configuration parameter specifies whether computers are added in groups based on group assignment to roles.
TargetSystem\LDAP\MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem\LDAP\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\LDAP\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable

Configuration Parameter	Description
TargetSystem\LDAP\ PersonAutoFullSync	<p data-bbox="887 266 1369 329">user accounts. User accounts do not obtain an account definition.</p> <p data-bbox="887 353 1369 517">This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.</p>

Appendix: Default Project Template for LDAP

A default project template ensures that all required information is added in the One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

Detailed information about this topic

- [OpenDJ Basic Template](#) on page 127
- [Default Project Template for Active Directory Lightweight Directory Services](#) on page 128

OpenDJ Basic Template

This project template is based on OpenDJ. The template uses mappings for the following schema types.

Table 54: Mapping schema types to tables in the One Identity Manager schema.

Schema type in LDAP	Table in the One Identity Manager schema
domain	LDAPDomain
organization	LDAPContainer
organizationalUnit	LDAPContainer
locality	LDAPContainer

Schema type in LDAP	Table in the One Identity Manager schema
container	LDAPContainer
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount

Default Project Template for Active Directory Lightweight Directory Services

This project template is based on Active Directory Lightweight Directory Services (AD LDS). The template uses mappings for the following schema types.

Table 55: Mapping schema types to tables in the One Identity Manager schema.

Schema type in AD LDS	Table in the One Identity Manager schema
Container	LDAPContainer
country	LDAPContainer
domainDNS	LDAPContainer
foreignSecurityPrincipal	LDAPAccount
group	LDAPGroup
groupOfNames	LDAPGroup
inetOrgPerson	LDAPAccount
organization	LDAPContainer
organizationalUnit	LDAPContainer
user	LDAPAccount
userProxy	LDAPAccount
userProxyFull	LDAPAccount

Appendix: Authentication Modules for Logging into the One Identity Manager

The following authentication modules are available for logging into One Identity Manager in once this module has been installed.

LDAP user account (dynamic)

Login Data	Login name, identifier, distinguished name or user ID of an LDAP user account. LDAP user account's password.
Prerequisites	The employee exists in the One Identity Manager database. The LDAP user account exists in the One Identity Manager database and the employee is entered in the user account's master data. The configuration data for dynamically determining the system user is defined in the application. Thus, an employee can, for example, be assigned a system user dynamically depending on their department membership.
Set as default	No
Single Sign-On	No
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	If you log in using a login name, identifier or user ID, the corresponding user account is determined in the One Identity Manager database through the container's domain. Logging in with a distinguished name is done

directly. One Identity Manager determines which employee is assigned to the LDAP user account.

If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication.

- If this configuration parameter is set, the employee's main identity is used for authentication.
- If the parameter is not set, the employee's subidentity is used for authentication.

The application configuration data is used to determine a system user, which is automatically assigned to the employee. The user interface and write permissions are loaded through the system user that is dynamically assigned to the logged in employee.

Data modifications are attributed to the current user account.

Modify the following configuration parameters in the Designer to implement the authentication module.

Table 56: Configuration Parameters for the Authentication Module

Configuration parameter	Meaning
TargetSystem\LDAP\Authentication	The configuration parameter allows configuration of the LDAP authentication module.
TargetSystem\LDAP\Authentication\Authentication	The configuration parameter specified the authentication mechanism. Permitted values are "Secure", "Encryption", "SecureSocketsLayer", "ReadonlyServer", "Anonymous", "FastBind", "Signing", "Sealing", "Delegation" and "ServerBind". The value can be combined with commas (,). For more information about authentication types, see the MSDN Library . Default is ServerBind.
TargetSystem\LDAP\Authentication\Port	LDAP server's port. Default is port 389.
TargetSystem\LDAP\Authentication\RootDN	The configuration parameter contains the root domain's distinguished name. Syntax:

Configuration parameter	Meaning
	dc=MyDomain
TargetSystem\LDAP\Authentication\Server	The configuration parameter contains the name of the LDAP server.

LDAP user account (role based)

Login Data	<p>Login name, identifier, distinguished name or user ID of an LDAP user account.</p> <p>LDAP user account's password.</p>
Prerequisites	<p>The employee exists in the One Identity Manager database.</p> <p>The employee is assigned at least one application role.</p> <p>The LDAP user account exists in the One Identity Manager database and the employee is entered in the user account's master data.</p> <p>The configuration data for dynamically determining the system user is defined in the application. Thus, an employee can, for example, be assigned a system user dynamically depending on their department membership.</p>
Set as default	No
Single Sign-On	No
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	<p>If you log in using a login name, identifier or user ID, the corresponding user account is determined in the One Identity Manager database through the container's domain. Logging in with a distinguished name is done directly. One Identity Manager determines which employee is assigned to the LDAP user account.</p> <p>If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication.</p> <ul style="list-style-type: none"> • If this configuration parameter is set, the employee's main identity is used for authentication. • If the parameter is not set, the employee's subidentity is used for authentication. <p>A dynamic system user determined from the employee's application roles.</p>

The user interface and the write permissions are loaded through this system user.

Data modifications are attributed to the current user account.

Modify the following configuration parameters in the Designer to implement the authentication module.

Table 57: Configuration Parameters for the Authentication Module

Configuration parameter	Meaning
TargetSystem\LDAP\Authentication	The configuration parameter allows configuration of the LDAP authentication module.
TargetSystem\LDAP\Authentication\Authentication	The configuration parameter specified the authentication mechanism. Permitted values are "Secure", "Encryption", "SecureSocketsLayer", "ReadOnlyServer", "Anonymous", "FastBind", "Signing", "Sealing", "Delegation" and "ServerBind". The value can be combined with commas (,). For more information about authentication types, see the MSDN Library . Default is ServerBind.
TargetSystem\LDAP\Authentication\Port	LDAP server's port. Default is port 389.
TargetSystem\LDAP\Authentication\RootDN	The configuration parameter contains the root domain's distinguished name. Syntax: dc=MyDomain
TargetSystem\LDAP\Authentication\Server	The configuration parameter contains the name of the LDAP server.

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

Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

Technical support resources

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

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

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

A

- account definition 40
 - add to IT Shop 54
 - assign automatically 52
 - assign to all employees 52
 - assign to business role 51
 - assign to cost center 51
 - assign to department 51
 - assign to employee 50, 53
 - assign to LDAP domain 55
 - assign to location 51
 - assign to system roles 53
 - create 41
 - delete 56
 - IT operating data 46-47
 - manage level 43
- Active Directory domain
 - report 120
- architecture overview 7
- authentication module
 - LDAP user account (dynamic) 129
 - LDAP user account (role based) 129

C

- calculation schedule
 - disable 37
- configuration parameter 123

D

- direction of synchronization
 - direction target system 18, 31

in direction of 18

E

- email notification 68
- employee assignment
 - automatic 92
 - manual 95
 - remove 95
 - search criteria 94
 - table column 94
- exclusion definition 108

G

- group
 - effective 108
 - exclusion 108

I

- IT operating data
 - change 49
- IT Shop shelf
 - assign account definition 54

J

- Job server
 - edit 14

L

LDAP computer

- assign group 105, 119
- computer name 118
- container 118
- device 118
- domain 118
- edit 118
- object class 118

LDAP container

- address 116
- business unit 114
- contact 116
- domain 114
- edit 114
- manage 114
- object class 114
- target system manager 70, 114

LDAP domain

- account definition 73
- account definition (initial) 55
- application roles 8
- category 76, 110
- domain name 75
- edit 73
- employee assignment 94
- object class 75
- overview of all assignments 121
- set up 73
- synchronization 73
- system type 73
- target system manager 8, 70, 73

LDAP group

- add to 106

- add to system role 105
- administrator 99
- assign computer 101, 105, 119
- assign extended properties 113
- assign to business role 103
- assign to cost center 102
- assign to department 102
- assign to location 102
- assign user account 90, 101, 104
- business unit 99
- category 99, 110
- container 99
- delete 113
- domain 99
- object class 99
- risk index 99
- service item 99
- set up 99

LDAP user account

- account definition 55, 83
- account manager 88
- address 87
- administrative user account 79
- assign employee 78, 82-83, 92
- assign extended properties 91
- assign group 90, 104
- business unit 88
- category 83, 110
- company 88
- container 83
- default PC 89
- default user accounts 79
- delete 97
- department 88
- disable 83, 96

- domain 83
- email address 87
- employee 83
- employee number 88
- identity 79, 83
- image 87
- inherit application 83
- inherit group 83
- location 88
- lock 96-97
- login name 83
- manage 78
- manage level 83, 90
- object class 83
- password
 - initial 66
- phone 87
- privileged user account 79, 83
- restore 97
- risk index 83
- set up 82
- title 88
- type 79
- user ID 89
- wizard 88

login data 68

M

- membership
 - modify provisioning 36

N

- notification 68

O

- object
 - delete immediately 34
 - outstanding 34
 - publish 34
- One Identity Manager
 - administrator 8
 - target system administrator 8
 - target system manager 8, 70, 114
 - user 8
- outstanding object 34

P

- password
 - initial 68
- password policy 57
 - assign 65
 - character sets 60
 - check password 64
 - conversion script 61, 63
 - default policy 59, 65
 - display name 59
 - edit 59
 - error message 59
 - excluded list 64
 - failed logins 60
 - generate password 64
 - initial password 60
 - name components 60
 - password age 60
 - password cycle 60
 - password length 60
 - password strength 60

- predefined 58
- test script 61
- project template
 - Active Directory Lightweight Directory Services 128
 - OpenDJ 127
- provisioning
 - members list 36

R

- revision filter 33

S

- schema
 - changes 32
 - shrink 32
 - update 32
- synchronization
 - accelerate 33
 - authorizations 12
 - base object
 - create 31
 - configure 18, 30
 - connection parameter 18, 30-31
 - different domains 31
 - extended schema 31
 - prevent 37
 - scope 30
 - set up 11
 - start 18
 - synchronization project
 - create 18
 - target system schema 31
 - user 12

- variable 30
- variable set 31
- workflow 18, 31
- synchronization analysis report 37
- synchronization configuration
 - customize 30-31
- synchronization log 29
- synchronization project
 - create 18
 - disable 37
 - edit 76
 - project template 127
- synchronization server
 - configure 14
 - install 14
 - Job server 14
- synchronization workflow
 - create 18, 31

T

- target system synchronization 34
- template
 - IT operating data, modify 49

U

- user account
 - administrative user account 79
 - apply template 49
 - default user accounts 79
 - identity 79
 - password
 - notification 68
 - privileged user account 79
 - type 79