ONE IDENTITY™

One Identity Manager 8.1.3

Administration Guide for Connecting to LDAP

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

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

One Identity Manager Administration Guide for Connecting to LDAP
Updated - June 2020
Version - 8.1.3

Contents

1

Managing LDAP environments

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

The default One Identity Manager installation concentrates on 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 synchronization 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 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 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

In One Identity Manager, the following servers play a role in managing LDAP:

- LDAP server

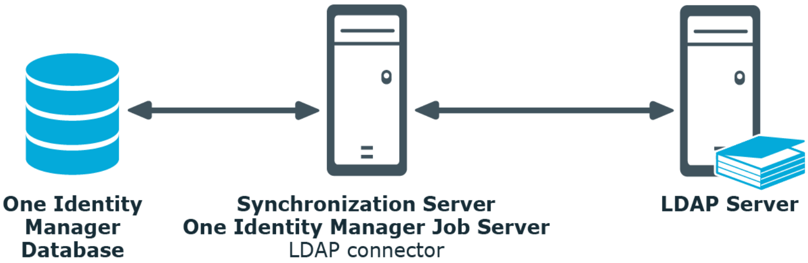
  The LDAP server with the LDAP directory. This server is a selected live server with a good network connection to the synchronization server. The synchronization server connects to this server in order to access the LDAP objects.

- Synchronization server

  Synchronization server for synchronizing One Identity Manager data with LDAP. The One Identity Manager Service with the LDAP connector is installed on this server. 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 Database
Synchronization Server
One Identity Manager Job Server
LDAP connector
LDAP Server

One Identity Manager users for managing LDAP

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

Table 1: Users

User	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other employees to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | LDAP** or a child application role. Users with this application role: • Assume administrative tasks for the target system.

User	Tasks
	• Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: • Assign groups to IT Shop structures.
Administrators for organizations	Administrators must be assigned to the **Identity Management | Organizations | Administrators** application role. Users with this application role: • Assign groups to departments, cost centers, and locations.
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role.

User	Tasks
	Users with this application role: - Assign groups to business roles.

Synchronizing LDAP directories

One Identity Manager supports synchronization of LDAP version 3 confirm directory servers. The LDAP connector requires the directory server to be RFC conform. Specifically, to conform to the RFC 4514 standard (String Representation of Distinguished Names) and RFC 4512 (Directory Information Models).

> NOTE: On certain LDAP systems, write operations on entries can cause errors if they are not-RFC compliance.

One Identity Manager is responsible for synchronizing data between the One Identity Manager Service database and the LDAP directory.

This sections explains how to:

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

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

Detailed information about this topic

- Setting up initial LDAP directory synchronization on page 13
- Customizing the synchronization configuration on page 30
- Executing synchronization on page 41
- Troubleshooting on page 48

Setting up initial LDAP directory synchronization

The Synchronization Editor provides a project template that can be used to set up the synchronization of user accounts and permissions for the LDAP environment. You use these project templates to create synchronization projects with which you import the data from an LDAP directory into your One Identity Manager database. In addition, the required processes are created that are used for the provisioning of changes to target system objects from the One Identity Manager database into the target system.

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

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

1. Prepare a user account with sufficient permissions for synchronization.
2. One Identity Manager components for managing LDAP environments are available if the **TargetSystem | LDAP** configuration parameter is enabled.
    - In the Designer, check if the configuration parameter is set. 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 a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with LDAP on page 14
- Special cases for synchronizing Active Directory Lightweight Directory Services on page 15
- Special cases for synchronizing Oracle Directory Server Enterprise Edition on page 16
- Setting up the LDAP synchronization server on page 17
- Creating a synchronization project for initial synchronization of an LDAP domain on page 20
- Configuration parameters for managing an LDAP environment on page 144
- Default project template for LDAP on page 147
- Generic LDAP connector settings on page 149

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	The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires access permissions to the internal web service. NOTE: If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • `%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 **Synchronization** default system user is provided to execute synchronization with an application server.

Related topics

- Special cases for synchronizing Active Directory Lightweight Directory Services on page 15

- Special cases for synchronizing Oracle Directory Server Enterprise Edition on page 16

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 authentication, 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 **Administrators** group 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 that resides on a local computer or in an Active Directory domain.

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

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

- **Negotiate** must be used as the 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 must 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 **Administrators** group 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 a login password.

Special cases for synchronizing Oracle Directory Server Enterprise Edition

Oracle Directory Server Enterprise Edition (DSEE) does not support searching by page. Because of this, the connector must be able to load a schema type’s list of synchronization objects, all at once. If using a conventional Oracle DSEE, LDAP user, limits on the server side are reached in large directories that cause this type of load action to fail.

Possible message:

```
Size Limit exceeded

Time Limit exceeded
```

There, limits for the synchronization user are removed. To achieve this, you must set the following LDAP attributes on the synchronization user in the directory:

- `nsTimeLimit`: Maximum timeout for a search query in seconds. This value can be increased or decreased depending on the size of the directory.
  (Recommendation: **7200**.)
- `nsSizeLimit`: Maximum number of search results for a search query. This value can be increased or decreased depending on the size of the directory.
  (Recommendation: **500000**.)

Setting up the LDAP synchronization server

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

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

Detailed information about this topic

- System requirements for the LDAP synchronization server on page 17
- Installing the One Identity Manager Service with an LDAP connector on page 17

System requirements for the LDAP 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

  The following versions are supported:

  - Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 or later

  NOTE: Take the target system manufacturer's recommendations into account.

Installing the One Identity Manager Service with an LDAP connector

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 Identity Manager.

Table 3: Properties of the Job server

Property	Value
Server function	LDAP connector
Machine role	Server | Jobserver | LDAP directories

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

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

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

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

NOTE: The program performs a 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 remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

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

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

       - OR -

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

b. Enter the following data for the Job server.

    - **Server**: Name of the Job server.
    - **Queue**: Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this unique queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
    - **Full server name**: Full server name in accordance with DNS syntax.

      Syntax:

      `<Name of servers>.<Fully qualified domain name>`

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

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

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

   - For a direct connection to the database:
     a. Select **Process collection | sqlprovider**.
     b. Click the **Connection parameter** entry, then click the **Edit** button.
     c. Enter the connection data for the One Identity Manager database.
   - For a connection to the application server:
     a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
     b. Click the **Connection parameter** entry, then click the **Edit** button.
     c. Enter the connection data for the application server.
     d. Click the **Authentication data** entry and click the **Edit** button.
     e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files.
10. On the **Select private key file** page, select the file with the private key.

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

11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Name or IP address of the server that the service is installed and started on.
    - **Service account**: User account data for the One Identity Manager Service.
        - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.
        - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.
    - **Installation account**: Data for the administrative user account to install the service.
        - To use the current user's account, set the **Current user** option.
        - To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.
    - To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.
12. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.
13. Click **Finish** on the last page of the Server Installer.

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

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 environment. The following describes the steps for initial configuration of a synchronization project. For more detailed information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Related topics

- Information required for setting up a synchronization project on page 21
- Creating an initial synchronization project for an LDAP domain with the generic LDAP connector on page 23

Information required for setting up a synchronization project

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

Table 4: Information required for setting up a synchronization project

Data	Explanation
LDAP server's DNS name	IP address or full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects. Syntax: `<Name of servers>.<Fully qualified domain name>`
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 server	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 14.
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 Identity Manager. Use the following properties when you set up the Job server.

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td></td><td>

Table 5: Additional properties for the Job server

<table>
<tr><th>Property</th><th>Value</th></tr>
<tr><td>Server function</td><td>LDAP connector</td></tr>
<tr><td>Machine role</td><td>Server | Jobserver | LDAP directories</td></tr>
</table>

For more information, see Setting up the LDAP synchronization server on page 17.

</td></tr>
<tr><td>One Identity Manager database connection data</td><td>

- Database server
- Database
- SQL Server login and password
- Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

</td></tr>
<tr><td>Remote connection server</td><td>

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

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

Remote connection server configuration:

- One Identity Manager Service is started
- **RemoteConnectPlugin** is installed
- 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 as the synchronization server (with regard to the installed software and entitlements). 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*.

</td></tr>
</table>

Creating an initial synchronization project for an LDAP domain with the generic LDAP connector

> NOTE: The following sequence describes how to configure a synchronization project if the Synchronization Editor is both:
>
> - Executed in default mode
> - Started from the Launchpad
>
> If you execute the project wizard in expert mode or directly from the Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.

To set up an initial synchronization project for an LDAP domain

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

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

2. Select the **Target system type LDAP** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. On the **Choose target system** page, select the **LDAP connector**.
4. On the **System access** page, specify how One Identity Manager can access the target system.
   - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
   - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
5. Specify settings for the wizard using **Configure advanced settings (expert mode)** 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.
   - For customized LDAP systems, enable the option. You can set the following options for this case:
     - Definition of virtual classes for non-RFC compliant object mappings
     - Definition of auxiliary classes of **Auxiliary** type
     - Definition of system attributes for object identification, revision properties and additional operational attributes
     - Definition of additional attributes for supporting dynamic groups

For more information, see Advanced settings of a generic LDAP connector on page 34.

6. On the **Network** page, enter network settings for the LDAP server connection.
    a. In the **Host** pane, enter the connection settings for the LDAP server.
        - **Server**: IP address or full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects
        - **Port**: Communications port on the server. LDAP default communications port is 389.

    b. Click **Test**.

       The system tries to connect to the server.

    c. On the **Additional settings** pane, enter the additional settings for communication with the LDAP server.
        - **Protocol version**: Version of the LDAP protocol. The default value is **3**.
        - **No encryption**: No encryption is used.
        - **SSL/TLS encryption**: An SSL/TLS encrypted connection is established.
        - **Use StartTLS**: StartTLS is used.
7. Enter authentication data on the **Authentication** page.
    a. In the **Authentication method** pane, select the authentication type for the login to the target system.
        - **Authentication method**: Select the authentication type for logging in to the LDAP system. The following are permitted:
            - **Basic**: Uses default authentication.
            - **Negotiate**: Uses Negotiate authentication from Microsoft.
            - **Anonymous**: Establishes a connection without passing login credentials.
            - **Kerberos**: Uses Kerberos authentication.
            - **NTLM**: Uses Windows NT Challenge/Response (NTLM) authentication.

    b. Depending on the selected authentication method, additional information may be required. Enter this information under **Credentials**.
        - **User name**: Name of the user account for logging in to LDAP.
        - **Password**: Password for the user account.
        - **Enable sealing**: Sealing is enabled. Set this option if the selected authentication method supports sealing.
        - **Enable signing**: Signing is enabled. Set this option if the selected authentication method supports signing.

c. On the **Verify LDAP connection** pane, click **Test connection**.

   An attempt is made to log into the server.

8. The **LDAP server information** page displays the information about the LDAP schema.

9. On the **Search options** page, specify the search parameters for finding the LDAP objects to be loaded.

   Table 6: Find options

Property	Description
Base DN	Root entry for the search query, normally the LDAP domain.
Save LDAP schema in local cache	Specifies whether the LDAP schema should be kept in local cache. This accelerates synchronization and provisioning of LDAP objects. The cache is stored on the computer used to create the connection, under `%Appdata%\...\Local\One Identity\One Identity Manager\Cache\GenericLdapConnector`.
Request timeout (seconds)	Timeout for LDAP requests in seconds. Default: **3600**
Use paged search	Specifies whether LDAP objects are loaded by page. If you set this option, you include the page size.
Page size	Maximum number of objects to load per page. Default: **500**

10. On the **Modification capabilities** page, specify the kind of write operations supported by the LDAP server.

    - Enable the **Server supports renaming of entries** option if the LDAP server supports renaming of entries.
    - Enable the **Server supports moving of entries** option if the LDAP server supports moving of entries.

      NOTE: Some servers only support renaming of entries on leaf nodes. In this case, you will get an error message when trying to rename other nodes.
    - Enable the **Use DeleteTree control when deleting entries** option if you want the LDAP server to sent the **DeleteTree** control to delete entries with sub-entries during deletion.

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

    - **Password attribute**: An attribute that represents the password of a user account, for example, `userPassword`.
    - **Password change method**: A method you can use to change passwords.

Permitted values are:

- **Default**: Default method for changing the passwords. The password is written directly to the password attribute.
- **ADLDS**: A password change method used for systems that are based on Microsoft Active Directory Lightweight Directory Services (AD LDS).

12. You can save the connection data on the last page of the system connection wizard.
    - Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
    - Click **Finish**, to end the system connection wizard and return to the project wizard.
13. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

    > NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not shown if a synchronization project already exists.
14. 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.
15. Select a project template on the **Select project template** page to use for setting up the synchronization configuration.

Table 7: Standard project templates

Project template	Description
OpenDJ synchronisation	This project template is 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 synchronisation	This project template is based on Active Directory Lightweight Directory Services (AD LDS).

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

Table 8: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.

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

17. On the **Synchronization server** page, select a synchronization server to execute synchronization.

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

    a. Click + to add a new Job server.

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

    c. Click **OK**.

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

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

18. Enter the general setting for the synchronization project under **General**.

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

Table 9: General properties of the synchronization project

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: You cannot change the script language once the synchronization project has been saved. If you use a project template, the template's script language is used.
Description	Text field for additional explanation.

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

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

    The synchronization project is created, saved, and enabled immediately.

    > NOTE: If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.
    >
    > Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor‘s start page, click **Verify project**.

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

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

Related topics

- Information required for setting up a synchronization project on page 21
- Users and permissions for synchronizing with LDAP on page 14
- Special cases for synchronizing Active Directory Lightweight Directory Services on page 15
- Special cases for synchronizing Oracle Directory Server Enterprise Edition on page 16
- Setting up the LDAP synchronization server on page 17

- Configuring the synchronization log on page 29
- Customizing the synchronization configuration on page 30
- Advanced settings of a generic LDAP connector on page 34
- Tasks after a synchronization on page 45
- OpenDJ project template for the generic LDAP connector on page 147
- Active Directory Lightweight Directory Services project template for the generic LDAP connector on page 148

Configuring the synchronization log

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

To configure the content of the synchronization log

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

   - OR -

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

   > NOTE: Some content generates a particularly large volume of log data!
   >
   > The synchronization log should only contain data required for error analysis and other analyzes.
5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- Displaying synchronization results on page 43

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of an LDAP domain, you can use the 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 to be able to regularly compare the database with the LDAP environment and to synchronize changes.

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

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
- Changing settings of LDAP domain system connections on page 32
- Updating schemas on page 36
- Speeding up synchronization with revision filtering on page 37
- Configuring the provisioning of memberships on page 38
- Configuring single object synchronization on page 39
- Accelerating provisioning and single object synchronization on page 40

Configuring synchronization 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). To use One Identity Manager as the master system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

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

Related topics

- Configuring synchronization of several LDAP domains on page 31

Configuring synchronization of several LDAP domains

In some circumstances, it is possible to use a synchronization project to synchronize different 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 domains. Use the wizard to attach a base object.
   - In the wizard, select the LDAP connector and declare the connection parameters. The connection parameters are saved in a special variable set.

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

Related topics

- Configuring synchronization in LDAP domains on page 31

Changing settings of LDAP domain system connections

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

a. Specify a specialized variable set and change the values of the affected variables.

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).

b. Edit the target system connection with the system connection wizard and change the effected values.

   The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- Editing connection parameters in the variable set on page 32
- Editing target system connection properties on page 34
- Advanced settings of a generic LDAP connector on page 34
- Generic LDAP connector settings on page 149

Editing connection parameters in the variable set

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

> NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project for synchronization uses different LDAP domains.

To customize connection parameters in a specialized variable set

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Target system** category.
3. Open the **Connection parameters** view.

   Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration | Variables** category.

   All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on in the variable set view's toolbar.
   - To rename the variable set, select the variable set and click the variable set view in the toolbar . Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration | Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration | Base objects** category.
13. Select the base object and click .

    - OR -

    To add a new base object, click .
14. In the **Variable set** menu, select the specialized variable set.
15. Save the changes.

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

Related topics

- Editing target system connection properties on page 34

Editing target system connection properties

The advanced settings of the target system connection can be changed using the system connection wizard. If variables are defined for the settings, the changes are transferred to the active variable set.

> NOTE: In the following circumstances, the default values cannot be restored:
>
> - The connection parameters are not defined as variables.
> - The default variable set is selected as an active variable set.
>
> In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit advanced settings with the system connection wizard

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

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

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

   This starts the system connection wizard.

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

Related topics

- Editing connection parameters in the variable set on page 32

Advanced settings of a generic LDAP connector

> IMPORTANT: Changes to advanced settings should only be carried out by experienced Synchronization Editor users and system administrators.

Use the system connection wizard to configure the following extended properties of the generic connector:

- Definition of auxiliary classes of type **Auxiliary**
- Definition of virtual classes for non-RFC compliant object mappings
- Definition of system attributes for object identification, revision properties and additional operational attributes
- Definition of additional attributes for supporting dynamic groups

> NOTE: To make advanced settings, on the start page of the system connection wizard,

> set the **Configure advanced settings (expert mode)** option.

Define auxiliary classes

On the **Define auxiliary classes** page, select the structural classes that are handled as auxiliary classes by the LDAP connector. This may be necessary if a non-RFC compliant LDAP system allows assignment of several structural object classes to one entry although only one structural class is allowed.

Assigning more than one structural class means that an LDAP entry cannot be uniquely assigned to a schema type. If structural object classes have been defined that only serve as property extensions (meaning auxiliary classes), you can, with help from this option, set the connector to handle the object class as an **auxiliary class**.

> NOTE: Object classes that are configured as **auxiliary** are subsequently not handled as independent schema types and cannot, therefore, be synchronized separately.

Assigning auxiliary classes

On the **Assign auxiliary classes** page, assign additional auxiliary classes to structural classes.

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.

> NOTE: To map the attributes of the auxiliary classes in One Identity Manager, custom extensions to the One Identity Manager schema may be necessary under certain circumstances. Use the Schema Extension program to do this.

Defining virtual classes

On the **Virtual classes** page, define additional virtual classes. Objects made up of several structural classes can only be created in non-RFC compliant LDAP systems. They consist of one or more different classes that are not derived from each other, such as **OrganizationalUnit** and **inetOrgPerson**.

To create a virtual class

1. In the system connection wizard, on the **Virtual classes** page, click + in the **Configured virtual classes** pane and enter the virtual classes’ name in the **Virtual class** field.
2. In the **Select structural classes** pane, select the structural classes that are mapped to the virtual class.

Specifying additional system attributes

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

- In the **Object identification attribute** pane, select the attribute that can be used to uniquely identify the objects in the LDAP. The attribute must be unique and set for all objects LDAP.
- In the **Revision properties** pane, specify which attributes can be used for revision filtering.
- In the **Additional operational attributes** pane, specify which attributes should also be determined for the LDAP objects. Functional attributes are used for managing directories. Attributes are only determined if they are explicitly given.

  > NOTE: To map the operational attributes in One Identity Manager, custom extensions to the One Identity Manager schema may be required. Use the Schema Extension program to do this.

Defining attributes for supporting dynamic groups

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

Related topics

- Generic LDAP connector settings on page 149

Updating schemas

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

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

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

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

- Enabling the synchronization project
- Saving the synchronization project for the first time
- Compressing a schema

To update a system connection schema

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

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Speeding up synchronization with revision filtering

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 properties 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. (`DPRRevisionStore` table, `value` column). 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.

The revision is found at start of synchronization. Objects modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

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 **Use revision filter** item from **Revision filtering** menu.

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 **Use revision filter** item from the **Revision filtering** menu.

> 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*.

Configuring the provisioning of memberships

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

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

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and previously deleted memberships are added again.

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

To allow separate provisioning of memberships

1. In the Manager, select the **LDAP | Basic configuration data | Target system types** category.

2. Select **LDAP** in the result list.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
    - This option can only be enabled for assignment tables that have a base table with `XDateSubItem` or `CCC_XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically (for example, `LDAPAccountInLDAPGroup`, `LDAPGroupInLDAPGroup` and `LDAPMachineInLDAPGroup`).
5. Click **Merge mode**.
6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and not the entire members list.

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

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

To restore the default condition

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

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

Configuring single object synchronization

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

Prerequisites

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

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

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

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

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

   Example:
8. Save the changes.

Related topics

- Synchronizing single objects on page 44
- Post-processing outstanding objects on page 45

Accelerating provisioning and single object synchronization

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

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

> have not been completely processed.
>
> Once load balancing is no longer required, ensure that the synchronization server executes the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.

   - Assign the **LDAP connector** server function to the Job server.

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

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

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

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

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

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

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

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

To use the synchronization server without load balancing.

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

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

Executing synchronization

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

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

Detailed information about this topic

- Starting synchronization on page 42
- Deactivating synchronization on page 44
- Displaying synchronization results on page 43
- Synchronizing single objects on page 44

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

> IMPORTANT: As long as a synchronization process is running, you must not start another synchronization process for the same target system. This especially applies, if the same synchronization objects would be processed.
>
> - If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
>   - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
> - Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.

- Use the schedule to ensure that the start up configurations are run in sequence.
- Group start up configurations with the same start up behavior.

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

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

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

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

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

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

Related topics

- Configuring the synchronization log on page 29
- Troubleshooting on page 48

Deactivating synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Detailed information about this topic

- Creating a synchronization project for initial synchronization of an LDAP domain on page 20

Synchronizing single objects

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

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

To synchronize a single object

1. Select the object type in the navigation view.
2. In the result list, select the object that you want to synchronize.
3. Select the **Synchronize this object** task.

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

Detailed information about this topic

- Configuring single object synchronization on page 39

Tasks after a synchronization

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

- Post-processing outstanding objects on page 45
- Adding custom tables to the target system synchronization on page 47
- Managing LDAP user accounts through account definitions on page 48

Post-processing outstanding objects

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

Outstanding objects:

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

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

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select the **LDAP | Target system synchronization: LDAP** category.

   All the synchronization tables assigned to the **LDAP** target system type are displayed in the navigation view.

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

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

- The synchronization log has already been deleted.

  - OR -

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

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

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

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

> TIP:
>
> ***To display object properties of an outstanding object***
>
> 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 on one of the following icons in the form toolbar to execute the respective method.

Table 10: Methods for handling outstanding objects

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

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

NOTE: By default, the selected objects are processed in parallel, which speeds up

> execution of the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.
>
> Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.
>
> ***To disable bulk processing***
>
> - In the form's toolbar, click ⧉ to disable bulk processing.

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

To add custom tables to target system synchronization

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

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

Adding custom tables to the target system synchronization

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

To add custom tables to target system synchronization

1. In the Manager, select the **LDAP | Basic configuration data | Target system types** category.
2. In the result list, select the **LDAP** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.

6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

Related topics

- Post-processing outstanding objects on page 45

Managing LDAP user accounts through account definitions

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

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

Detailed information about this topic

- Assigning account definitions to linked LDAP user accounts on page 115

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

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

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

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

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

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

Related topics

- Displaying synchronization results on page 43

3

Basic configuration data

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

- Configuration parameters

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

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

  For more information, see Configuration parameters for managing an LDAP environment on page 144.

- Account definitions

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

  For more information, see Account definitions for LDAP user accounts on page 51.

- Password policies

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

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

  For more information, see Password policies for LDAP user accounts on page 69.

- 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 45.

- Servers

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

  For more information, see Job server for LDAP-specific process handling on page 81.

- Target system managers

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

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

  For more information, see Target system managers on page 87.

Account definitions for LDAP user accounts

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

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

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

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

The following steps are required to implement an account definition:

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

Detailed information about this topic

- Creating an account definition on page 52
- Creating manage levels on page 54
- Creating a formatting rule for IT operating data on page 57
- Collecting IT operating data on page 59
- Assigning account definitions to employees on page 61
- Assigning account definitions to LDAP domains on page 67

Creating an account definition

To create a new account definition

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list. Select the **Change master data** task.

   -OR-

   Click + in the result list.
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 52

Master data for an account definition

Enter the following data for an account definition:

Table 11: Master data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.

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

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

Creating 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.

One Identity Manager supplies a default configuration for manage levels:

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

> NOTE: The **Full managed** and **Unmanaged** manage levels are analyzed in templates. You can customize the supplied templates in the Designer.
>
> You can define other manage levels depending on your requirements. You need to amend the templates to include manage level approaches.

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For 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. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage levels.

   - OR -

   In the **Remove assignments** pane, remove the manage levels.
5. Save the changes.

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

To edit a manage level

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Manage levels** category.
2. Select the manage level in the result list. Select the **Change master data** task.

- OR -

Click + in the result list.

3. Edit the manage level's master data.
4. Save the changes.

Related topics

- Master data for manage levels on page 56

Master data for manage levels

Enter the following data for a manage level.

Table 12: Master data for manage levels

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

Property	Description
security is at risk	risk are locked.
Retain groups if user account disabled	Specifies whether disabled 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 automatically creating user accounts for an employee in the target system and modifying them.

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

To create a mapping rule for IT operating data

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

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

Table 13: Mapping rule for IT operating data

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

4. Save the changes.

Related topics

- Collecting IT operating data on page 59

Collecting IT operating data

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

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

Example

Normally, each employee in department A obtains a default user account in the 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 "Department" property 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, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

To define IT operating data

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

3. Click **Add** and enter the following data.

Table 14: IT operating data

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

4. Save the changes.

Related topics

- Creating a formatting rule for IT operating data on page 57

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To execute the template

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

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

Old value:	Current value of the object property.
New value:	Value that the object property would have following modification of the IT operating data.
Selection:	Specifies whether or not the new value is transferred to the user account.

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

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

> NOTE: If a user account already exists and is disabled, then it is re-enabled. In this case, you must change the user account manage level afterward.

Prerequisites for indirect assignment of account definitions to employees

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

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

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

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 62
- Assigning account definitions to business roles on page 63
- Assigning account definitions to all employees on page 63
- Assigning account definitions directly to employees on page 64
- Assigning account definitions to LDAP domains on page 67

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
    - On the **Departments** tab, assign departments.
    - On the **Locations** tab, assign locations.
    - On the **Cost centers** tab, assign cost centers.

    > TIP: In the **Remove assignments** pane, you can remove assigned organizations.
    >
    > ***To remove an assignment***
    >
    > - Select the organization and double-click ✓.
5. Save the changes.

Related topics

- Assigning account definitions to business roles on page 63
- Assigning account definitions to all employees on page 63
- Assigning account definitions directly to employees on page 64

Assigning account definitions to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

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

   > TIP: In the **Remove assignments** pane, you can remove assigned business roles.
   >
   > ***To remove an assignment***
   >
   > - Select the business role and double-click ✓.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 62
- Assigning account definitions to all employees on page 63
- Assigning account definitions directly to employees on page 64

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, enable the **Automatic assignment to employees** option.

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

5. Save the changes.

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

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 62
- Assigning account definitions to business roles on page 63
- Assigning account definitions directly to employees on page 64

Assigning account definitions directly to employees

To assign an account definition directly to employees

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

   > TIP: In the **Remove assignments** pane, you can remove assigned employees.
   >
   > ***To remove an assignment***
   >
   > - Select the employee and double-click ✓.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 62
- Assigning account definitions to business roles on page 63
- Assigning account definitions to all employees on page 63

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

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

   > TIP: In the **Remove assignments** pane, you can remove assigned system roles.
   >
   > ***To remove an assignment***
   >
   > - Select the system role and double-click ✓.

5. Save the changes.

Adding account definitions to the IT Shop

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

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

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

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

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

To add an account definition to the IT Shop

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

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

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

To remove an account definition from individual IT Shop shelves

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

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

To remove an account definition from all IT Shop shelves

1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

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

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

For more information about requests 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 52
- Assigning account definitions to departments, cost centers, and locations on page 62

- Assigning account definitions to business roles on page 63
- Assigning account definitions directly to employees on page 64
- Assigning account definitions to system roles on page 65

Assigning account definitions to LDAP domains

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

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

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

To assign the account definition to a target system

1. In the Manager, select the domain in the **LDAP | Domains** category.
2. Select the **Change master data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Detailed information about this topic

- Automatic assignment of employees to LDAP user accounts on page 112

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.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
   1. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
   2. Select an account definition in the result list.
   3. Select the **Change master data** task.

    d. On the **General** tab, disable the **Automatic assignment to employees** option.

    e. Save the changes.

2. Remove direct assignments of the account definition to employees.

    a. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.

    b. Select an account definition in the result list.

    c. Select the **Assign to employees** task.

    d. In the **Remove assignments** pane, remove the employees.

    e. Save the changes.

3. Remove the account definition's assignments to departments, cost centers, and locations.

    a. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.

    b. Select an account definition in the result list.

    c. Select the **Assign organizations** task.

    d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.

    e. Save the changes.

4. Remove the account definition's assignments to business roles.

    a. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.

    b. Select an account definition in the result list.

    c. Select the **Assign business roles** task.

       In the **Remove assignments** pane, remove the business roles.

    d. Save the changes.

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

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

   To remove an account definition from all IT Shop shelves

    a. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

       - OR -

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

    b. Select an account definition in the result list.

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

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

e. Click **OK**.

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

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
    a. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
    b. Select an account definition in the result list.
    c. Select the **Change master data** task.
    d. From the **Required account definition** menu, remove the account definition.
    e. Save the changes.
7. Remove the account definition's assignments to target systems.
    a. In the Manager, select the domain in the **LDAP | Domains** category.
    b. Select the **Change master data** task.
    c. On the **General** tab, remove the assigned account definitions.
    d. Save the changes.
8. Delete the account definition.
    a. In the Manager, select the **LDAP | Basic configuration data | Account definitions | Account definitions** category.
    b. Select an account definition in the result list.
    c. Click to delete an account definition.

Password policies for LDAP user accounts

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

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

Detailed information about this topic

- Predefined password policies on page 70
- Using password policies on page 71
- Editing password policies on page 73
- Custom scripts for password requirements on page 76
- Password exclusion list on page 79
- Checking a password on page 79
- Testing password generation on page 79

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.1.3, the configuration parameter settings for forming passwords are passed on to the target system-specific password policies.

The **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.

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

Using password policies

The **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.

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

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

1. Password policy of the account definition of the user account.
2. Password policy of the manage level of the user account.
3. Password policy for the LDAP container of the user account.
4. Password policy for the LDAP domain of the user account.
5. The **One Identity Manager password policy** (default policy).

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

To reassign a password policy

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

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

Table 15: Assigning a password policy

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

5. Save the changes.

To change a password policy's assignment

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

Editing password policies

To edit a password policy

1. In the Manager, select the **LDAP | Basic configuration data | Password policies** category.
2. Select the password policy in the result list and select **Change master data**.

   - OR -

   Click in the result list.
3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

- General master data for password policies on page 73
- Policy settings on page 74
- Character classes for passwords on page 75
- Custom scripts for password requirements on page 76

General master data for password policies

Enter the following master data for a password policy.

Table 16: Master data for a password policy

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

Policy settings

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

Table 17: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. Only taken into account when logging in to One Identity Manager. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more detailed information, see the *One Identity Manager Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the

Property	Meaning
	password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more detailed information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

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

Table 18: Character classes for passwords

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

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

Custom scripts for password requirements

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

Detailed information about this topic

- Checking passwords with a script on page 76
- Generating passwords with a script on page 77

Checking passwords with a script

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example of a script that checks a password

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

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

        Dim pwd = spwd.ToInsecureArray()

        If pwd.Length>0

                If pwd(0)="?" Or pwd(0)="!"

                        Throw New Exception(#LD("Password can't start with '?' or '!'")#)

                End If

        End If

        If pwd.Length>2

                If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)

                        Throw New Exception(#LD("Invalid character sequence in password")#)

                End If

        End If

End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **LDAP | Basic configuration data | Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change master data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
    e. Save the changes.

Related topics

- Generating passwords with a script on page 77

Generating passwords with a script

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

The script replaces the **?** and **!** characters at the beginning of random passwords with **_**.

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

      Dim pwd = spwd.ToInsecureArray()

      ' replace invalid characters at first position

      If pwd.Length>0

            If pwd(0)="?" Or pwd(0)="!"

                  spwd.SetAt(0, CChar("_"))

            End If

      End If

End Sub
```

To use a custom script for generating a password

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

Related topics

- Checking passwords with a script on page 76

Password exclusion list

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

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

To add a term to the restricted list

1. In the Designer, select the **Base Data | Security settings | Restricted passwords** category.
2. Create a new entry with the **Object | New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking a password

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

To check if a password conforms to the password policy

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

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

Testing password generation

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

To generate a password that conforms to the password policy

1. In the Manager, select the **LDAP | Basic configuration data | Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change master data** task.

4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new LDAP user accounts

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

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

Related topics

- Password policies for LDAP user accounts on page 69
- Email notifications about login data on page 80

Email notifications about login data

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

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

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the *One Identity Manager Installation Guide*.

2. In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.
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 can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

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

To send initial login data by email

1. In the Designer, set the **TargetSystem | LDAP | Accounts | InitialRandomPassword** configuration parameter.
2. In the Designer, set the **TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the recipient of the notification as a value.
3. In the Designer, set the **TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

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

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

> TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Job server for LDAP-specific process handling

In order to handle -specific processes in One Identity Manager, the synchronization server and its server functions must be declared. You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data | Installation | Job server** category. For detailed information, see *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **LDAP | Basic configuration data | Server** category and edit the Job server’s master data.

  Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

Related topics

- System requirements for the LDAP synchronization server on page 17
- Editing LDAP Job servers on page 82

Editing LDAP Job servers

To edit a Job server and its functions

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

Detailed information about this topic

- General master data for Job servers on page 82
- Specifying server functions on page 85
- Installing the One Identity Manager Service with an LDAP connector on page 17

General master data for Job servers

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

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

Table 19: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of server>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the `Robocopy` and `rsync` programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the `Robocopy` program between servers with a Windows operating system or with the `rsync` program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.

Property	Meaning
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Last fetch time	Last time the process was collected.
Last	The time of the last check for loaded process steps with a dispatch value that

Property	Meaning
timeout check	exceeds the one in the **Common | Jobservice | LoadedJobsTimeOut** configuration parameter.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 85

Specifying server functions

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

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

Table 20: Permitted server functions

Server function	Remark
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
LDAP connector	Server on which the LDAP connector is installed. This server synchronizes the LDAP target system.
LDAP store	Server containing the LDAP store.
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can run SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the

Server function	Remark
	generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Native database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for running synchronization with an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.

Related topics

- General master data for Job servers on page 82

Target system managers

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

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

For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.

   Target system managers with the default application role are authorized to edit all the domains in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual domains.

Table 21: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | LDAP** or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects.

User	Tasks
	- 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 a One Identity Manager administrator (**Base role | Administrators** application role)
2. Select the **One Identity Manager Administration | Target systems | Administrators** category.
3. Select the **Assign employees** task.
4. Assign the employee you want and save the changes.

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

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

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

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

To specify target system managers for individual domains

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

   - OR -

Next to the **Target system manager** menu, click to create a new application role.

   a. Enter the application role name and assign the **Target systems | LDAP** parent application role.

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

6. Save the changes.
7. Assign employees to this application role who are permitted to edit the 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 LDAP on page 9
- General master data for LDAP domains on page 90
- LDAP container structures on page 135

LDAP domains

> INFORMATION: If you use a default project template, the Synchronization Editor sets up the domains in the One Identity Manager database.

To edit master data for an LDAP domain

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

Detailed information about this topic

- General master data for LDAP domains on page 90
- LDAP specific master data for LDAP domains on page 92
- Specifying categories for inheriting LDAP groups on page 93

General master data for LDAP domains

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

Table 22: 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
	`Docu.Testlab.dd`

Property	Description
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, in the input field, you can add object classes and auxiliary classes 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)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this domain and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role in which target system managers 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. 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.
Synchronized by	Type of synchronization through which the data is synchronized between the domain and One Identity Manager. You can no longer change the synchronization type once objects for these domains are present in One Identity Manager. If you create a domain with the Synchronization Editor, **One Identity Manager** is used.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>

Table 23: Permitted values

<table>
<tr><th>Value</th><th>Synchronization by</th><th>Provisioned by</th></tr>
<tr><td>One Identity Manager</td><td>LDAP connector</td><td>LDAP connector</td></tr>
<tr><td>No synchronization</td><td>none</td><td>none</td></tr>
</table>

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

</td></tr>
<tr><td>Description</td><td>Text field for additional explanation.</td></tr>
<tr><td>Structural object class</td><td>Structural object class representing the object type.</td></tr>
</table>

Related topics

- Automatic assignment of employees to LDAP user accounts on page 112
- Target system managers on page 87

LDAP specific master data for LDAP domains

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

Table 24: 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, in the input field, you can add object classes

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

To define a category

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

Detailed information about this topic

- LDAP group inheritance based on categories on page 131

Editing synchronization projects

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

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

To open an existing synchronization project in the Synchronization Editor

1. In the Manager, select the **LDAP | Domains** category.
2. Select the domain in the result list. Select the **Change master data** task.
3. Select the **Edit synchronization project...** task.

Related topics

- Customizing the synchronization configuration on page 30

LDAP user accounts

You manage user account in LDAP with One Identity Manager. 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 95
- Supported user account types on page 96
- Entering master data for LDAP user accounts on page 102

Linking user accounts to employees

The main feature of One Identity Manager is to map employees together with the master data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

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

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

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

- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

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

Related topics

- Entering master data for LDAP user accounts on page 102
- Account definitions for LDAP user accounts on page 51
- Automatic assignment of employees to LDAP user accounts on page 112

Supported user account types

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

- Identity

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

Table 25: Identities of user accounts

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

Identity	Description	Value of the IdentityType column
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

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

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

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

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

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

- Privileged user account

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

Detailed information about this topic

- Default user accounts on page 98
- Administrative user accounts on page 98
- Providing administrative user accounts for one employee on page 99
- Providing administrative user accounts for several employees on page 100
- Privileged user accounts on page 101

Default user accounts

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

To create default user accounts through account definitions

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

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

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

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

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

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

Related topics

- Account definitions for LDAP user accounts on page 51

Administrative user accounts

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

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

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

Related topics

- Providing administrative user accounts for one employee on page 99
- Providing administrative user accounts for several employees on page 100

Providing administrative user accounts for one employee

Prerequisites

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

To prepare an administrative user account for a person

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

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

Related topics

- Providing administrative user accounts for several employees on page 100
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

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

To prepare an administrative user account for multiple employees

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

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

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

To remove an assignment

- Select the employee and double-click ✓.

Related topics

- Providing administrative user accounts for one employee on page 99
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

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

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

To create privileged users through account definitions

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

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

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

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.

- To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the IsGroupAccount column with a default value of **0** and set the **Always use default value** option.

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

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

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

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

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

- To use a prefix for the login name, in the Designer, set the **TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_Prefix** configuration parameter.
- To use a postfix for the login name, in the Designer, set the**TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_Postfix** configuration parameter.

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

Related topics

- Account definitions for LDAP user accounts on page 51

Entering master data for LDAP user accounts

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

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

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

To create a user account

1. In the Manager, select the **LDAP | User accounts** category.
2. Click + in the result list.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

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

To manually assign or create a user account for an employee

1. In the Manager, select the **Employees | Employees** category.
2. Select the employee in the result list and run the **Assign LDAP user accounts** task.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic

- General master data of LDAP user accounts on page 103
- Contact data for an LDAP user account on page 107
- Address information for LDAP user accounts on page 107
- Organizational data for LDAP user accounts on page 108
- Miscellaneous data for an LDAP user account on page 109

Related topics

- Supported user account types on page 96
- Account definitions for LDAP user accounts on page 51

General master data of LDAP user accounts

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

Table 26: General 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 are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click + next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved.
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
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 **INETORGPERSON** object class.
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 **INETORGPERSON** object class. However, in the input field, you can add object classes and auxiliary classes 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	User account display name. The display name is made up of the first and

Property	Description
name	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.
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	Password for the user account. The employee’s central password can be mapped to the user account password. For detailed information about an employee’s central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use an initial password for the user accounts, it is automatically entered when a user account is created. 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.
Password confirmation	Reconfirm password.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For 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. Groups can

Property	Description
	be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative permissions, used by one employee. • **Sponsored identity**: User account that is used for a specific purpose, such as training. • **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • **Service identity**: Service account.
Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
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 <User account is deactivated> option.

Related topics

- Account definitions for LDAP user accounts on page 51
- Password policies for LDAP user accounts on page 69
- Initial password for new LDAP user accounts on page 80
- Linking user accounts to employees on page 95
- Disabling LDAP user accounts on page 116

Contact data for an LDAP user account

On the **Contact data** tab, enter the data used by this user account for contacting the employee by telephone.

Table 27: Contact data

Property	Description
Image	Picture to display in a telephone book, for example. • Load the image using the 📂 button. • 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.
International ISDN no.	International 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 LDAP user accounts

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

Table 28: 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 LDAP user accounts

On the **Organizational** tab, enter the following organizational master data.

Table 29: 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 input field is automatically filled out with respect to the manage level.

Property	Description
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 30: 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 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. In the Manager, select the **LDAP | User accounts** category.
2. Select the user account in the result list.
3. Select the **LDAP user account overview** task.

Changing manage levels for LDAP user accounts

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

To change the manage level for a user account

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

Related topics

- Entering master data for LDAP user accounts on page 102

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, such as 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. In the Manager, select the **LDAP | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign groups.

   > TIP: In the **Remove assignments** pane, you can remove the assignment of groups.
   >
   > ***To remove an assignment***
   >
   > - Select the group and double-click ✓.

5. Save the changes.

Related topics

- Assigning LDAP groups directly to LDAP user accounts and LDAP computers on page 121

Assigning extended properties to LDAP user accounts

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

To specify extended properties for a user account

1. In the Manager, select the **LDAP | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   > TIP: In the **Remove assignments** pane, you can remove assigned extended properties.
   >
   > ***To remove an assignment***
   >
   > - Select the extended property and double-click ✓.

5. Save the changes.

For 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

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 on the basis of existing user account master data. This mechanism can be triggered after a new user account is created either manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | LDAP | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the **TargetSystem | LDAP | PersonAutoDefault** configuration parameter and select the required mode.
- Use the **TargetSystem | LDAP | PersonAutoDisabledAccounts** configuration parameter to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the domain. Ensure that the manage level to be used is entered as the default manage 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 a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the domain is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

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

For more information, see Managing LDAP user accounts through account definitions on page 48.

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 52
- Assigning account definitions to LDAP domains on page 67
- Changing manage levels for LDAP user accounts on page 110
- Assigning account definitions to linked LDAP user accounts on page 115
- Editing search criteria for automatic employee assignment on page 113

Editing search criteria for automatic employee assignment

The criteria for employee assignments are defined for 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 criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (AccountToPersonMatchingRule) in 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.

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 assignments to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user accounts for the respective user account.

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

To specify criteria for employee assignment

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

   Table 31: Standard search criteria for user accounts

Apply to	Column for employee	Column for 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

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

Table 32: 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 using a suggestion list

1. Click **Suggested assignments**.
    a. Check the **Selection** box of all the user accounts to which you want to assign the suggested employees. Multi-select is possible.
    b. Click **Assign selected.**
    c. Confirm the security prompt with **Yes**.

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

   – OR –
2. Click **No employee assignment**.
    a. Click the **Select employee** option of the user account to which you want to assign an employee. Select an employee from the menu.
    b. Check the **Selection** box of all the 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**.

       The employees displayed in the **Employee** column are assigned to the selected user accounts.

To remove assignments

1. Click **Assigned user accounts**.
    a. Click the **Selection** box of all user accounts you want to delete the employee assignment from. Multi-select is possible.
    b. Click **Remove selected**.
    c. Confirm the security prompt with **Yes**.

       The assigned employees are removed 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 112

Assigning account definitions to linked LDAP user accounts

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

- Employees and user accounts were linked manually.
- Automatic employee assignment is configured, but when a user account is inserted, no account definition is assigned in the domain.

To select user accounts through account definitions

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

Detailed information about this topic

- Assigning account definitions to LDAP domains on page 67

Disabling LDAP user accounts

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

Scenario:

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

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

Scenario:

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

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

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

To disable the user account when the configuration parameter is disabled

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

Scenario:

- User accounts not linked to employees.

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

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

Related topics

- Account definitions for LDAP user accounts on page 51
- Creating manage levels on page 54
- Deleting and restoring LDAP user accounts on page 117
- 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 assignment of an account definition is removed, the user account that was created from this account definition is deleted.

To delete a user account

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

To restore a user account

1. In the Manager, select the **LDAP | User accounts** category.
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 accounts are deleted from the database and cannot be restored anymore. In the Designer, you can set an alternative delay on the `LDAPAccount` table.

Related topics

- Disabling LDAP user accounts on page 116

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, locations, business roles, or the IT Shop.

To edit group master data

1. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list and run the **Change master data** task.
3. On the master data form, edit the master data for the group.
4. Save the changes.

Detailed information about this topic

- LDAP group master data on page 119
- Assigning LDAP groups directly to LDAP user accounts and LDAP computers on page 121

LDAP group master data

Enter the following master data:

Table 33: 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.
Name	Name of the group.

Property	Description
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 **GROUPOFNAMES**.
Object class	List of classes defining the attributes for this object. By default, containers in One Identity Manager are added with **GROUPOFNAMES**. However, in the input field, you can add object classes and auxiliary classes that are used by other LDAP and X.500 directory services.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
Condition	LDAP filter for finding memberships in a dynamic group.
dynamic group	Specifies whether this is a dynamic group.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.

Related topics

- LDAP group inheritance based on categories on page 131
- 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 directly to LDAP user accounts and LDAP computers

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

- If you add an employee to roles and that employee owns an LDAP user account, the LDAP user account is added to the LDAP group.
- If you add a device to roles, the LDAP computer that references the device is added to the LDAP groups.
- If a device owns a workdesk and you add the workdesk to roles, the LDAP computer, which references this device, is also added to all LDAP groups of the workdesk's roles.

Prerequisites for the indirect assignment of employees to LDAP user accounts

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

Prerequisites for indirect assignment to LDAP computers

- The assignment of devices and LDAP groups is permitted for departments, cost centers, locations, or business roles.
- The LDAP computer is connected to a device.
- The device is labeled as a PC or server.
- The **TargetSystem | LDAP | HardwareInGroupFromOrg** configuration parameter is set.

Prerequisites for indirect assignment to LDAP computers through workdesks are:

- The assignment of workdesks and LDAP groups is permitted for departments, cost centers, locations, or business roles.
- The LDAP computer is connected to a device.
- The device is labeled as a PC or server.
- The device owns a workdesk.

Furthermore, LDAP groups can be requested through the Web Portal. To do this, add employees to a shop as customers. All LDAP groups are assigned to this shop can be requested by the customers. Requested LDAP groups are assigned to the employees after approval is granted.

Through system roles, LDAP groups can be grouped together and assigned to employees and workdesks as a package. You can create system roles that contain only LDAP groups. System entitlements from different target systems can also be grouped together in a system role.

To react quickly to special requests, you can also assign LDAP groups directly to LDAP user accounts and LDAP computers.

For detailed information see the following guides:

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

Detailed information about this topic

- Assigning LDAP groups to departments, cost centers, and locations on page 123
- Assigning LDAP groups to business roles on page 124
- Assigning LDAP user accounts directly to LDAP groups on page 125
- Assigning LDAP computers directly to LDAP groups on page 126
- Adding LDAP groups to system roles on page 126
- Adding LDAP groups to the IT Shop on page 127

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. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

   > TIP: In the **Remove assignments** pane, you can remove assigned organizations.
   >
   > ***To remove an assignment***
   >
   > - Select the organization and double-click ✓.
5. Save the changes.

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

1. In the Manager, select the **Organizations | Departments** category.

   - OR -

   In the Manager, select the **Organizations | Cost centers** category.

   - OR -

   In the Manager, select the **Organizations | Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign LDAP groups** task.
4. In the **Add assignments** pane, assign groups.

   > TIP: In the **Remove assignments** pane, you can remove the assignment of groups.
   >
   > ***To remove an assignment***
   >
   > - Select the group and double-click ✓.
5. Save the changes.

Related topics

- Assigning LDAP groups to business roles on page 124
- Assigning LDAP user accounts directly to LDAP groups on page 125
- Assigning LDAP computers directly to LDAP groups on page 126
- Adding LDAP groups to system roles on page 126
- Adding LDAP groups to the IT Shop on page 127
- One Identity Manager users for managing LDAP on page 9

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. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

   > TIP: In the **Remove assignments** pane, you can remove assigned business roles.
   >
   > ***To remove an assignment***
   >
   > - Select the business role and double-click ✓.
5. Save the changes.

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

1. In the Manager, select the **Business roles | <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign LDAP groups** task.
4. In the **Add assignments** pane, assign groups.

   > TIP: In the **Remove assignments** pane, you can remove the assignment of groups.
   >
   > ***To remove an assignment***
   >
   > - Select the group and double-click ✓.
5. Save the changes.

Related topics

- Assigning LDAP groups to departments, cost centers, and locations on page 123
- Assigning LDAP user accounts directly to LDAP groups on page 125
- Assigning LDAP computers directly to LDAP groups on page 126
- Adding LDAP groups to system roles on page 126
- Adding LDAP groups to the IT Shop on page 127
- One Identity Manager users for managing LDAP on page 9

Assigning LDAP user accounts directly to LDAP groups

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is done by allocating the employee and groups into company structures such as 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. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In **Add assignments** pane, assign user accounts.

   > TIP: In the **Remove assignments** pane, you can remove assigned user accounts.
   >
   > ***To remove an assignment***
   >
   > - Select the user account and double-click ✓.

5. Save the changes.

Related topics

- Assigning LDAP groups directly to LDAP user accounts on page 110
- Assigning LDAP groups to departments, cost centers, and locations on page 123
- Assigning LDAP groups to business roles on page 124
- Assigning LDAP computers directly to LDAP groups on page 126
- Adding LDAP groups to system roles on page 126
- Adding LDAP groups to the IT Shop on page 127

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 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. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **Assign computers** task.
4. In the **Add assignments** pane, assign computers.

   - OR -

   In the **Remove assignments** pane, remove computers.
5. Save the changes.

Related topics

- Assigning LDAP computers directly to LDAP groups on page 140
- Assigning LDAP groups to departments, cost centers, and locations on page 123
- Assigning LDAP groups to business roles on page 124
- Assigning LDAP user accounts directly to LDAP groups on page 125
- Adding LDAP groups to system roles on page 126
- Adding LDAP groups to the IT Shop on page 127

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 user accounts belonging to these employees inherit the group. This task is not available for dynamic groups.

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

To assign a group to system roles

1. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   > TIP: In the **Remove assignments** pane, you can remove assigned system roles.
   >
   > ***To remove an assignment***
   >
   > - Select the system role and double-click ✓.

5. Save the changes.

Related topics

- Assigning LDAP groups to departments, cost centers, and locations on page 123
- Assigning LDAP groups to business roles on page 124
- Assigning LDAP user accounts directly to LDAP groups on page 125
- Assigning LDAP computers directly to LDAP groups on page 126
- Adding LDAP groups to the IT Shop on page 127

Adding LDAP groups to the IT Shop

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

- The group is not a dynamic group.
- The group must be labeled with the **IT Shop** option.
- The group must be assigned a service item.

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

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

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

To add a group to the IT Shop.

1. In the Manager select the **LDAP | Groups** category (non role-based login) category.

   - OR -

In the Manager, select the **Entitlements | LDAP groups** (role-based login) category.

2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the group to the IT Shop shelves.
5. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager select the **LDAP | Groups** category (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements | LDAP groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
5. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **LDAP | Groups** category (non role-based login) category.

   - OR -

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

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

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

Related topics

- LDAP group master data on page 119
- Assigning LDAP groups to departments, cost centers, and locations on page 123
- Assigning LDAP groups to business roles on page 124
- Assigning LDAP user accounts directly to LDAP groups on page 125

- Assigning LDAP computers directly to LDAP groups on page 126
- Adding LDAP groups to system roles on page 126

Additional tasks for managing LDAP groups

After you have entered the master data, 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. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **LDAP group overview** task.

Effectiveness of group memberships

Table 34: Configuration parameters for conditional inheritance

Configuration parameter	Effect when set
QER | Structures | Inherite | 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. Changes to this parameter require the database to be recompiled.

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

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

NOTE:

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

The effectiveness of the assignments is mapped in the `LDAPAccountInLDAPGroup` and `BaseTreeHasLDAPGroup` tables by the `XIsInEffect` column.

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

Clara Harris has a user account in this domain. She primarily belongs to the "Marketing" department. The "Control group" business role and the "Finance" department 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 35: Specifying excluded groups (`LDAPGroupExclusion` table)

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

Table 36: 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 "control group" business role 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 requests and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 37: 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 **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.
- Mutually exclusive groups belong to the same domain

To exclude a group

1. In the Manager, select the **LDAP | Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

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

LDAP group inheritance based on categories

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

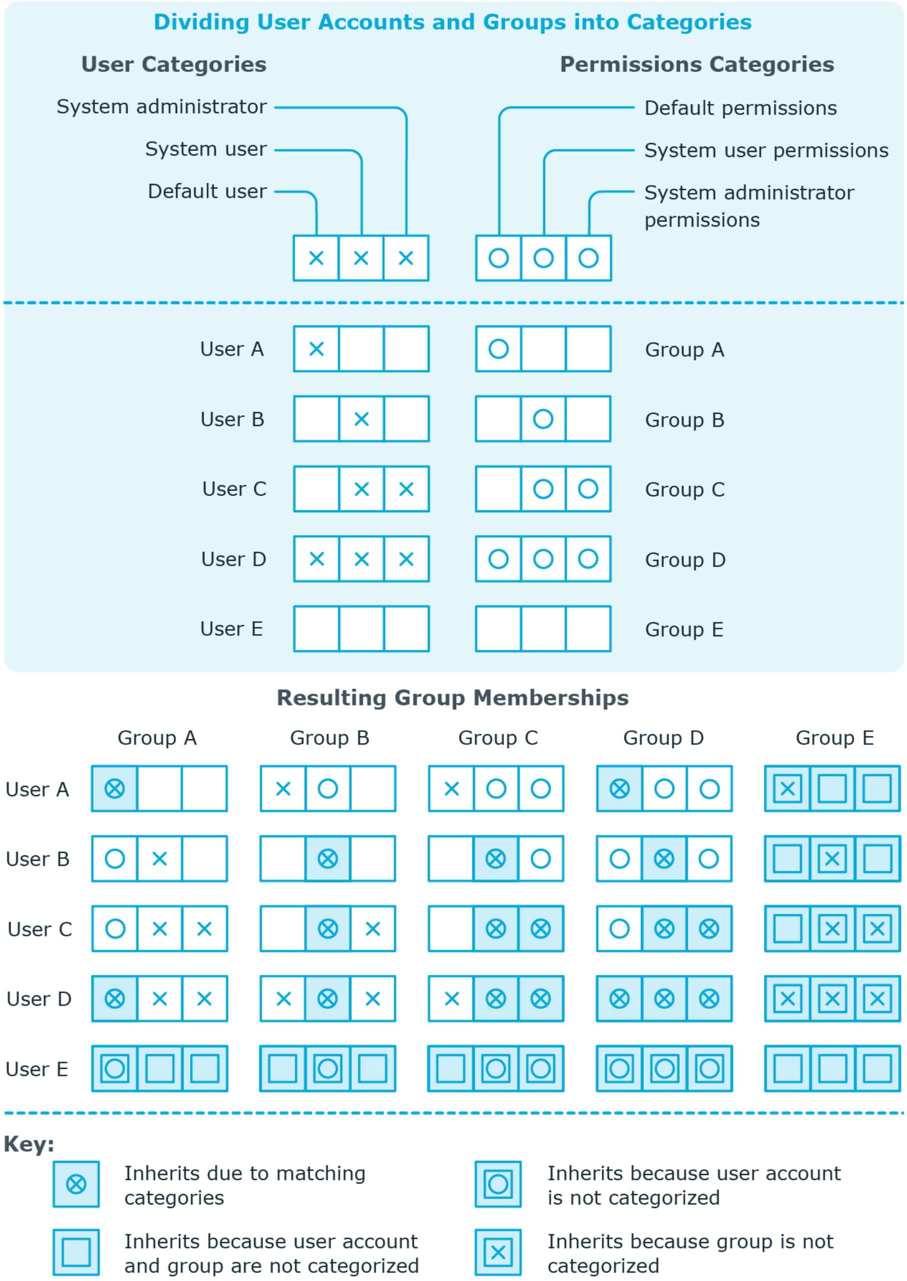
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or 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 38: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	System user permissions
3	System administrator	System administrator permissions

Figure 2: Example of inheriting through categories.


Dividing User Accounts and Groups into Categories
User Categories
System administrator
System user
Default user
Permissions Categories
Default permissions
System user permissions
System administrator permissions
User A
User B
User C
User D
User E
Group A
Group B
Group C
Group D
Group E
Resulting Group Memberships
Group A
Group B
Group C
Group D
Group E
User A
User B
User C
User D
User E
Key:
Inherits due to matching categories
Inherits because user account is not categorized
Inherits because user account and group are not categorized
Inherits because group is not categorized

To use inheritance through categories

- In the Manager, 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 93
- General master data of LDAP user accounts on page 103
- LDAP group master data on page 119

Assigning extended properties to LDAP groups

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

To specify extended properties for a group

1. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   > TIP: In the **Remove assignments** pane, you can remove assigned extended properties.
   >
   > ***To remove an assignment***
   >
   > - Select the extended property and double-click ✓.

5. Save the changes.

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

Deleting LDAP groups

To delete a group

1. In the Manager, select the **LDAP | Groups** category.
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.

7

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. In the Manager, select the **LDAP | Contacts** category.
2. Select the container in the result list and run the **Change master data** task.

   - OR -

   Click + in the result list.
3. Edit the container's master data.
4. Save the changes.

Detailed information about this topic

- General master data for LDAP containers on page 135
- Contact data for LDAP containers on page 137
- Address information for LDAP containers on page 137

General master data for LDAP containers

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

Table 39: 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 **ORGANIZATIONALUNIT** object class.
Object class	List of classes defining the attributes for this object. By default, containers in One Identity Manager are added with the **ORGANIZATIONALUNIT** object class. However, in the input field, you can add object classes and auxiliary classes that are used by other LDAP and X.500 directory services.
Description	Text field for additional explanation.
Target system manager	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. 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.

Related topics

- Target system managers on page 87

Contact data for LDAP containers

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

Table 40: 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 41: 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. In the Manager, select the **LDAP | Computers** category.
2. In the result list, select the computer and run the **Change master data** task.

   - OR -

   Click ➕ in the result list.
3. Edit the computer's master data.
4. Save the changes.

Detailed information about this topic

- Master data for LDAP computers on page 139

Master data for LDAP computers

Enter the following data for a computer.

Table 42: Computer master data

Property	Description
Device	The computer is connected to this device. Specify a new device using the ➕ button next to the menu. For more detailed information about devices, see the *One Identity Manager Identity Management Base Module Administration Guide*
Name	Computer identifier

Property	Description
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, in the input field, you can add object classes and auxiliary classes that are used by other LDAP and X.500 directory services.

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. In the Manager, select the **LDAP | Computers** category.
2. Select the computer in the result list.
3. Select the **Assign groups** category.
4. In the **Add assignments** pane, assign groups.

   > TIP: In the **Remove assignments** pane, you can remove the assignment of groups.
   >
   > ***To remove an assignment***
   >
   > - Select the group and double-click ✓.

5. Save the changes.

Related topics

- Assigning LDAP groups directly to LDAP user accounts and LDAP computers on page 121

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 43: Reports for the target system

Report	Description
Overview of all assignments (domain)	This report find 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 that 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 contains a risk assessment.
Show unused user accounts	This report shows all user accounts in the domain that 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 provisioned by 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 **My One Identity Manager** category.
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 **My One Identity Manager** category.

Related topics

- Overview of all assignments on page 142

Overview of all assignments

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

Examples

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

To display detailed information about assignments

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

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the ⓘ icon in the report's toolbar.

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

Figure 3: Toolbar of the Overview of all assignments report.

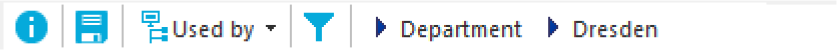


Table 44: Meaning of icons in the report toolbar

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

Appendix A

Configuration parameters for managing an LDAP environment

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

Table 45: Configuration parameters 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 this parameter require the database to be recompiled.
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 address stored in the **TargetSystem | LDAP | DefaultAddress** configuration parameter.
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The **Employee - new user account created** mail template is used.

Configuration parameter	Description
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem | 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. The **Employee - new user account with default properties created** mail template is used.
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	This configuration parameter allows configuration of the LDAP authentication module. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
TargetSystem | LDAP | Authentication | Authentic-ation	This 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. The default is **ServerBind**.
TargetSystem | LDAP | Authentication | Port	LDAP server port. The default is port **389**.
TargetSystem | LDAP | Authentication | RootDN	The configuration parameter contains a pipe (|) delimited list of root domains to use for finding the user account for authentication. Syntax:

Configuration parameter	Description

	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Example:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | Authentication | Server	This 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	The configuration parameter specifies whether computers are added to groups on the basis of 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 parameter specifies whether employees are automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
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.

Appendix B

Default project template for LDAP

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

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

Detailed information about this topic

- OpenDJ project template for the generic LDAP connector on page 147
- Active Directory Lightweight Directory Services project template for the generic LDAP connector on page 148

OpenDJ project template for the generic LDAP connector

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

Table 46: Mapping schema types to tables in the One Identity Manager schema.

Schema type in LDAP	Table in the One Identity Manager Schema
domain	LDPDomain
organization	LDAPContainer
organizationalUnit	LDAPContainer
locality	LDAPContainer
container	LDAPContainer

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

Active Directory Lightweight Directory Services project template for the generic LDAP connector

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

Table 47: 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 C

Generic LDAP connector settings

The following settings are configured for the system connection with the generic LDAP connector.

> NOTE: Some of the settings are only available if you set the **Configure advanced settings (expert mode)** option in the system connection wizard.

Table 48: Generic LDAP connector settings

Setting	Meaning
Server	IP address or full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects. Variable: `CP_Server`
Port	Communications port on the server. Default: **389** Variable: `CP_Port`
Authentication type	Authentication method for logging in to LDAP. The following are permitted: • **Basic**: Uses default authentication. • **Negotiate**: Uses Negotiate authentication from Microsoft. • **Anonymous**: Establishes a connection without passing login credentials. • **Kerberos**: Uses Kerberos authentication. • **NTLM**: Uses Windows NT Challenge/Response (NTLM) authentication. Default: **Basic** Variable: `CP_AuthenticationType` For more information about authentication types, see the MSDN Library.
User name	Name of the user account for logging in to LDAP. Variable: `CP_Username`

Setting	Meaning
Password	The user account’s password. Variable: `CP_Password`
Enable sealing	Specifies whether sealing is enabled.
Enable signing	Specifies whether signing is enabled.
Use SSL	SSL/TLS encrypted is used to establish a connection. Variable: `CP_UseSsl`
Use StartTLS	StartTLS is used for encryption. Variable: `CP_UseStartTls`
Protocol version	Version of the LDAP protocol. Default: **3**
Search base	Root entry for the search query, normally the LDAP domain. Variable: `CP_RootEntry`
Request timeout	Timeout for LDAP requests in seconds. Default: **3600** Variable: `CP_ClientTimeout`
Use paged search	Specifies whether LDAP objects are loaded by page. If you use this option (default), enter the page size.
Page size	Maximum number of objects to load per page. Default: **500**
Use DeleteTree control when deleting entries	Specifies if the LDAP server sends the **DeleteTree** control to delete entries with sub-entries during deletion. Variable:`CP_LDAP_UseDeleteTree`
Save LDAP schema in local cache	Specifies whether the LDAP schema should be kept in local cache. This accelerates synchronization and provisioning of LDAP objects. The cache is stored on the computer used to create the connection, under `%Appdata%\...\Local\One Identity\One Identity Manager\Cache\LdapConnector`. Default: **False** Variable: `CP_CacheSchema`
Object identification attribute	Attribute that can be used to uniquely identify the objects in LDAP. The attribute must be unique and set for all objects LDAP. Default: **entryUUID**

Setting	Meaning
	Variable: `CP_Guid_Attribute`
Revision properties	Properties used for revision filtering. Default: **createTimestamp**, **modifyTimestamp**
Define auxiliary classes	You can use this schema function to change the type of an object class. This may be necessary if a non-RFC compliant LDAP system allows assignment of several structural object classes to one entry although only one structural class is allowed. Assigning more than one structural class means that an LDAP entry cannot be uniquely assigned to a schema type. If structural object classes have been defined that only serve as property extensions (meaning **auxiliary** classes), you can, with help from this option, set the connector to handle the object class as an **auxiliary** class. NOTE: Object classes that are configured as **auxiliary** are subsequently not handled as independent schema types and cannot, therefore, be synchronized separately.
Virtual classes	Additional virtual classes. These support LDAP system that are non-RFC compliant and allow more that one structural class for each object.
Server supports renaming of entries	If set, the server supports renaming of entries. Default: **False**
Server supports moving of entries	If set, the server supports moving of entries. Default: **False**
Auxiliary class assignment	Assigns additional auxiliary classes to structural classes. 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. NOTE: To map the attributes of the auxiliary classes in One Identity Manager, custom extensions to the One Identity Manager schema may be necessary under certain circumstances. Use the Schema Extension program to do this.
Functional attributes	Attributes that are calculated for LDAP objects. Functional attributes are used for managing directories. Functional attributes are added to each schema class of the parent function. NOTE: To map the operational attributes in One Identity Manager, custom extensions to the One Identity Manager schema may be required. Use the Schema Extension program to do this.

Setting	Meaning
Identity dynamic groups	Attributes that contain the URL with search data for determining members of dynamic groups, for example `memberURL`.
Password attribute	Attribute that represents the password of a user account, for example, `userPassword`.
Password change method	Method for changing passwords. Permitted values are: • **Default**: Default method for changing the passwords. The password is written directly to the password attribute. • **ADLDS**: A password change method used for systems that are based on Microsoft Active Directory Lightweight Directory Services (AD LDS).

About us

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

Contacting us

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

Technical support resources

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

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

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

Index