ONE IDENTITY

by Quest

One Identity Manager 9.2

Administration Guide for Connecting to LDAP

Contents

About this guide

The *One Identity Manager Administration Guide for Connecting to LDAP* describes how you set up synchronization of LDAP with One Identity Manager. The guide explains how to use One Identity Manager to manage the user accounts and groups of your LDAP environment.

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

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

Available documentation

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

Managing LDAP environments

One Identity Manager allows administration of objects, such as identities, 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 identity 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 identities are provided with the necessary user accounts in One Identity Manager. Different mechanisms can be used to link identities to their user accounts. These user accounts can also be managed separately from identities 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.

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

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
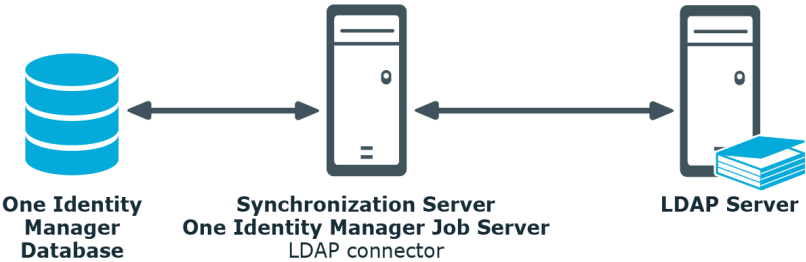
One Identity Manager users for managing LDAP

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

Table 1: Users

Users	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 identities to be target system

Users	Tasks
	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.
	• Create, change, or delete target system objects.
	• Edit password policies for the target system.
	• Prepare groups to add to the IT Shop.
	• Can add identities that do not have the **Primary identity** identity type.
	• 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 identities within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.
	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	Tasks
	Users with this application role: • Assign groups to IT Shop structures.
Product owner for the IT Shop	Product owners must be assigned to the **Request & Fulfillment | IT Shop | Product owners** application role or a child application role. Users with this application role: • Approve through requests. • Edit service items and service categories under their management.
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. Users with this application role: • Assign groups to business roles.

Configuration parameters for managing LDAP environments

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for various 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 175.

Synchronizing LDAP directories

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

NOTE:

- The LDAP connector requires the directory server to be RFC conform. In particular, the requirements of RFC 4514 (Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names) and RFC 4512 (Lightweight Directory Access Protocol (LDAP): Directory Information Models) must be ensured.

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

- The connected LDAP server should manage the referential integrity of entries itself. For example, the `Refint` plug-in from OpenLDAP (Overlays: Referential Integrity) If the server does not support this mechanism or it is not enabled, deleting or renaming can result in orphaned entries of referenced properties (for example `Member`).

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager 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 more 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

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, processes are created that are required to provision 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.

NOTE: Objects imported from different directory services that have the identical canonical names and distinguished names in the One Identity Manager database, could result in duplicate display values in current attestations, such as system entitlements, as well as in reports on target system objects and target system entitlements. Customizations may need to be made to attestation procedures and reports.

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.

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

   - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.

3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.

4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

Users and permissions for synchronizing with LDAP

The following users play a role 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 the One Identity Manager Service requires user permissions to carry out operations at file level (adding 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 permissions for the internal web service.
	NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions for the internal web service with the following command

User	Permissions
	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 run synchronization using an application server.

Related topics

- Special cases for synchronizing Active Directory Lightweight Directory Services on page 17
- Special cases for synchronizing Oracle Directory Server Enterprise Edition on page 19

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 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=Domain,DC=com`

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@<domain.com>`

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=Domain,DC=com`

- 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 run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.

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

Detailed information about this topic

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 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012

- Microsoft .NET Framework version 4.8 or later

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

Installing One Identity Manager Service with an LDAP connector

The One Identity Manager Service must be installed on the synchronization server with the LDAP connector. The synchronization server must be declared as a Job server in One Identity Manager.

Table 3: Properties of the Job server

Property	Value
Server function	LDAP connector
Machine role	Server | Job Server | 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).

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

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

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

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

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

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

2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.

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

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

1. Start the Server Installer program.

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

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

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

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

   a. Select a Job server from the **Server** menu.

      - OR -

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

   b. Enter the following data for the Job server.

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

steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.

- **Full server name**: Full server name in accordance with DNS syntax.

  Syntax:

  `<Name of 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 more information about configuring the service, see the *One Identity Manager Configuration Guide*.

   For a direct connection to the database:

   a. In the module list, select **Process collection > sqlprovider**.

   b. Click the **Connection parameter** entry, then click the **Edit** button.

   c. Enter the connection data for the One Identity Manager database.

   d. Click **OK**.

   For a connection to the application server:

   a. In the module list, select the **Process collection** entry and click the **Insert** button.

   b. Select **AppServerJobProvider** and click **OK**.

   c. In the module list, select **Process collection > AppServerJobProvider**.

   d. Click the **Connection parameter** entry, then click the **Edit** button.

   e. Enter the address (URL) for the application server and click **OK**.

   f. Click the **Authentication data** entry and click the **Edit** button.

   g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

   h. Click **OK**.

7. To configure the installation, click **Next**.

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

9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.

10. On the **Service access** page, enter the service's installation data.

    - **Computer**: Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.

      To run the installation locally, select **Local installation** from the menu.

    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

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

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

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

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

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

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

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 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 to set up a synchronization project on page 24
- Creating an initial synchronization project for an LDAP domain with the LDAP connector V2 on page 25

Information required to set 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	Authentication type for establishing a connection to the target system. 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 16.
Synchronization server for LDAP	All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The One Identity Manager Service with the 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. • Server function: **LDAP connector** • Machine role: **Server | Job Server | LDAP directories** For more information, see Setting up the LDAP synchronization server on page 19.
One Identity Manager database connection data	• Database server • Database name • SQL Server login and password

Data	Explanation
	• Specifies whether integrated Windows authentication is used
	Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	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 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*.

Creating an initial synchronization project for an LDAP domain with the LDAP connector V2

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

- Run in default mode
- Started from the Launchpad

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

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

To set up an initial synchronization project for an LDAP domain

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

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

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

   This starts the Synchronization Editor's project wizard.

1. On the **Choose target system** page, select **LDAP connector (version 2)**.

2. On the wizard's start page, click **Next**.

3. On the **System access** page, specify how One Identity Manager can access the target system.

   - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.

   - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.

4. On the **Connection credentials** page, enter the connection data for accessing the LDAP system. An attempt is then made to connect to establish a connection to the 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. The LDAP default communications port is **389**.

   - **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.

     - **External**: Uses certificate-based authentication as the external method.

     Depending on the selected authentication method, additional information may be required for logging in.

- **User name**: Name of the user account for logging in to LDAP.
- **Password**: Password for the user account.
- **Enable sealing**: Set this option if the selected authentication method supports sealing (**Sealing**).
- **Enable signing**: Set this option if the selected authentication method supports signing (**Signing**).
- **Client certificate**: Select a client certificate. The certificates are determined from the user certificates (**Current user** certificate store) on the currently connected host. This is either the local computer that the Synchronization Editor was started on or the Job server used for connecting remotely.

  NOTE: Ensure that the selected certificate is also installed on all Job servers that will connect to the LDAP system.

  TIP: By clicking 🛈 next to the field, you can display additional information about the selected certificate, for example, subject, certification authority and validity period.

- **Encryption**: Specify encryption for the connection. You have the following options:
  - **None**: No encryption is used.
  - **SSL**: An SSL/TLS encrypted connection is used.
  - **StartTLS**: StartTLS is used for encryption.
- **Server certificate verification**: The server certificate is checked during SSL or StartTLS encryption.

  NOTE: The server certificate must be valid. The root certification authority's certificate must be the computer certificate (**Local Computer** certificate store) either on the host that the Synchronization Editor was started on or on the Job server connected remotely. Ensure that the certificate is also installed on all Job servers that will connect to the LDAP system.

- **Protocol version**: Version of the LDAP protocol. The default value is **3**.

5. On the **Select the schema source** page, select the source to provide the schema information. You have the following options:
   - **Load schema from LDAP Server**: The schema is loaded from the LDAP. (Default)
   - **Load schema from given LDIF string**: If the LDAP server's schema is not available, you can give an alternative source.

To load the server's schema (default)

1. In the **Source** menu, select **Load schema from LDAP Server**.
2. (Optional) Click 🔄.

3. (Optional) To check the schema, click ☑.

    Errors that are found during analysis of the schema are displayed in the **Schema parsing errors** pane.

To load a schema from an LDIF string

1. In the **Source** menu, select **Load schema from given LDIF string**.

2. In the **Identifier** field, enter a name for the schema source.

3. Insert the schema definition straight into the field.

    - OR -

    Click 📁 and select the file containing the schema.

4. To check the schema, click ☑.

    Errors that are found during analysis of the schema are displayed in the **Schema parsing errors** pane. If you double-click on an error message, you jump to the corresponding place in the schema.

6. On the **Select configuration preset** page, specify how the connector is preconfigured. A configuration is already suggested based on the known server. Alternatively, you can enter the configuration manually. In this case, configure the setting for search queries, object changes, and object deletion.

    - **Use preset**: Enable this option if you want to use the configuration provided for the connector. A configuration is already suggested based on the known LDAP system. You have the following options:

        - OpenDJ

        - Oracle DSEE

        - Microsoft AD LDS or Active Directory

        - Novell/NetIQ eDirectory

    - **Configure manually**: Enable this option if you want to create the configuration manually. In this case, additional pages are offered on which you can specify the settings for search queries, object changes, and object deletion.

        1. On the **Search settings** page, set the options for LDAP search queries.

            The search function are structured hierarchically and are run in the order of configuration. Each search function is applied to the result of the previous search. The following search functions are available:

            - **Default Searcher**: Default search settings.

                - **Use paged search**: Specifies whether LDAP objects are loaded by page. This information is automatically queried through the selected preconfiguration or from the LDAP server. If the option is enabled, enter the page size.

- **Page size**: Enter the maximum number of objects to load per page. (Default **500**)

- **Remove spaces in distinguished names**: Removes all spaces in distinguished name objects that, according to RFC, are not allowed or non-significant.

  If the function does not exist, according to RFC, all spaces that are non allowed or non-significant are not removed from the distinguished name and can cause errors in certain circumstances.

- **AD (LDS) Search implementation**: Additional search settings for Active Directory Lightweight Directory Service.

  - **Chunk size**: If attributes with a large number of value are returned from a Microsoft based LDAP server, the server only sends a certain number of values back (normally 1500.) To query all the values, several queries with a scope limit are sent.

    The chunk size determines how many value are return per query. If the select chunk size is larger than the maximum size that the server can process, it is adjusted automatically.

    Enter the valid sizes: (Default **1000**)

To add a search function

1. In the **Search settings** pane, click ➕.

2. In the menu, select the search function and click 🖫.

   Change the order of the search functions using ⬆ and ⬇.

To edit a search function

- In the **Search settings** pane, select the search function and edit the configuration in the detailed view.

To delete a search function

- In the **Search settings** pane, select the search function and click 🗑.

2. On the **Modify settings** page, set additional options to modify the objects. The following options are available:

   - **Default Modify implementation**: Default implementation for modifying objects.

   - **Tolerate 'Attribute already exists' and 'no such attribute' and retry**: Use this function to tolerate existing or missing attributes in the LDAP system when an object is changed, for example, updating group memberships. (Default)

If this function is not available, changes to objects that affect existing or missing attribute in the LDAP system can cause errors.

To add functions

1. In the **Modify settings** pane, click ➕.
2. In the menu, select the function and click 💾.

To delete a function

- In the **Modify settings** pane, select the function and click 🗑.

3. On the **Delete settings** page, set additional options for deleting objects. The following options are available:

  - **Default delete implementation**: Default configuration for deleting objects.

    - **Use DeleteTree control when deleting entries**: Specifies whether the LDAP server sends the **DeleteTree** control to delete entries with sub-entries during deletion. This information is automatically queried through the selected preconfiguration or from the LDAP server.

To edit a function

- In the **Delete settings** pane, select the function and edit the configuration in the detailed view.

7. On the **LDAP schema extensions** page, configure additional schema functions that are run while the schema is being loaded.

   Schema functions are structured hierarchically. A schema function is always applied to its parent schema function. The connection processes schema functions hierarchically top-down. The following schema functions are available:

   - **Load schema from LDAP Server/Load schema for LDIF string**: Source for determining the schema.

   - **Return operational attributes**: This schema function specifies, which attributes are additionally found for the 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.

   - **Auxiliary class assigment**: Use schema function to assign additional auxiliary classes to structural classes. Auxiliary classes are classes of **Auxiliary** type 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.

- **Switch type of object classes**: 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.

- **Cache Schema**: This schema function keeps the LDAP schema stored in local cache. It is recommended to queue this function after the schema has loaded. 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.
  ```

- **Load AD LDS schema extension**: This schema function loads additional information required for synchronizing the Active Directory Lightweight Directory Service.

To add a schema function

1. In the **LDAP schema extensions** pane, click ➕.
2. In the menu, select the schema function and click 🖫.

   Change the order of the schema functions using ⬆ and ⬇.

To edit a schema function

- In the **LDAP schema extensions** pane, select the schema function and edit the configuration in the detailed view.

To delete a schema function

- In the **LDAP schema extensions** pane, select the schema function and click 🗑.

8. On the **Search base** page, define the root entry (normally the domain) that serves as the basis of the search queries. In the **Search base** menu, select an entry or enter a root value.

9. 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.

10. 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.

11. 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.

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

Table 5: Specify target system access

Option	Meaning
	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.
	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 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

Option	Meaning
	schema classes whose schema types have write access.

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

    If the synchronization server is not declared as a Job server for this target system 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.

       TIP: You can also implement an existing Job server as the synchronization server for this target system.

       - To select a Job server, click 🪄.

       This automatically assigns the server function matching this Job server.

    c. Click **OK**.

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

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

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

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

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

    NOTE:

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

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

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

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

Related topics

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 and synchronization workflow.

To configure the content of the synchronization log for a system connection

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

   - OR -

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

2. In the **General** section, click **Setup**.

3. In the **Synchronization log** section, 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**.

To configure the content of the synchronization log for a synchronization workflow

1. In the Synchronization Editor, select the **Workflows** category.

2. Select a workflow in the navigation view.

3. In the **General** section, click **Edit**.

4. Select the **Synchronization log** tab.

5. 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.

6. 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 53

Adjusting the synchronization configuration for LDAP environments

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 primary 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 method, 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.

- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

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

Detailed information about this topic

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

To create a synchronization configuration for synchronizing LDAP domains

1. In the Synchronization Editor, open the synchronization project.

2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.

3. Create a new workflow with the workflow wizard.

   This creates a workflow with **Target system** as its direction of synchronization.

4. Create a new start up configuration. Use the new workflow to do this.

5. Save the changes.

6. Run a consistency check.

Related topics

-

Configuring synchronization of 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 the domains are identical.
- All virtual schema properties used in the mapping must exist in the extended schema of the 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. In the Synchronization Editor, open the synchronization project.

3. Create a new base object for every other domain.

   - Use the wizard to attach a base object.
   - In the wizard, select the LDAP connector.
   - Declare the connection parameters. The connection parameters are saved in a special variable set.

   A start up configuration is created that uses the newly created variable set.

4. Change other elements of the synchronization configuration as required.

5. Save the changes.

6. Run a consistency check.

Related topics

- Configuring synchronization in LDAP domains on page 36

Support for the eduPerson object class

One Identity Manager supports the **eduPerson** object class. This object class is mainly used in directories of universities and colleges to simplify communication between institutions. For more information on **eduPerson**, see https://wiki.refeds.org/display/STAN/eduPerson.

The following schema properties are supported:

- EduPersonAffiliation
- EduPersonEntitlement
- EduPersonNickname
- EduPersonOrgDN
- EduPersonOrgUnitDN
- EduPersonPrimaryAffiliation
- EduPersonPrimaryOrgUnitDN
- EduPersonPrincipalName
- EduPersonPrincipalNamePrior
- EduPersonScopedAffiliation
- EduPersonTargetedId
- EduPersonAssurance
- EduPersonUniqueId
- EduPersonOrcId
- EduPersonAnalyticsTag

The schema properties are not mapped in the default template for synchronization projects. If you want to use the object class, customize the mapping in the Synchronization Editor. For more information about editing property mapping rules in the Synchronization Editor, see the *One Identity Manager Target System Synchronization Reference Guide*.

Create custom templates and formatting rule as required. For more information about customizing the One Identity Manager schema, see the *One Identity Manager Configuration Guide*.

Related topics

- EduPerson extensions for LDAP user accounts on page 148

Changing system connection settings of LDAP domains

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

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 is used for synchronizing different LDAP domains.

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.

   Some connection parameters can be converted to variables here. For other parameters, variables are already created.

4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.

All specialized variable sets are shown in the lower part of the document view.

6. Select a specialized variable set or click on ⊞ in the variable set view's toolbar.

   - To rename the variable set, select the variable set and click the variable set view in the toolbar 🏷. Enter a name for the variable set.

7. Select the previously added variable and enter a new value.

8. Select the **Configuration > Start up configurations** category.

9. Select a start up configuration and click **Edit**.

10. Select the **General** tab.

11. Select the specialized variable set in the **Variable set** menu.

12. Select the **Configuration > Base objects** category.

13. Select the base object and click 📝.

    - OR -

    To add a new base object, click ⊞ .

14. Select the specialized variable set in the **Variable set** menu.

15. Save the changes.

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

Related topics

- Editing target system connection properties on page 40

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. In the Synchronization Editor, open the synchronization project.

2. In the toolbar, select the active variable set to be used for the connection to the target system.

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

3. Select the **Configuration > Target system** category.

4. Click **Edit connection**.

   This starts the system connection wizard.

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

6. Save the changes.

Related topics

-

Extended schema configuration with the LDAP connector V2

By preconfiguring this connector that you can select in the system connection wizard, the required schema configuration is already set up. If, in exceptional cases, it becomes necessary to make changes you can use the system connection wizard to configure schema types, schema properties, and methods.

IMPORTANT: Changes to the schema configuration should only be carried out by experienced Synchronization Editor users and system administrators.

NOTE: To make advanced settings, on the start page of the system connection wizard, set the **Configure advanced settings** option.

On the **Connector schema configuration** page, a hierarchical meta schema is displayed showing the schema types that will be created. You can add, edit, or delete schema classes, schema properties, and methods. The information displayed is similar to the information in the Synchronization Editor.

Use these setting to:

- Specify which schema property is used for revision filtering.
- Specify which schema property is used to uniquely identify an object.
- Define virtual schema types if necessary.

Implementation types

NOTE: Global settings for implementing read and write access are stored in the **Schema** entry on the **Connector schema configuration**.

Table 6: Implementation

Implementation	Meaning
Query implementation	Implementation used for calling up entries from the LDAP server.
	The `DefaultQueryStrategy` implementation uses the configured LDAP connection to call up entries.
Type resolution implementation	The implementation that inspects LDAP entries returned by LDAP servers to determine and assign the connector schema type for the resulting connector object.
	This option can only be changed in the through the user with the `Request & Fulfillment | | Administrators` application role.
Read access implementation	Implementation converts a schema property's values based on an LDAP entry.
Reference handling	Implementation for creating or resolving reference values of an LDAP entry's schema property. A reference in LDAP is usually a property pointing to another entry through a distinguished name.
Commit implementation	The implementation to be used when entries are saved by the connector to the LDAP server.
	The `DefaultCommitStrategy` implementation calls the methods `Insert`, `Update`, or `Delete` depending on the state of the object.
Insert method implementation	Implementation to use for the schema types' `Insert` method.
	The `DefaultInsertMethodStrategy` implementation will send `add` requests to the LDAP server to publish new entries.
Update method implementation	Implementation to use for the schema types' `Update` method.
	The `DefaultUpdateMethodStrategy` implementation sends `modify` and `modifydn` requests to the LDAP server to publish changes to existing entries.
Implementation for delete method	Implementation to use for the schema types' `Delete` method.
	The `DefaultDeleteMethodStrategy` implementation sends `delete` requests to the LDAP server to delete existing entries.

Schema property handler

Handler	Meaning
DNBackLinkPropertyHandler	Backlink handler. This handler resolves backlinks between schema properties.
	Example:
	This handler is configured for the group's `Member` schema property. The `MemberOf` schema property is

Handler	Meaning
	selected as **Backlink property**.
	If a user account is assigned to a group, the user account is entered in the in the target system in the group's `Member` schema property. The handler determines the referenced object, in this case, the user account and enters the group reference in the `MemberOf` schema property.
MirrorPropertyHandler	Mirror property handler This handler transfers values and changes of a schema property, for which the handler is defined, to the schema property given under **Mirror property**.
	Example:
	This handler is configured for the group's `Member` schema property. The `equivalentToMe` schema property is selected as **Mirror property**.
	If a user account is assigned to a group, the user account is entered in the in the target system in the group's `Member` schema property. This is also added to the `equivalentToMe` schema property.
RdnPropertyHandler	This handler handles the `vrtEntryRDN` virtual schema property. The `vrtEntryRDN` schema property represents the relative distinguished names of the entry. The distinguished name is made up of one or more pairs of attribute name and attribute value combined, with the syntax `<attribute name>=<attribute value>[+<attribute name>=<attribute value>]`
	Examples:
	`CN=Pat Identity1`
	`OU=Sales`
	`CN=Jo User1+UID=char`
	The handler ensures that when the `vrtEntryRDN` is set, the matching referenced property of the LDAP entry is set the same.
	Example:
	If the `vrtEntryRDN` has the value **CN=Pat Identity1**, the `CN` property is set to **Pat Identity1**.
	If the `vrtEntryRDN` has the value **OU=Sales**, the `OU` property is set to **Sales**.

Handler	Meaning
	If the `vrtEntryRDN` has the value **CN=Jo User1+UID=char**, the `CN` property is set to **Jo User1UID** and the `UID` is given the value **char**.
DefaultValueModificationHandler	This handler ensures that there is always at least one defined default value is written to a schema property. This can currently be free text or the distinguished name of the object that the value is defined on, such as a group.
	A `CheckForDefaultValueAction` operation is queued at the start and when changes are made to the schema property that was assigned to the handler.
	The handler ensure the following behavior:
	• If the object was just added, it checks that the schema property contains a value. If this is not the case, the default value is written to the schema property.
	• If this is a change, first the property is loaded from the target system.
	There are the following possible cases:
	• In LDAP, the schema property is already set to the default value. The pending change will allocate another (additional) value to the schema property.
	The default value is removed from the schema property in LDAP and the new value is allocated to the schema property.
	• In LDAP, the schema property is not set to the default value yet. The pending change will clear the schema property or delete the last value, for example.
	In LDAP, the default value is allocated to the schema property.

To edit a schema type

- In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

  On the right-side of the view, you can see the schema type's properties.

To add a simple virtual schema type

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane and click ➕.

2. Edit the schema type properties.

To create a virtual schema type from several schema classes

1. In the system connection wizard on the **Connector schema configuration** page, in the **Schema** pane, select the schema classes to be combined using **Ctrl + select** and click 📄.

2. Edit the schema type properties.

To delete a virtual schema type

- In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane and click ❌.

To edit a method

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

2. In **Methods**, select the method.

   On the right-side of the view, you can see the method's properties.

To add a method

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

2. Select the **Methods** item and click ➕.

3. Edit the method's properties.

To delete a method

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

2. Select the method in the **Methods** list and click ❌.

To edit a schema property

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

2. Select the schema property in the **Properties** list.

   On the right-side of the view, you can see the schema property's attributes.

To add a virtual schema property

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

2. Select the **Properties** item and click ⊕.

3. Edit the schema property details.

To delete a virtual schema property

1. In the system connection wizard on the **Connector schema configuration** page, select the schema type in the **Schema** pane.

2. Select the schema property in the **Properties** list and click ⊗.

Related topics

- Editing target system connection properties on page 40
- LDAP connector V2 settings on page 183

Updating schemas

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

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

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

- A schema was changed by:
    - Changes to a target system schema
    - Customizations to the One Identity Manager schema
    - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
    - Enabling the synchronization project
    - Saving the synchronization project for the first time
    - Compressing a schema

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.

2. Select the **Configuration > Target system** category.

   - OR -

   Select the **Configuration > One Identity Manager connection** category.

3. Select the **General** view and click **Update schema**.

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

   This reloads the schema data.

To edit a mapping

1. In the Synchronization Editor, open the synchronization project.

2. Select the **Mappings** category.

3. Select a mapping in the navigation view.

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

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

Speeding up synchronization with revision filtering

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 date it was run on 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

- In the Synchronization Editor, open the synchronization project.
- Edit the workflow properties. Select the **Use revision filter** item from **Revision filtering** menu.

To permit revision filtering for a start up configuration

- In the Synchronization Editor, open the synchronization project.
- 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 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 as an object property in list form in the target system.

  Example: List of user accounts in the `Member` property of an LDAP group (`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. In the result list, select the **LDAP** target system type.
3. Select the **Configure tables for publishing** task.

4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.

5. Click **Merge mode**.

   NOTE:

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

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

     Example: `LDAPAccountInLDAPGroup`, `LDAPGroupInLDAPGroup`, and `LDAPMachineInLDAPGroup`

6. Save the changes.

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

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

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

To restore the original condition

1. Select the auxiliary table for which you want to restore the condition.

2. Right-click on the selected row and select the **Restore original values** context menu item.

3. Save the changes.

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

Example of a condition on the `LDAPAccountInLDAPGroup` assignment table:

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

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

Configuring single object synchronization

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

Prerequisites

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

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

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

1. In the Manager, select the **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: `FK(UID_LDPDomain).XObjectKey`
8. Save the changes.

Related topics

- Synchronizing single objects on page 55
- Post-processing outstanding objects on page 56

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

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

   - Job servers that share processing must have the **No process assignment** option enabled.

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

Detailed information about this topic

   - Editing LDAP Job servers on page 168

Running synchronization

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

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

Detailed information about this topic

- Starting synchronization on page 52
- Deactivating synchronization on page 54
- Displaying synchronization results on page 53
- Synchronizing single objects on page 55
- Pausing handling of target system specific processes (Offline mode) on page 60

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.

3. Select a start up configuration in the document view and click **Run**.

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

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.

  - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.

- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.

  - Use the schedule to ensure that the start up configurations are run in sequence.

  - Group start up configurations with the same start up behavior.

Displaying synchronization results

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

To display a synchronization log

1. In the Synchronization Editor, open the synchronization project.

2. Select the **Logs** category.

3. Click ▶ in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.

4. Select a log by double-clicking it.

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

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.

2. Select the **Logs** category.

3. Click ⚡ in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.

4. Select a log by double-clicking it.

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

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

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

Related topics

- Configuring the synchronization log on page 34
- Troubleshooting on page 59

Deactivating synchronization

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

To prevent regular synchronization

1. In the Synchronization Editor, open the synchronization project.
2. Select the start up configuration and deactivate the configured schedule.

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited 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. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of an LDAP domain on page 23
- Pausing handling of target system specific processes (Offline mode) on page 60

Synchronizing single objects

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

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

To synchronize a single object

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

2. Select the object type in the navigation view.

3. In the result list, select the object that you want to synchronize.

4. Select the **Synchronize this object** task.

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

Features of synchronizing memberships

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

Example:

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

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

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

Detailed information about this topic

- Configuring single object synchronization on page 50

Tasks following synchronization

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

Post-processing outstanding objects

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.

   The navigation view lists all the synchronization tables assigned to the **LDAP** target system type.

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

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

   - The synchronization log has already been deleted.

     - OR -

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

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

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

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

To display object properties of an outstanding object

1. Select the object on the target system synchronization form.

2. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.

4. Click on one of the following icons in the form toolbar to run the respective method.

Table 7: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account.
		Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object.
		This runs a target system specific process that triggers the provisioning process for the object.
		Prerequisites:
		• 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.

TIP: If a method cannot be run due to certain restrictions, the respective icon is disabled.

- To display the constraint's details, click the **Show** button in the **Constraints** column.

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

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

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

To disable bulk processing

- Disable the 🗇 icon in the form's toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the

Connection is read-only option must not be set for the target system connection.

Adding custom tables to the target system synchronization

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

To add custom tables to target system synchronization

1. In the Manager, select the **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 56

Managing LDAP user accounts through account definitions

In the default installation, after synchronizing, identities are automatically created for the user accounts.If an account definition for the domain is not known at the time of synchronization, user accounts are linked with identities. 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 89

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

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

- Analyzing synchronization

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

- Logging messages

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

- Reset start information

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

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

Related topics

Ignoring data error in synchronization

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

To ignoring data errors during synchronization in One Identity Manager

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > One Identity Manager connection** category.
3. In the **General** view, click **Edit connection**.

   This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

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

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

5. Save the changes.

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

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

Pausing handling of target system specific processes (Offline mode)

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

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

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

Prerequisites

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

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

To allow offline mode for a base object

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

4. Enable **Offline mode available**.

5. Click **OK**.

6. Save the changes.

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

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

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

To flag a target system as offline

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

2. Select **Manage > System monitoring > Flag target systems as offline**.

3. Click **Run**.

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

4. Select the base object whose target system connection is not available.

5. Click **Switch offline**.

6. Confirm the security prompt with **OK**.

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

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

Related topics

- Deactivating synchronization on page 54

Managing LDAP user accounts and identities

The main feature of One Identity Manager is to map identities together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to identities. This provides an overview of the permissions for each identity 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. Identities 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 identities. One Identity Manager supports the following methods for linking identities and their user accounts:

- Identities can automatically obtain their account definitions using user account resources.

  If an identity does not yet have a user account in a LDAP domain, a new user account is created. This is done by assigning account definitions to an identity using the integrated inheritance mechanisms and subsequent process handling.

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

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

- Identities and user accounts can be entered manually and assigned to each other.

For more information about basic handling and administration of identities and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

Account definitions for LDAP user accounts

One Identity Manager has account definitions for automatically allocating user accounts to identities. You can create account definitions for every target system. If an identity 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 identity.

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

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

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

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 identities and target systems

Detailed information about this topic

Creating account definitions

Create one or more account definitions for the target system.

To create a new account definition

1. In the Manager, select the **LDAP > Basic configuration data > Account definitions > Account definitions** category.
2. Click ![plus icon] in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Detailed information about this topic

Editing account definitions

You can edit the main data of account definitions.

To edit 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 **Change main data** task.

4. Enter the account definition's main data.

5. Save the changes.

Related topics

- Main data for account definitions on page 65
- Creating account definitions on page 64
- Assigning manage levels to account definitions on page 69

Main data for account definitions

Enter the following data for an account definition:

Table 8: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. 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 assigning the account

ONE IDENTITY
by Quest

Property	Description
	definition to identities. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set.
	For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The resource can also be assigned directly to identities 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. This account definition can be requested through the Web Portal and allocated by defined approval processes. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to identities	Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the **Enable automatic assignment to identities** The account definition is assigned to every identity that is not marked as external. Once a new internal identity is created, they automatically obtain this account definition.
	To automatically remove the account definition assignment from all identities, use the **Disable automatic assignment to identities**. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated identities.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): 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 deactivated identities.
	Option set: The account definition assignment remains in effect. The user account remains intact.

Property	Description
	Option not set (default): 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 identities.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): 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 identities posing a security risk.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): 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.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.
	• If you add an identity 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 identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the identity but they do no inherit any further properties. When a new user account is added with this manage level and an identity is assigned, some of the identity's properties are transferred initially. If the identity 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 identity. When a new user account is created with this manage level and an identity is assigned, the identity's properties are transferred in an initial state. If the identity 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 how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

- Identity user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the identity 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 identity's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this identity. Existing group memberships are deleted.

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.
3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

Related topics

- Main data for manage levels on page 70
- Creating manage levels on page 68
- Assigning manage levels to account definitions on page 69

Creating manage levels

One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

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

To create a manage level

1. In the Manager, select the **LDAP > Basic configuration data > Account definitions > Manage levels** category.

2. Click ▮ in the result list.

3. On the main data form, edit the main data of the manage level.

4. Save the changes.

Related topics

- Main data for manage levels on page 70
- Editing manage levels on page 67
- Assigning manage levels to account definitions on page 69

Assigning manage levels to account definitions

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

To assign manage levels to an account definition

1. In the Manager, select the **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 level.

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

   ### To remove an assignment

   - Select the manage level and double-click ⊘.

5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 9: Main data for manage levels

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

Creating mapping rules for IT operating data

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

The following IT operating data is used in the One Identity Manager default configuration for automatically creating user accounts for an identity 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.

4. Click **Add** and enter the following information:

    - **Column**: User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

    - **Source**: Specifies which roles to use in order to find the user account properties. You have the following options:

        - Primary department

        - Primary location

        - Primary cost center

        - Primary business roles

          NOTE: The business role can only be used if the Business Roles Module is available.

        - Empty

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

    - **Default value**: Default value of the property for an identity's user account if the value is not determined dynamically from the IT operating data.

- **Always use default value**: Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.

- **Notify when applying the default**: Specifies whether an email is sent to a specific mailbox when the default value is used. The **Identity - new user account with default properties created** mail template is used.

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

5. Save the changes.

Related topics

Entering IT operating data

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity 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 identity in department A obtains a default user account in the domain A. In addition, certain identities in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

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

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.

2. Select the **Edit IT operating data** task.

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

    *   **Effects on**: Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

        ### *To specify an application scope*

        a. Click ➔ next to the field.

        b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table or an account definition.

        c. Select the specific target system or account definition under **Effects on**.

        d. Click **OK**.

    *   **Column**: Select the user account property for which the value is set.

        In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

    *   **Value**: Enter a fixed value to assign to the user account's property.

4. Save the changes.

Related topics

*   Creating mapping rules for IT operating data on page 71
*   Modify IT operating data on page 73

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 identity to a primary department, cost center, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

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

2. Select an account definition in the result list.

3. Select the **Run templates** task.

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

   - **Old value**: Value of the object property before changing the IT operating data.

   - **New value**: Value of the object property after changing the IT operating data.

   - **Selection**: Specifies whether the new value is copied to the user account.

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

5. Click **Apply**.

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

Assigning account definitions to identities

Account definitions are assigned to company identities.

Indirect assignment is the default method for assigning account definitions to identities. Account definitions are assigned to departments, cost centers, locations, or roles. The identities 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 identities.

You can automatically assign special account definitions to all company identities. 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 identities 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 identity already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

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

NOTE: As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

Prerequisites for indirect assignment of account definitions to identities

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task and configure the permitted assignments.

   - To generally allow an assignment, enable the **Assignments allowed** column.

   - To allow direct assignment, enable the **Direct assignments permitted** column.

3. Save the changes.

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

Detailed information about this topic

Assigning account definitions to departments, cost centers, and locations

Assign account definitions to departments, cost centers, and locations in order to assign identities to them through these organizations.

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 76
- Assigning account definitions to all identities on page 77
- Assigning account definitions directly to identities on page 78
- Assigning account definitions to system roles on page 78
- Adding account definitions in the IT Shop on page 79

Assigning account definitions to business roles

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

You can assign account definitions to business roles in order to assign them to identities through business roles.

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, select the role class and assign business roles.

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

> ***To remove an assignment***
> - Select the business role and double-click ✅.

5. Save the changes.

Related topics

  - Assigning account definitions to departments, cost centers, and locations on page 75
  - Assigning account definitions to all identities on page 77
  - Assigning account definitions directly to identities on page 78
  - Assigning account definitions to system roles on page 78
  - Adding account definitions in the IT Shop on page 79

Assigning account definitions to all identities

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

IMPORTANT: Only run this task if you can ensure that all current internal identities in the database and all pending newly added internal identities obtain a user account in this target system.

To assign an account definition to all identities

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 main data** task.
4. Select the **Disable automatic assignment to identities** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all identities, run the DISABLE AUTOMATIC ASSIGNMENT TO IDENTITIES task. The account definition cannot be reassigned to identities from this point on. Existing assignments remain intact.

Related topics

  - Assigning account definitions to departments, cost centers, and locations on page 75
  - Assigning account definitions to business roles on page 76
  - Assigning account definitions directly to identities on page 78

- Assigning account definitions to system roles on page 78
- Adding account definitions in the IT Shop on page 79

Assigning account definitions directly to identities

Account definitions can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and account definitions in company structures, like departments, cost centers, locations, or business roles.

To react quickly to special requests, you can assign account definitions directly to identities.

To assign an account definition directly to identities

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 identities** task.

4. In the **Add assignments** pane, add identities.

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

   ### To remove an assignment

   - Select the identity and double-click ⊘.

5. Save the changes.

Related topics

Assigning account definitions to system roles

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

Use this task to add an account definition to system roles.

NOTE: Account definitions with the **Only use in IT Shop** option set 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.

Related topics

Adding account definitions in the IT Shop

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

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

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

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

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

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

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.

5. Save the changes.

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

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

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.

5. Save the changes.

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

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.

5. Save the changes.

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

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

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.

5. Save the changes.

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

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

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

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

5. Click **OK**.

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

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

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

2. Select an account definition in the result list.

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

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

5. Click **OK**.

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

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

Related topics

- Main data for account definitions on page 65
- Assigning account definitions to departments, cost centers, and locations on page 75
- Assigning account definitions to business roles on page 76
- Assigning account definitions to all identities on page 77
- Assigning account definitions directly to identities on page 78
- Assigning account definitions to system roles on page 78

Assigning account definitions to LDAP domains

The following prerequisites must be fulfilled if you implement automatic assignment of
user accounts and identities 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 identity (**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 main 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

-

Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all identities.

   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 main data** task.

   d. Select the **Disable automatic assignment to identities** task.

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

   f. Save the changes.

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

   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 identities** task.

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

   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.

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

   e. Save the changes.

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

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

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

   a. In the Manager, select the **Entitlements > Account definitions** category.

   b. Select an account definition in the result list.

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

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

   e. Click **OK**.

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

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

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

   b. Select an account definition in the result list.

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

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

   e. Click **OK**.

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

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

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

   b. Select an account definition in the result list.

   c. Select the **Change main data** task.

   d. From the **Required account definition** menu, remove the account definition.

   e. Save the changes.

7. Remove the account definition's assignments to target systems.

   a. In the Manager, select the domain in the **LDAP > Domains** category.

   b. Select the **Change main data** task.

   c. On the **General** tab, remove the assigned account definitions.

   d. Save the changes.

8. Delete the account definition.

   a. In the Manager, select the **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.

Assigning identities automatically to LDAP user accounts

When you add a user account, an existing identity can automatically be assigned to it. If necessary, a new identity can be created. The identity main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either manually or through synchronization.

Define criteria for finding identities to apply to automatic identity assignment. If a user account is linked to an identity 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 identities 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 identity assignments to user accounts remain intact.

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

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

Run the following tasks to assign identities automatically.

- If you want identities 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 identities 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 identities 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 identities assigned to the domain.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

In the default installation, after synchronizing, identities are automatically created for the user accounts.If an account definition for the domain is not known at the time of synchronization, user accounts are linked with identities. 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 58.

Related topics

- Creating account definitions on page 64
- Assigning account definitions to LDAP domains on page 81
- Changing manage levels for LDAP user accounts on page 88
- Assigning account definitions to linked LDAP user accounts on page 89
- Editing search criteria for automatic identity assignment on page 86

Editing search criteria for automatic identity assignment

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

The criteria for identity assignments are defined for the domain. You specify which user account properties must match the identity's properties such that the identity 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 identity assignment** column (`AccountToPersonMatchingRule`) in the `LDAPDomain` table.

Search criteria are evaluated when identities are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of identities to user accounts based on the search criteria and make the assignment directly.

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

To specify criteria for identity 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 identity assignment** task.
4. Specify which user account properties must match with which identity so that the identity is linked to the user account.

    Table 10: Search criteria for user accounts

Apply to	Identity column	Column for user account
LDAP user accounts	Central user account (CentralAccount)	Login name (UserID)

5. Save the changes.

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

Related topics

- Assigning identities automatically to LDAP user accounts on page 84
- Finding identities and directly assigning them to user accounts on page 87

Finding identities and directly assigning them to user accounts

Based on the search criteria, you can create a suggestion list for the assignment of identities to user accounts and make the assignment directly. User accounts are grouped in different views for this.

- **Suggested assignments**: This view lists all user accounts to which One Identity Manager can assign an identity. All identities are shown that were found using the search criteria and can be assigned.

- **Assigned user accounts**: This view lists all user accounts to which an identity is assigned.

- **No identity assignment**: This view lists all user accounts to which no identity is assigned and for which no identity was found using the search criteria.

NOTE: To display disabled user accounts or deactivated identities in the view, enable the **Even locked accounts are mapped** option.

If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.

To apply search criteria to user accounts

1. In the Manager, select the **LDAP > Domains** category.

2. Select the domain in the result list.

3. Select the **Define search criteria for identity assignment** task.

4. At the bottom of the form, click **Reload**.

   All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

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

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

To assign identities directly to user accounts

- Click **Suggested assignments**.

  1. Click the **Selection** box of all user accounts to which you want to assign the suggested identities. Multi-select is possible.

  2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.

  3. Click **Assign selected**.

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

   The identities determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

- OR -

- Click **No identity assignment**.

  1. Click **Select identity** for the user account to which you want to assign an identity. Select an identity from the menu.

  2. Click the **Selection** box of all user accounts to which you want to assign the selected identities. Multi-select is possible.

  3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.

  4. Click **Assign selected**.

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

     The identities displayed in the **Identity** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.

  1. Click the **Selection** box of all the user accounts with the identity assignment you want to delete. Multi-select is possible.

  2. Click **Remove selected**.

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

     The assigned identities are removed from the selected user accounts.

Changing manage levels for LDAP user accounts

The default manage level is applied if you create user accounts using automatic identity 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 main data** task.

4. Select the manage level in the **Manage level** list on the **General** tab.

5. Save the changes.

Related topics

- Creating LDAP user accounts on page 140

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:

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

To manage 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 81

Manually linking identities to LDAP user accounts

An identity can be linked to multiple LDAP user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One identity can also use default user accounts with different types.

To manually assign user accounts to an identity

1. In the Manager, select the **Identities > Identities** category.

2. Select the identity in the result list and run the **Assign LDAP user accounts** task.

3. Assign the user accounts.

4. Save the changes.

Related topics

Supported user account types

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

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

- Identity type

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

Table 11: Identity types of user accounts

Identity type	Description	Value of the IdentityType column
Primary identity	Identity's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the company, for example for subcontracts with other functional areas.	Organizational
Personalized administrator identity	User account with administrative permissions, used by an identity.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by multiple identities.	Shared
Service identity	Service account.	Service

- Privileged user account

  Privileged user accounts are used to provide identities 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

Normally, each identity obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the identity. The effect of the link and the scope of the identity'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 how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level.

3. Create a formatting rule for IT operating data.

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

   The type of IT operating data 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 identities.

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

Related topics

- Account definitions for LDAP user accounts on page 63

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 identity on page 92
- Providing administrative user accounts for several people on page 93

Providing administrative user accounts for one identity

Use this task to create an administrative user account that can be used by an identity.

Prerequisites

- The user account must be labeled as a personalized administrator identity.
- The identity that will be using the user account must be marked as a personalized administrator identity.
- The identity that will be using the user account must be linked to a main identity.

To prepare an administrative user account for an identity

1. Label the user account as a personalized administrator identity.

   a. In the Manager, select the **LDAP > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

   d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.

2. Link the user account to the identity that 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 main data** task.

   d. On the **General** tab, in the **Identity** selection list, select the identity that will be using this administrative user account.

      TIP: If you are the target system manager, you can selected 🔼 to create a new identity.

Related topics

- Providing administrative user accounts for several people on page 93

- For more information about mapping identity types, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several people

Use this task to create an administrative user account that can be used by more that one identity.

Prerequisite

- The user account must be labeled as a shared identity.

- There must be an identity with the type **Shared identity** available. The shared identity must have a manager.

- The identities who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple identities

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 main data** task.

    d. On the **General** tab, in the **Identity** menu, select **Shared identity**.

2. Link the user account to an identity.

    a. In the Manager, select the **LDAP > User accounts** category.

    b. Select the user account in the result list.

    c. Select the **Change main data** task.

    d. On the **General** tab, in the **Identity** menu, select an identity the type **Shared identity**.

       TIP: If you are the target system manager, you can use the 🔳 button to create a new shared identity.

3. Assign the identities 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 identities authorized to use** task.

    d. In the **Add assignments** pane, add identities.

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

       To remove an assignment

       • Select the identity and double-click ✅.

Related topics

- Providing administrative user accounts for one identity on page 92
- For more information about mapping identity types, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

Privileged user accounts are used to provide identities 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 how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships in the manage level.

4. Create a formatting rule for the IT operating data.

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

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

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.

   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.

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

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

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

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

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

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, specify how the login names are formatted in the template.

- 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. If necessary, modify the schedule in the Designer.

Related topics

- Account definitions for LDAP user accounts on page 63

Specifying deferred deletion for LDAP user accounts

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

You have the following options for configuring deferred deletion.

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

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

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

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

Example:

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

```
If Not $IsPrivilegedAccount:Bool$ Then

    Value = 10

End If
```

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

Managing memberships in LDAP groups

LDAP user accounts and LDAP computers can be grouped into LDAP groups that can be used to regulate access to resources.

In One Identity Manager, you can assign LDAP groups directly to LDAP user accounts and LDAP computers or they can be inherited through departments, cost centers, locations, or business roles. Users can also request the groups through the Web Portal. To do this, groups are provided in the IT Shop.

Detailed information about this topic

- Assigning LDAP groups to LDAP user accounts and LDAP computers in One Identity Manager on page 97
- Effectiveness of membership in LDAP user groups on page 108
- LDAP group inheritance based on categories on page 110
- Overview of all assignments on page 113

Assigning LDAP groups to LDAP user accounts and LDAP computers in One Identity Manager

You can assign LDAP groups directly or indirectly to LDAP user accounts and LDAP computers. Identities (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 identity (workdesk or device) is calculated from the position within the hierarchy and inheritance direction.

- If you add an identity to roles and that identity 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.

Furthermore, LDAP groups can be requested through the Web Portal. To do this, add identities 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 identities after approval is granted.

Through system roles, LDAP groups can be grouped together and assigned to identities and workdesks as a package. You can create system roles that contain only LDAP groups. You can also group any number of company resources into a system role.

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

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting 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

Prerequisites for indirect assignment of LDAP groups

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

Prerequisites for indirect assignment of LDAP groups to the LDAP user accounts of identities

1. Assignment of identities and LDAP groups is permitted for role classes (departments, cost centers, locations, or business roles).
2. The LDAP user account is linked to an identity.
3. The LDAP user account is labeled with the **Groups can be inherited** option.

Prerequisites for indirect assignment of LDAP groups to LDAP computers

1. Assignment of devices and LDAP groups is permitted for role classes (departments, cost centers, locations, or business roles).
2. The LDAP computer is connected to a device.
3. The device is labeled as a PC or server.
4. The **TargetSystem | LDAP | HardwareInGroupFromOrg** configuration parameter is set.

Prerequisites for indirect assignment to LDAP groups to LDAP computers through workdesks

1. Assignment of workdesks and LDAP groups is permitted for role classes (departments, cost centers, locations, or business roles).
2. The LDAP computer is connected to a device.
3. The device is labeled as a PC or server.
4. The device owns a workdesk.

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task and configure the permitted assignments.

  - To generally allow an assignment, enable the **Assignments allowed** column.
  - To allow direct assignment, enable the **Direct assignments permitted** column.

3. Save the changes.

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

Related topics

Assigning LDAP groups to departments, cost centers, and locations

Assign groups to departments, cost centers, or locations so that the group can be assigned to user accounts and computers through these organizations. This task is not available for dynamic groups.

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, a cost center, or a location (non role-based login or 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

- Prerequisites for indirect assignment of LDAP groups on page 99
- Assigning LDAP groups to business roles on page 101
- Adding LDAP groups to system roles on page 102
- Adding LDAP groups to the IT Shop on page 103
- Assigning LDAP user accounts directly to LDAP groups on page 105
- Assigning LDAP groups directly to LDAP user accounts on page 106
- Assigning LDAP computers directly to LDAP groups on page 107
- Assigning LDAP groups directly to LDAP computers on page 107
- One Identity Manager users for managing LDAP on page 11

Assigning LDAP groups to business roles

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

Assign the group to business roles so that the group is assigned to user accounts and computers through these business roles. This task is not available for dynamic groups.

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, select the role class and assign business roles.

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

   To remove an assignment

   - Select the business role and double-click ✅.

5. Save the changes.

To assign groups to a business role (non role-based login or 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 the groups.

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

   To remove an assignment

   - Select the group and double-click ✅.

5. Save the changes.

Related topics

Adding LDAP groups to system roles

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

Use this task to add a group to system roles.

If you assign a system role to identities, all LDAP user accounts owned by these identities inherit the group.

If you assign a system role to workdesks, all LDAP computers associated with this workdesk 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 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

- Prerequisites for indirect assignment of LDAP groups on page 99
- Assigning LDAP groups to departments, cost centers, and locations on page 100
- Assigning LDAP groups to business roles on page 101
- Adding LDAP groups to the IT Shop on page 103
- Assigning LDAP user accounts directly to LDAP groups on page 105
- Assigning LDAP groups directly to LDAP user accounts on page 106
- Assigning LDAP computers directly to LDAP groups on page 107
- Assigning LDAP groups directly to LDAP computers on page 107

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 identities 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** (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. Select the **IT Shop structures** tab.

5. In the **Add assignments** pane, assign the group to the IT Shop shelves.

6. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager, select the **LDAP > Groups** (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. Select the **IT Shop structures** tab.

5. In the **Remove assignments** pane, remove the group from the IT Shop shelves.

6. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **LDAP > Groups** (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 information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Prerequisites for indirect assignment of LDAP groups on page 99
- LDAP group main data on page 154
- Assigning LDAP groups to departments, cost centers, and locations on page 100
- Assigning LDAP groups to business roles on page 101
- Adding LDAP groups to system roles on page 102
- Assigning LDAP user accounts directly to LDAP groups on page 105
- Assigning LDAP groups directly to LDAP user accounts on page 106
- Assigning LDAP computers directly to LDAP groups on page 107
- Assigning LDAP groups directly to LDAP computers on page 107
- One Identity Manager users for managing LDAP on page 11

Assigning LDAP user accounts directly to LDAP groups

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

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 user accounts directly to a group

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 the **Add assignments** pane, assign the user accounts.

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

   To remove an assignment

   - Select the user account and double-click ⊘.

5. Save the changes.

Related topics

Assigning LDAP groups directly to LDAP user accounts

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

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 the groups.

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

   To remove an assignment
   - Select the group and double-click ⊘.
5. Save the changes.

Related topics

Assigning LDAP computers directly to LDAP groups

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.

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

   ### *To remove an assignment*

   - Select the computer and double-click ⊘.

5. Save the changes.

Related topics

- Assigning LDAP groups directly to LDAP computers on page 107
- Assigning LDAP groups to departments, cost centers, and locations on page 100
- Assigning LDAP groups to business roles on page 101
- Adding LDAP groups to system roles on page 102
- Adding LDAP groups to the IT Shop on page 103

Assigning LDAP groups directly to LDAP computers

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

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 the groups.

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

5. Save the changes.

Related topics

Effectiveness of membership in LDAP user groups

When groups are assigned to user accounts an identity 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.

ONE IDENTITY
by Quest

Example: 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.

Jo User1 has a user account in this domain. They primarily belong to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to them secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B, and C.

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

Table 12: Specifying excluded groups (`LDAPGroupExclusion` table)

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

Table 13: Effective assignments

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

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

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. That means that the identity is authorized to trigger requests and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 14: Excluded groups and effective assignments

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

Prerequisites

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

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

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

- Mutually exclusive groups belong to the same 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 no longer mutually exclusive.

5. Save the changes.

LDAP group inheritance based on categories

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table.

Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

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 15: 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.
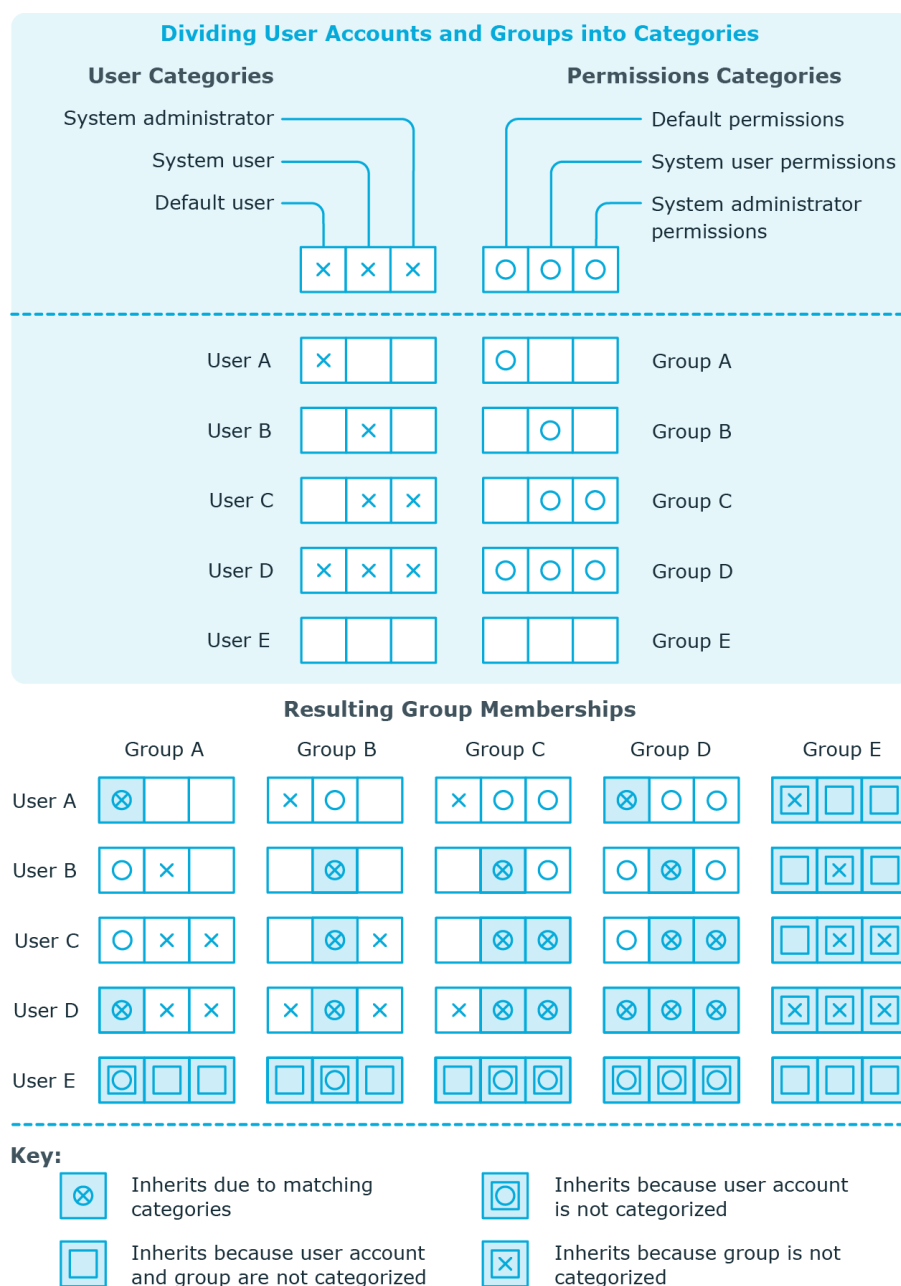
To use inheritance through categories

1. In the Manager, define the categories in the domain.

2. Assign categories to user accounts and contacts through their main data.

3. Assign categories to groups through their main data.

Related topics

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

Example:

- If the report is created for a resource, all roles are determined in which there are identities with this resource.

- If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.

- If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.

- If the report is created for a department, all roles are determined in which identities of the selected department are also members.

- If the report is created for a business role, all roles are determined in which identities 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 identities 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 identities 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 identities 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 identities for tracking. This creates a new business role to which the identities are assigned.

Figure 3: Toolbar of the Overview of all assignments report.
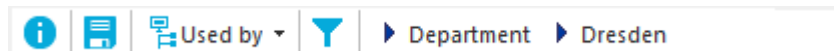
Table 16: Meaning of icons in the report toolbar

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

Login credentials for LDAP user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login credentials generated to users.

Detailed information about this topic

- Password policies for LDAP user accounts on page 115
- Initial password for new LDAP user accounts on page 127
- Email notifications about login data on page 127

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 identities' 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 116
- Using password policies on page 117
- Editing password policies on page 118
- Creating password policies on page 119

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 identities, user accounts, or system users.

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

Password policy for forming identities' central passwords

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

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

For more information about password policies for identities, 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 9.2, 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 user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's LDAP container.
4. Password policy of the user account's LDAP domain.
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.

- **Apply to**: Application scope of the password policy.

  To specify an application scope

  1. Click ➔ next to the field.

  2. Select one of the following references under **Table**:

     - The table that contains the base objects of synchronization.

     - To apply the password policy based on the account definition, select the **TSBAccountDef** table.

     - To apply the password policy based on the manage level, select the **TSBBehavior** table.

  3. Under **Apply to**, select the table that contains the base objects.

     - If you have selected the table containing the base objects of synchronization, next select the specific target system.

     - If you have selected the **TSBAccountDef** table, next select the specific account definition.

     - If you have selected the **TSBBehavior** table, next select the specific manage level.

  4. Click **OK**.

- **Password column**: Name of the password column.
- **Password policy**: Name of the password policy to use.

5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **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

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

To edit a password policy

1. In the Manager, select the **LDAP > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Edit the password policy's main data.

5. Save the changes.

Detailed information about this topic

- General main data of password policies on page 119
- Policy settings on page 120
- Character classes for passwords on page 121
- Custom scripts for password requirements on page 123

Creating password policies

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

To create a password policy

1. In the Manager, select the **LDAP > Basic configuration data > Password policies** category.

2. Click 🔳 in the result list.

3. On the main data form, enter the main data of the password policy.

4. Save the changes.

Detailed information about this topic

- General main data of password policies on page 119
- Policy settings on page 120
- Character classes for passwords on page 121
- Custom scripts for password requirements on page 123

General main data of password policies

Enter the following main data of a password policy.

Table 17: main data for a password policy

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

Policy settings

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

Table 18: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into

Property	Meaning
	account.
	This data is only taken into account if the One Identity Manager login was through a system user or identity based authentication module. If a user has exceeded the maximum number of failed logins, the identity or system user will not be able to log in to One Identity Manager.
	You can use the Password Reset Portal to reset the passwords of identities and system users who have been locked. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

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

Table 19: Character classes for passwords

Property	Meaning
Required number of	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken

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

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

Custom scripts for password requirements

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

Detailed information about this topic

Checking passwords with a script

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.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
LDAP

Login credentials for LDAP user accounts

123

> **Example: Script that checks a password**
>
> A password cannot start with **?** or **!** . The password cannot start with three identical characters. The script checks a given password for validity.
>
> ```
> Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
> As System.Security.SecureString)
>
>       Dim pwd = spwd.ToInsecureArray()
>
>       If pwd.Length>0
>
>             If pwd(0)="?" Or pwd(0)="!"
>
>                   Throw New Exception(#LD("Password can't start with '?' or
>                   '!'")#)
>
>             End If
>
>       End If
>
>       If pwd.Length>2
>
>             If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
>
>                   Throw New Exception(#LD("Invalid character sequence in
>                   password")#)
>
>             End If
>
>       End If
>
> End Sub
> ```

To use a custom script for checking a password

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

Related topics

- Generating passwords with a script on page 125

Generating passwords with a script

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example: Script that generates a password

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

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

     Dim pwd = spwd.ToInsecureArray()

     ' replace invalid characters at first position

     If pwd.Length>0

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

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

          End If

     End If

End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.

2. Edit the password policy.

    a. In the Manager, select the **LDAP > Basic configuration data > Password policies** category.

    b. In the result list, select the password policy.

    c. Select the **Change main data** task.

d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.

e. Save the changes.

Related topics

- Checking passwords with a script on page 123

Editing the excluded list for passwords

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

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

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.

2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.

3. Save the changes.

Checking passwords

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

To verify if a password conforms to the password policy

1. In the Manager, select the **LDAP > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Select the **Test** tab.

5. Select the table and object to be tested in **Base object for test**.

6. Enter a password in **Enter password to test**.

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

Testing the generation of passwords

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

To generate a password that conforms to the password policy

1. In the Manager, select the **LDAP > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Select the **Test** tab.

5. Click **Generate**.

    This generates and displays a password.

Initial password for new LDAP user accounts

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

- When you create the user account, enter a password in the main data.

- Assign a randomly generated initial password to enter when you create user accounts.

    - In the Designer, set the **TargetSystem | LDAP | Accounts | InitialRandomPassword** configuration parameter.

    - Apply target system specific password policies and define the character sets that the password must contain.

    - Specify which identity will receive the initial password by email.

Related topics

- Password policies for LDAP user accounts on page 115
- Email notifications about login data on page 127

Email notifications about login data

You can configure the login credentials 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 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 identities have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

4. Ensure that a language can be determined for all identities. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

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

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 message recipient as a value.

3. In the Designer, set the **TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

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

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

Mapping LDAP objects in One Identity Manager

In One Identity Manager, user accounts, groups, computers, and container structures of an LDAP domain are mapped. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

Detailed information about this topic

LDAP domains

The target system for the synchronization with an LDAP directory is the domain. Domains are added as base objects for the synchronization in One Identity Manager. They are used to configure provisioning processes, automatic assignment of identities to user accounts, and to pass down LDAP user groups to user accounts.

Detailed information about this topic

-
-
-
-

Creating LDAP domains

NOTE: If you use a default project template, the Synchronization Editor sets up the domains in the One Identity Manager database. If necessary, domains can also be created in the Manager.

To create an LDAP domain

1. In the Manager, select the **LDAP > Domains** category.
2. Click ➕ in the result list.
3. On the main data form, edit the main data for the domain.
4. Save the changes.

Related topics

-
-
-
-

Editing main data of LDAP domains

NOTE: One Identity Manager sets up the domains in the Synchronization Editor database.

To edit the main data of an LDAP domain

1. In the Manager, select the **LDAP > Domains** category.
2. Select the domain in the result list.
3. Select the **Change main data** task.
4. Edit the domain's main data.
5. Save the changes.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
LDAP

Mapping LDAP objects in One Identity Manager

130

Related topics

General main data for LDAP domains

Enter the following general main data.

Table 20: Domain main 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`

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 identities 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 identity (**Linked**) if no account

Property	Description
	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 21: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	LDAP connector	LDAP connector
No synchronization	none	none

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

Property	Description
Description	Text field for additional explanation.
Structural object class	Structural object class representing the object type.

Related topics

- Assigning account definitions to LDAP domains on page 81
- Assigning identities automatically to LDAP user accounts on page 84
- Target system managers for LDAP on page 165

LDAP specific main data for LDAP domains

Enter the following main data for LDAP:

Table 22: 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 root domain>.`
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 and auxiliary classes that are used by other LDAP and X.500 directory services.
Search mask	Search mask for another LDAP object.

Defining categories for inheritance by LDAP groups

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

To define a category

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

Detailed information about this topic

- LDAP group inheritance based on categories on page 110

Editing the synchronization project for an LDAP domain

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.
3. Select the **Change main data** task.
4. Select the **Edit synchronization project** task.

Related topics

- Adjusting the synchronization configuration for LDAP environments on page 35

Displaying the LDAP domain overview

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

To obtain an overview of a domain

1. In the Manager, select the **LDAP > Domains** category.
2. Select the domain in the result list.
3. Select the **LDAP domain overview** task.

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.

Detailed information about this topic

- Creating LDAP containers on page 135
- Editing main data of LDAP containers on page 135
- General main data for LDAP containers on page 136
- Contact data for LDAP containers on page 137
- Address information for LDAP containers on page 138
- Assigning extended properties to LDAP containers on page 138
- Displaying the LDAP container overview on page 139
- Synchronizing single objects on page 55

Creating LDAP containers

Containers are imported into the One Identity Manager by synchronization. You can set up new containers in One Identity Manager.

To create a container

1. In the Manager, select the **LDAP > Container** category.
2. Click ⊞ in the result list.
3. Edit the container's main data.
4. Save the changes.

Related topics

- Editing main data of LDAP containers on page 135
- General main data for LDAP containers on page 136
- Contact data for LDAP containers on page 137
- Address information for LDAP containers on page 138

Editing main data of LDAP containers

You can edit existing containers in One Identity Manager.

To edit a container

1. In the Manager, select the **LDAP > Container** category.

2. Select the container in the result list and run the **Change main data** task.

3. Edit the container's main data.

4. Save the changes.

Related topics

General main data for LDAP containers

Enter the following general main data.

Table 23: Main 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.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
LDAP

Mapping LDAP objects in One Identity Manager

136

Property	Description
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

-

Contact data for LDAP containers

Enter data for reachability

Table 24: 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.

Table 25: Address data

Property	Description
Building name	Name of the building.
Location ID	Location ID (country and city).
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.
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.

Assigning extended properties to LDAP containers

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

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

To specify extended properties for a container

1. In the Manager, select the **LDAP > Container** category.

2. Select the container in the result list.

3. Select **Assign extended properties**.

4. In the **Add assignments** pane, assign extended properties.

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

    To remove an assignment

    - Select the extended property and double-click ✅.

5. Save the changes.

Displaying the LDAP container overview

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

To obtain an overview of a container

1. In the Manager, select the **LDAP > Container** category.

2. Select the container in the result list.

3. Select the **LDAP container overview** task.

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 permissions to network resources.

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

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

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

Related topics

- Managing LDAP user accounts and identities on page 62
- Managing memberships in LDAP groups on page 97
- Account definitions for LDAP user accounts on page 63
- Creating LDAP user accounts on page 140
- Editing main data of LDAP user accounts on page 140
- General main data of LDAP user accounts on page 141

Creating LDAP user accounts

User accounts are imported into One Identity Manager during synchronization. You can set up new user accounts in One Identity Manager.

To create a user account

1. In the Manager, select the **LDAP > User accounts** category.
2. Click in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

Related topics

Editing main data of LDAP user accounts

You can edit existing user accounts in One Identity Manager.

To edit main data 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 **Change main data** task.

4. Edit the user account's resource data.

5. Save the changes.

Related topics

General main data of LDAP user accounts

Enter the following general main data.

Table 26: Additional main data of a user account

Property	Description
Identity	Identity that uses this user account. • An identity is already entered if the user account was generated by an account definition. • If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account. • If you create the user account manually, you can select an identity in the menu. The menu displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the **QER | Person| HideDeactivatedIdentities** configuration parameter. | NOTE: If you assign a deactivated identity to a user account, it might

Property	Description
		be locked or deleted depending on the configuration.
	You can create a new identity 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 identity main data. Which login data is required depends on the selected identity type.
No link to an identity required	Specifies whether the user account is intentionally not assigned an identity. The option is automatically set if a user account is included in the exclusion list for automatic identity assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an identity (for example, if several identities use the user account).
	If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an identity can be filtered according to various criteria.
Not linked to an identity	Indicates why the **No link to an identity required** option is enabled for this user account. Possible values: **By administrator**: The option was set manually by the administrator. **By attestation**: The user account was attested. **By exclusion criterion**: The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the user account was created.
	Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned identity 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.
	NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the identity. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (X0rigin=1).
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

Property	Description
	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 identity 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 name	User account display name. The display name is made up of the first and last names.
Distinguished name	User account's distinguished name. The distinguished name is formatted from the user account's identifier and the container and cannot be changed.
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 identity's central user account depending on the manage level.
Password	Password for the user account. The identity's central password can be

Property	Description
	mapped to the user account password. For more information about an identity's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. 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 more 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 identity'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 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 type	User account's identity type Permitted values are: • **Primary identity**: Identity'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 identity. • **Sponsored identity**: User account to use for a specific purpose. Training, for example. • **Shared identity**: User account with administrative permissions, used by several identities. Assign all identities that use this user account.

Property	Description
	• **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 linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests. • If you add an identity 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 identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
User account is disabled	Specifies whether the user account is disabled. If a user account is not required for a period of time, you can temporarily disable the user account by using the "User account is disabled" option.

Related topics

- Account definitions for LDAP user accounts on page 63
- Password policies for LDAP user accounts on page 115
- Initial password for new LDAP user accounts on page 127
- Managing LDAP user accounts and identities on page 62
- Managing memberships in LDAP groups on page 97
- Prerequisites for indirect assignment of LDAP groups on page 99
- Disabling LDAP user accounts on page 150

Contact information for LDAP user accounts

Enter the data used by this user account for contacting the identity 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 🗑.

Property	Description
Email address	Email address. If you assigned an account definition, the email address is made up of the identity'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 used by this user account for contacting the identity.

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

Property	Description
	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

Enter the following organizational main data.

Table 29: Organizational main data

Property	Description
Business unit	Business unit to which the identity is assigned.
Department	Identity's department If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Location	Identity'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 ID (country and city).
Employment	Job details.
Personnel number	Number for identifying the identity, 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.
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.

Property	Description
Secretary	Secretary's user account.
Country ID	The country ID.
Company	Identity'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.

EduPerson extensions for LDAP user accounts

On the **Higher education** tab, the following information for the **eduPerson** object class is displayed.

Table 30: eduPerson main data

Property	Description
User identi-fier	A unique identifier for an identity. The identifier should be have the form "**user@scope**". The **user** part is a name-based identifier for the identity. The **scope** part is the administrative domain of the identity system in which the identifier was created and assigned.
Unique alias	Unique and permanent pseudonymous identifier of an identity. This value is provider-specific.
Global identi-fier	Unique, globally valid identifier for an identity.
Nickname	The short name of the identity.
Institution	Distinguished name of the institution to which the identity belongs.
Institution units	Distinguished name of the unit in the institution to which the identity belongs. You can enter more that one unit.
Institution unit (primary)	Distinguished name of the primary unit in the institution to which the identity belongs.
Affiliation	Categorization of the identity's affiliation with the institution, such as student, faculty, staff, alumni. You can enter more that one type.
Scoped affil-iation	Category and institution to which the identity belongs. You can enter more that one scoped affiliation. Example: student@university.com
Primary affil-	Primary category and institution to which the identity belongs.

ONE IDENTITY
by Quest

Property	Description
iation	Example: student@university.com
Permissions	Permissions that control access and how certain resources are accessed.
ORCID IDs	Unique identifiers used primarily to relate an identity to its scientific publications.
Level of assurance	Quantifies the trustworthiness of the identity.
Prior user identifier	Previous user IDs that were associated with the identity. The values must not contain the currently valid user identifier.
Analytics tag	String that can be used for reporting or analysis.

Related topics

Miscellaneous data for LDAP user accounts

Enter the following main data:

Table 31: Miscellaneous main data

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

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.

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

To specify extended properties for a user account

1. In the Manager, select the **LDAP > User accounts** category.

2. Select the user account in the result list.

3. Select **Assign extended properties**.

4. In the **Add assignments** pane, assign extended properties.

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

   ### *To remove an assignment*
   - Select the extended property and double-click ⊘.

5. Save the changes.

Disabling LDAP user accounts

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

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

User accounts managed through account definitions are disabled when the identity 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 identities. No account definition is applied.

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

- If the configuration parameter is set, the identity's user accounts are disabled when the identity is permanently or temporarily disabled.

- If the configuration parameter is not set, the identity'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 main data** task.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
LDAP

Mapping LDAP objects in One Identity Manager

150

4. On the **General** tab, set the **Account is disabled** option.

5. Save the changes.

Scenario: The user accounts are not linked to identities.

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

1. In the Manager, select the **LDAP > User accounts** category.

2. Select the user account in the result list.

3. Select the **Change main data** task.

4. On the **General** tab, set the **Account is disabled** option.

5. Save the changes.

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

Related topics

- Account definitions for LDAP user accounts on page 63
- Creating manage levels on page 68
- Deleting and restoring LDAP user accounts on page 151

Deleting and restoring LDAP user accounts

NOTE: As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

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

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

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

1. In the Manager, select the **LDAP > User accounts** category.

2. Select the user account in the result list.

3. Click in the result list.

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

To restore a user account

1. In the Manager, select the **LDAP > User accounts** category.

2. Select the user account in the result list.

3. Click 🖳 in the result list.

Related topics

- Disabling LDAP user accounts on page 150
- Specifying deferred deletion for LDAP user accounts on page 96

Displaying the LDAP user account overview

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.

LDAP groups

LDAP user accounts, computers, and groups can be grouped into groups that can be used to regulate access to resources. 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. You can assign groups to departments, cost centers, locations, business roles, system roles, or the IT Shop.

Related topics

- Managing memberships in LDAP groups on page 97
- Creating LDAP groups on page 153
- Editing main data of LDAP groups on page 153
- LDAP group main data on page 154
- Adding LDAP groups to LDAP groups on page 155
- Assigning extended properties to LDAP groups on page 155
- Deleting LDAP groups on page 156

Creating LDAP groups

Groups are loaded into One Identity Manager by synchronization. You can set up new groups in One Identity Manager.

To create a group

1. In the Manager, select the **LDAP > Groups** category.
2. Click ⊞ in the result list.
3. On the main data form, edit the main data of the group.
4. Save the changes.

Related topics

Editing main data of LDAP groups

You can edit existing groups in One Identity Manager.

To edit group main data

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

Related topics

LDAP group main data

Enter the following general main data.

Table 32: General main 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.
Display name	Name for displaying the group in the user interface of One Identity Manager tools.
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. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated.
	For more information 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

Property	Description
	this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. 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 through the Web Portal and allocated by defined approval processes. Direct assignment of the group to hierarchical roles or user accounts is not permitted.

Related topics

- LDAP group inheritance based on categories on page 110
- Adding LDAP groups to the IT Shop on page 103

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.

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

To specify extended properties for a group

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

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

   ### *To remove an assignment*

   - Select the extended property and double-click ⊘.

5. Save the changes.

Adding LDAP groups to LDAP groups

Use this task to add a group to another group. This means that the groups can be hierarchically structured.

To assign groups directly to a group as members

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

2. Select the group in the result list.

3. Select the **Assign groups** category.

4. Select the **Has members** tab.

5. Assign child groups in **Add assignments**.

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

6. Save the changes.

To add a group as a member of other groups

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

2. Select the group in the result list.

3. Select the **Assign groups** task.

4. Select the **Is member of** tab.

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

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

6. Save the changes.

Deleting LDAP groups

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

To delete a group

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

2. Select the group in the result list.

3. Click 🗑 in the result list.

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

Displaying the LDAP group overview

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.

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.

Related topics

- Creating LDAP computers on page 157
- Editing main data of LDAP computers on page 158
- Main data for LDAP computers on page 158
- Displaying the LDAP computer overview on page 159
- Managing memberships in LDAP groups on page 97
- Synchronizing single objects on page 55

Creating LDAP computers

Computers are imported into the One Identity Manager by synchronization. You can set up new computers in One Identity Manager.

To create a computer

1. In the Manager, select the **LDAP > Computers** category.

2. Click ![add icon] in the result list.

3. Edit the computer's main data.

4. Save the changes.

Related topics

-
-

Editing main data of LDAP computers

You can edit existing computers in One Identity Manager.

To edit a computer's main data

1. In the Manager, select the **LDAP > Computers** category.
2. In the results list, select the computer and perform the **Edit master data** task.
3. Edit the computer's main data.
4. Save the changes.

Related topics

-
-

Main data for LDAP computers

Enter the following data for a computer.

Table 33: Computer main data

Property	Description
Device	The computer is connected to this device. Specify a new device using the button next to the menu. For more information about devices, see the *One Identity Manager Identity Management Base Module Administration Guide*.
Name	Computer identifier
Domain	Domain in which to create the computer.
Container	Container in which to create the computer. The distinguished name of the computer is determined by a template when the container is selected.
Structural object class	Structural object class representing the object type.
Object class	List of classes defining the attributes for this object. However, in the input field, you can add object classes and auxiliary classes that are used by other LDAP and X.500 directory services.

Related topics

- [Prerequisites for indirect assignment of LDAP groups](#) on page 99

Displaying the LDAP computer overview

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

To obtain an overview of a computer

1. In the Manager, select the **LDAP > Computers** category.

2. Select the computer in the result list.

3. Select the **Computer overview** task.

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 34: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history.
		Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts overview (incl. history)	Container	This report shows all the container's user accounts with their permissions including a history.
		Select the end date for displaying the history (**Min. date**). Older changes and assignments

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

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

Table 35: Additional reports for the target system

Report	Description
LDAP user account and group administration	This report contains a summary of user account and group 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 113

Handling of LDAP objects in the Web Portal

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

- Managing user accounts and identities

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

- Managing group assignments

  When a group is assigned to an IT Shop shelf, the group can be requested by the customers of the shop in the Web Portal. The request undergoes a defined approval process. The group is not assigned until it has been approved by an authorized identity.

  In the Web Portal, managers and administrators of organizations can assign groups to the departments, cost centers, or locations for which they are responsible. The groups are passed on to all persons who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, managers, and administrators of business roles can assign groups in the Web Portal to the business roles for which they are responsible. The groups are passed on to all persons who are members of these business roles.

  If the System Roles Module is available, supervisors of system roles can assign groups to the system roles in the Web Portal. The groups are passed on to all persons to whom these system roles are assigned.

- Attestation

  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

  If the Compliance Rules Module is available, you can define rules that identify the invalid group memberships and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check rule violations and to grant exception approvals.

  If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

  You can use the risk index of groups to evaluate the risk of entitlement assignments for the company.One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the identities, user accounts, and their entitlements and risks.

For more information about the named topics, see Managing LDAP user accounts and identities on page 62, Managing memberships in LDAP groups on page 97, and the following guides:

- *One Identity Manager Web Designer Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

Basic data for managing an LDAP environment

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

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to identities. You can create account definitions for every target system. If an identity 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 identity.

  For more information, see Account definitions for LDAP user accounts on page 63.

- Password policies

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the identities' 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 115.

- Target system types

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

  For more information, see Post-processing outstanding objects on page 56.

- Target system managers

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

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

For more information, see .

- Servers

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

    For more information, see .

Target system managers for LDAP

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

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

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

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates identities to be target system administrators.

2. These target system administrators add identities 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 identities within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual domains.

Table 36: 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.

User	Tasks

- Edit password policies for the target system.
- Prepare groups to add to the IT Shop.
- Can add identities that do not have the **Primary identity** identity type.
- 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 identities within their area of responsibility as target system managers and create child application roles if required.

To initially specify identities 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 identities** task.
4. Assign the identity and save the changes.

To add the first identities 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 identities** task.
4. Assign the identities you want and save the changes.

To authorize other identities 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 identities** task.
4. Assign the identities 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 main data** task.

5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

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

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

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

6. Save the changes.

7. Assign identities 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

Job server for LDAP-specific process handling

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

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.

- In the Manager, select an entry for the Job server in the **LDAP > Basic configuration data > Server** category and edit the Job server's main data.

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

NOTE: One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

Related topics

Editing LDAP Job servers

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.

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 main data** task.
4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

General main data of Job servers

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 37: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax.
	Syntax:
	`<Name of servers>.<Fully qualified domain name>`

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

Property	Meaning
	queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating.

Property	Meaning
	NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
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 171

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 38: 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

Server function	Remark
	One Identity Manager database is installed on. It can run SQL tasks.
	The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.
	Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the ScriptComponent process component.
Generic 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 synchronizing 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 main data of Job servers on page 168

Troubleshooting

Possible errors when synchronizing an OpenDJ environment

Issue

Error synchronizing an OpenDJ system if a password begins with an open curly bracket.

Cause

The LDAP server interprets a generated password of the form `{<abc>}<def>` as a hash value. However, the LDAP server does not allow hashed passwords to be passed.

Solution

The LDAP server can be configured so that a hashed password of the form `{<algorithm>}hash` can be passed.

- On the LDAP server: Allow already hashed passwords to be passed.
- In the synchronization project: Only pass hashed passwords. Use the script properties for mapping schema properties that contain passwords. Create the password's hash value in the script.

Errors connecting multiple LDAP systems with the same distinguished name

Issues

An error occurs when creating multiple synchronization projects for connecting an LDAP domain or when connecting instances with identical names.

```
The domain with the distinguished name '{0}' is already used in the
synchronization project '{1}'. Only one synchronization project is allowed per
domain and connector.
```

Cause

This problem occurs if the synchronization projects were created with an older One Identity Manager version.

The domain name (`Ident_Domain`) is used to search for LDAP domains in the database. In synchronization projects created with an older One Identity Manager version, LDAP domain names are formatted with `<DN component 1>`.

Solution

- With newly created synchronization projects, the LDAP domain names are formed with `<DN component 1> (<server from connection parameters>)`.

- For existing synchronization projects created with the generic LDAP connector, apply the **VPR#33513** patch. This creates a variable and value for $IdentDomain$ in all variable sets and changes the scope to `DistinguishedName = '$CP_RootEntry$'` and `Ident_Domain='$IdentDomain$'`.

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

- LDAP domains that are already in the database are not renamed. If necessary, manually adjust the LDAP domain names (`Ident_Domain`). For more information, see LDAP domains on page 129.

NOTE: Objects imported from different directory services that have the identical canonical names and distinguished names in the One Identity Manager database, could result in duplicate display values in current attestations, such as system entitlements, as well as in reports on target system objects and target system entitlements. Customizations may need to be made to attestation procedures and reports.

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 39: Configuration parameters for LDAP directory synchronization

Configuration parameters	Description
TargetSystem | LDAP	Preprocessor relevant configuration parameter for controlling database model components for LDAP target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
	If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
TargetSystem | LDAP | Accounts	Allows configuration of user account data.
TargetSystem | LDAP | Accounts | InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo	Identity to receive an email with the random generated password (manager cost center/department/location/business role, identity'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.

Configuration parameters	Description
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Identity – new user account created** mail template is used.
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The **Identity – initial password for new user account** mail template is used.
TargetSystem | LDAP | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Identity – new user account with default properties created** mail template is used.
TargetSystem | LDAP | Accounts | PrivilegedAccount	Allows configuration of privileged LDAP user account settings.
TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem | LDAP | Authentication	Allows configuration of the LDAP authentication module. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
TargetSystem | LDAP | Authentication | Authentication	Authentication mechanism. Permitted values are **Secure**, **Encryption**, **SecureSocketsLayer**, **ReadonlyServer**, **Anonymous**, **FastBind**, **Signing**, **Sealing**, **Delegation**, and **ServerBind**. The value can be combined with commas (,). For more information about authentication types, see the MSDN Library. Default: **ServerBind**
TargetSystem | LDAP | Authentication | Port	Communications port on the server. Default: **389**

Configuration parameters	Description

TargetSystem | LDAP | Authentication | RootDN	Pipe (|) delimited list of root domains to be used to find the user account for authentication.
	
	Syntax:
	
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	
	Example:
	
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | Authentication | Server	Name of the LDAP server.
TargetSystem | LDAP | AuthenticationV2	Allows configuration of the LDAP authentication module. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
TargetSystem | LDAP | AuthenticationV2 | AcceptSelfSigned	Specifies whether self-signed certificates are accepted.
TargetSystem | LDAP | AuthenticationV2 | Authentication	Authentication method for logging in to LDAP. The following are permitted: • **Basic**: Uses default authentication. • **Negotiate**: Uses Negotiate authentication from Microsoft. • **Kerberos**: Uses Kerberos authentication. • **NTLM**: Uses Windows NT Challenge/Response (NTLM) authentication. Default: **Basic** For more information about authentication types, see the MSDN Library.
TargetSystem | LDAP | AuthenticationV2 | ClientTimeout	Client timeout in seconds.
TargetSystem | LDAP | AuthenticationV2 | Port	Communications port on the server. Default: **389**
TargetSystem | LDAP | AuthenticationV2 | ProtocolVersion	Version of the LDAP protocol. The values **2** and **3** are permitted. Default: **3**
TargetSystem | LDAP |	Pipe (|) delimited list of root domains to be used to find

Configuration parameters	Description

AuthenticationV2 | RootDN	the user account for authentication.
	
	Syntax:
	
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	
	Example:
	
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | AuthenticationV2 | Security	Connection security. Permitted values are **None**, **SSL** and **STARTTLS**.
TargetSystem | LDAP | AuthenticationV2 | Server	Name of the LDAP server.
TargetSystem | LDAP | AuthenticationV2 | UseSealing	Specifies whether sealing is enabled.
TargetSystem | LDAP | AuthenticationV2 | UseSigning	Specifies whether signing is enabled.
TargetSystem | LDAP | AuthenticationV2 | VerifyServerCertificate	Specifies whether to check the server certificate when encrypting with SSL.
TargetSystem | LDAP | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | LDAP | HardwareInGroupFromOrg	Specifies whether computers are added to groups based on group assignment to roles.
TargetSystem | LDAP | MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. 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	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem | LDAP | PersonAutoDisabledAccounts	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem | LDAP | PersonAutoFullSync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.

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 LDAP connector V2

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

Table 40: Mapping schema types to tables in the One Identity Manager schema.

Schema type in LDAP	Table in the One Identity Manager Schema
Container	LDAPContainer
country	LDAPContainer

Schema type in LDAP	Table in the One Identity Manager Schema
domain	LDPDomain
groupOfEntries	LDAPGroup
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount
locality	LDAPContainer
organization	LDAPContainer
organizationalUnit	LDAPContainer

Active Directory Lightweight Directory Services project template for the LDAP connector V2

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

Table 41: Mapping schema types to tables in the One Identity Manager schema.

Schema type in AD LDS	Table in the One Identity Manager schema
domainDNS	LDAPContainer
country	LDAPContainer
locality	LDAPContainer
organization	LDAPContainer
container	LDAPContainer
organizationalUnit	LDAPContainer
inetOrgPerson	LDAPAccount
user	LDAPAccount
userProxy	LDAPAccount
userProxyFull	LDAPAccount

Schema type in AD LDS	Table in the One Identity Manager schema
foreignSecurityPrincipal	LDAPAccount
group	LDAPGroup
groupOfNames	LDAPGroup

Oracle Directory Server Enterprise Edition template for the LDAP connector V2

This project template is based on the Oracle Directory Server Enterprise Edition (DSEE). The project template uses mappings for the following schema types.

Table 42: Mapping schema types to tables in the One Identity Manager schema.

Schema type in LDAP	Table in the One Identity Manager schema
country	LDAPContainer
domain	LDPDomain
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount
locality	LDAPContainer
organization	LDAPContainer
organizationalUnit	LDAPContainer

Generic project template for the LDAP connector V2

This template can be used as a base template if there is no system-specifc template. You may have to modify it.

NOTE: Check the project and correct any error before you use the synchronization project.

The project template uses mappings for the following schema types.

Table 43: Mapping schema types to tables in the One Identity Manager schema.

Schema type in LDAP	Table in the One Identity Manager Schema
Container	LDAPContainer
country	LDAPContainer
domain	LDPDomain
groupOfEntries	LDAPGroup
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount
locality	LDAPContainer
organization	LDAPContainer
organizationalUnit	LDAPContainer

LDAP connector V2 settings

The following settings are configured for the system connection with the LDAP connector V2.

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

Table 44: LDAP connector V2 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_SdspLdapDriverDescriptorServer`
Port	Communications port on the server. Default: **389** Variable: `CP_SdspLdapDriverDescriptorPort`
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. • **External**: Uses certificate-based authentication as the external method. Default: **Basic** Variable: `CP_SdspLdapDriverDescriptorAuthenticationType` For more information about authentication types, see the MSDN

Setting	Meaning
	Library.
User name	Name of the user account for logging in to LDAP.
	Variable: `CP_SdspLdapDriverDescriptorUsername`
Password	The user account's password.
	Variable: `CP_SdspLdapDriverDescriptorPassword`
Enable sealing	Specifies whether sealing is enabled.
	Variable: `CP_SdspLdapDriverDescriptorUseSealing`
Enable signing	Specifies whether signing is enabled.
	Variable: `CP_SdspLdapDriverDescriptorUseSigning`
Use SSL	Specifies whether the connection is SSL/TLS encrypted.
	Variable: `CP_SdspLdapDriverDescriptorUseSsl`
Use StartTLS	Specifies whether StartTLS is used for encryption.
	Variable: `CP_SdspLdapDriverDescriptorUseStartTls`
Server certificate verification	Specifies whether the server certificate is checked with either SSL or StartTLS encryption.
	NOTE: The server certificate must be valid. The root certification authority's certificate must be the computer certificate (**Local Computer** certificate store) either on the host that the Synchronization Editor was started on or on the Job server connected remotely. Ensure that the certificate is also installed on all Job servers that will connect to the LDAP system.
	Variable: `CP_SdspLdapDriverDescriptorVerifyServerCertificate`
Protocol version	Version of the LDAP protocol.
	Default: **3**
	Variable: `CP_SdspLdapDriverDescriptorProtocolVersion`
Search base	Root entry for the search query, normally the LDAP domain.
	Variable: `CP_LdapContextDescriptorBaseDn`
Request timeout	Timeout for LDAP requests in seconds.
	Default: **3600**
	Variable: `CP_SdspLdapDriverDescriptorClientTimeout`
LDAP domain UID	Unique identifier for the LDAP domain in the `LDPDomain` table.
	Variable: `UID_LDPDomain`
Default Searcher:	Specifies whether LDAP objects are loaded by page. This information

ONE IDENTITY
by Quest

Setting	Meaning
Use paged search	is automatically queried through the selected preconfiguration or from the LDAP server. If the option is enabled, enter the page size.
	Variable: `CP_SdspDefaultSearchDescriptorUsePagedSearch`
Default Searcher: Page size	Maximum number of objects to load per page.
	Default: **500**
	Variable: `CP_SdspDefaultSearchDescriptorPageSize`
AD (LDS) Search implementation: Chunk size	If attributes with a large number of value are returned from a Microsoft based LDAP server, the server only sends a certain number of values back (normally 1500.) To query all the values, several queries with a scope limit are sent.
	The chunk size determines how many value are return per query. If the select chunk size is larger than the maximum size that the server can process, it is adjusted automatically.
	Default: **1000**
	Variable: `CP_AdLdsSearchFeatureDescriptorChunkSize`
Default delete implementation: Use DeleteTree control when deleting entries	Specifies if the LDAP server sends the **DeleteTree** control to delete entries with sub-entries during deletion. This information is automatically queried through the selected preconfiguration or from the LDAP server.
	Variable:`CP_SdspDefaultDeleteDescriptorUseDeleteTree`
Load schema from LDAP Server	The schema is loaded from the LDAP server. (default)
Load schema from given LDIF string	Alternative source to load the schema from if the LDAP server's schema is not available. The LDIF string is saved in the system connection (`DPRSystemConnection.ConnectionParameter`.) The means the `*.ldif` file is not distributed.
Remove spaces in distinguished names	This function removes all spaces in distinguished name objects that, according to RFC, are not allowed or non-significant.
	If the function does not exist, according to RFC, all spaces that are non allowed or non-significant are not removed from the distinguished name and can cause errors in certain circumstances.
	Default: **False**
Tolerate 'Attribute already exists' and 'no such attribute' and retry	Use this function to tolerate existing or missing attributes in the LDAP system when an object is changed, for example, updating group memberships.
	If this function is not available, changes to objects that affect existing or missing attribute in the LDAP system can cause errors.

Setting	Meaning
	Default: **True**
Return operational attributes	This schema function specifies, which attributes are additionally found for the 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.
Auxiliary class assignment	Use this schema function to 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.
Switch type of object class	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.
Cache schema	This schema function keeps the LDAP schema stored in local cache. It is recommended to queue this function after the schema has loaded. 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`.
Load AD LDS schema extension	This schema function loads additional information required for synchronizing the Active Directory Lightweight Directory Service.

Setting	Meaning
Driver	Driver to use for accessing the LDAP system.
	Default: **LDAP via Windows API (SdspLdapDriver)**
LDAP domain	Unique identifier of the domain in the form:
	`<DN part 1> (<server from connection parameters>)`
	Variable: $IdentDomain$

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