ONE IDENTITY

One Identity Manager 10.0

Administration Guide for Connecting
to Active Directory

Contents

Managing Active Directory environments

Complex Windows environments, which include Active Directory, can be mapped and synchronized in One Identity Manager. Administration of One Identity Manager objects such as users, contact groups, computers, and organizational units is possible using hierarchical domain structures in Active Directory.

One Identity Manager provides company identities with the necessary user accounts. There are different ways for you to connect identities to their user accounts. You can also manage user accounts independently of identities and thus set up administrator user accounts.

Administration of groups in One Identity Manager enables users to be supplied with necessary authorizations. You can set up organizational units in a hierarchical container structure in One Identity Manager. Organizational units (branches or departments) are used to logically organize objects such as users, groups, and computers. This makes it easier to manage objects.

> **NOTE:** The Active Directory module must be installed as a prerequisite for managing One Identity Manager in Active Directory Module For more information, see Installing One Identity Manager.

Architecture overview

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

- Active Directory domain controller

  Domain controller against which the Active Directory objects are synchronized. The synchronization server connects to this server in order to access the Active Directory objects.

- Synchronization server

  Synchronization server for synchronizing One Identity Manager data with Active Directory. The One Identity Manager Service with the Active Directory

connector is installed on this server. The synchronization server connects to the Active Directory domain controller.

The Active Directory connector in One Identity Manager uses ADSI for communicating with a domain controller. The Active Directory connector is used for synchronization and provisioning Active Directory. The Active Directory connector communicates directly with a domain controller.

Figure 1: Architecture for synchronization

One Identity Manager users for managing Active Directory

The following users are used in setting up and administration of Active Directory.

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.

Users	Tasks
	• 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 administrators.
	• Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Active Directory** application role or a child application role.
	Users with this application role:
	• Assume administrative tasks for the target system.
	• Create, change, or delete the 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.
	• 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.
Administrators for custom tasks	Administrators must be assigned to the **Custom | Administrators** application role.
	Users with this application role:
	• Administrate custom application roles.
	• Set up child application roles for **Managers** and **Synchronization** if required.
Synchronization project owners	Synchronization project owners must be assigned to the **Custom | Synchronization** application role or a child application role.
	Users with this application role:
	• Configure synchronization in the Synchronization Editor.
	• Edit synchronization templates.
	• Authorize other identities as owners.

Users	Tasks
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 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 Active Directory 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.

Related topics

- Configuration parameters for managing an Active Directory environment on page 226

Synchronizing an Active Directory environment

One Identity Manager supports synchronization with Active Directory, shipped with Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, and Windows Server 2025.

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and the Active Directory directory.

This sections explains how to:

- Set up synchronization to import initial data from Active Directory domains to the One Identity Manager database.

- Adjust a synchronization configuration, for example, to synchronize different Active Directory domains with the same synchronization project.

- Start and deactivate the synchronization.

- Evaluate the synchronization results.

TIP: Before you set up synchronization with an Active Directory domain, familiarize yourself with the Synchronization Editor. For more information, see Working with the Synchronization Editor.

Setting up initial synchronization with an Active Directory domain

The Synchronization Editor provides a project template that can be used to set up the synchronization of user accounts and permissions for the Active Directory environment. You use these project templates to create synchronization projects with which you import the data from an Active Directory domain 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.

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

1. Prepare a user account with sufficient permissions for synchronizing in Active Directory.

2. One Identity Manager components for managing Active Directory environments are available if the **TargetSystem | ADS** 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.

   - 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.

Related topics

- Creating a synchronization project for initial synchronization of an Active Directory domain on page 24
- Configuration parameters for managing an Active Directory environment on page 226
- Default project template for Active Directory on page 231

Users and permissions for synchronizing with Active Directory

The following users play a role in synchronizing One Identity Manager with Active Directory.

Table 2: Users for synchronization

User	Permissions
User for accessing Active Directory	You must provide a user account with the following permissions for full synchronization of Active Directory objects with the supplied One Identity Manager default configuration.
	• Member of the **Domain Admins** Active Directory

User	Permissions
	group
	NOTE: In a hierarchical domain structure, the One Identity Manager Service's user account of a child domain is member of the **Enterprise Admins** group.
	There is no recommended practical minimum configuration whose permissions in terms of user administration effectiveness, differ from a member of the **Domain admins** group.
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 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. The default installation installs One Identity Manager under `%ProgramFiles%\One Identity`.
	Setting Remote Access Service (RAS) properties requires Remote Procedure Calls (RPC) which are run in the context of the One Identity Manager Service user account. To read or write these properties, the One Identity Manager Service user account must have the necessary permissions.
	To create administrative shares, the user account must

User	Permissions
	be a member of the **Domain Admins** Active Directory group.
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to run synchronization using an application server.

Necessary access permissions explained

The synchronization base object in Active Directory requires the following access permissions:

- Read
- Write

If the base object is the domain object, these permissions are needed to allow reading and setting domain properties such as password policies.

The following permissions are required for working unrestricted below the base object:

- Create All Child Objects
- Delete All Child Objects

To be able editing of specific properties in a user object that result in a change to the permission list of an Active Directory object (for example, the **Password cannot be changed** property), the following permissions are required:

- Read Permissions
- Modify Permissions

Prerequisite for further privileges:

- Modify Owner

Normally only group administrators have this privilege. If the One Identity Manager Service user account is not a member of this group or any equivalent group, it must put in a position to cope with accounts without any permissions.

The following permissions are required because all an object's values can, in principle, be modified through One Identity Manager:

- Read All Properties
- Write All Properties
- All Extended Rights
- DeleteSubTree

Essential user account functionality is partially stored as an entry in the permissions list of an Active Directory object. The One Identity Manager Service user account must be able to modify this permissions list. Example of properties maintained over the permissions list are UserCanNotChangePassword for the user account, or AllowWriteMembers for the group.

Modifying a permissions list assumes a wide range of permissions. If a user account that does not have the **Full Control** permissions for the corresponding Active Directory object is used for changing a permissions list, the change is only accepted under the following conditions.

- The user account is the owner of the object.

  – OR –

- The user account is member of the same primary group as the object owner. This is usually the **Domain administrators** group.

Otherwise the modifications are rejected.

If the **Take Ownership** permission is assigned to the user account, it is possible to initiate a change of owner and to change the permissions list accordingly. However, this falsifies the permissions state of the Active Directory object and is not recommended.

Furthermore, you require domain administrator permissions to use the delete and restore functions of the Active Directory recycling bin and for dealing with specially protected user account and groups.

> **NOTE:** In theory, the part of the synchronization with the Active Directory that imports the Active Directory objects into the One Identity Manager database also functions if only **Read** permissions and not **Write** permissions are assigned to the structure.
>
> The following problems may occur:
>
> - To include a user account for which only **Read** permissions exist in a group that is not the primary group of the user account, the One Identity Manager Service must have at least **Write** permissions for the group object.
>
> - Error states between the One Identity Manager database and Active Directory data occur, if One Identity Manager administration tools or database imports result in the creation of, or changes to objects in the Active Directory for which only **Read** permissions exist. These cases can be excluded with the suitable menu navigation in the administration tools, One Identity Manager object permissions, and by taking appropriate precautions when importing.

Communications ports and firewall configuration

One Identity Manager is made up of several components that can run in different network segments. In addition, One Identity Manager requires access to various network services, which can also be installed in different network segments. You must open various ports depending on which components and services you want to install behind the firewall.

The following ports are required:

Table 3: Communications port

Default port	Description
53	Domain Name System (DNS), mainly through UDP. Required for access to the Active Directory total structure.
80	Port for accessing web applications.
88	Kerberos authentication system (if Kerberos authentication is implemented). Required for authentication against Active Directory.
135	Microsoft End Point Mapper (EPMAP) (also, DCE/RPC Locator Service).
137	NetBIOS Name Service.
139	NetBIOS Session Service.
389	Lightweight Directory Access Protocol (LDAP Standard). Target system server communications port.
443	Default port for HTTPS connections.
445	Microsoft-DS Active Directory, Windows shares. Required for synchronization (TCP/UDP)
636	Lightweight Directory Access Protocol using TLS/SSL (LDAP S). Required for access to the Active Directory total structure.
1433	Port for communicating with the One Identity Manager database.
1880	Port for the HTTP protocol of One Identity Manager Service.
2880	Port for access tests with the Synchronization Editor, such as in the target system browser or for simulating synchronization. Default port for the `RemoteConnectPlugin`.
3268	Global catalog. Required for searching in the global catalog. Either port 3268 or 3269 should be open depending on the connection settings.
3269	Global catalog over SSL. Required for searching in the global catalog. Either port 3268 or 3269 should be open depending on the connection settings.

Setting up the Active Directory 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 Active Directory connector must be installed on the synchronization server.

System requirements for the Active Directory synchronization server

To set up synchronization with an Active Directory 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 2025
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016

- .NET 10.0 Desktop Runtime

  > **NOTE:** When connecting the target system, refer to the target system manufacturer's recommendations.

- If the synchronization server for the Active Directory target system is not a domain controller, the remote server administration tools (RSAT) must be installed on the synchronization server. For more information, see the *Microsoft documentation*.

Installing One Identity Manager Service with an Active Directory connector

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

Table 4: Properties of the Job server

Property	Value
Server function	Active Directory connector
Machine role	Server | Job Server | Active Directory

> **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.

2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service.

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, see Connection data for process generation.

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** drop-down.

      - 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 **Active Directory**.

5. On the **Server functions** page, select **Active Directory 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, see Configuring the One Identity Manager Service.

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, see One Identity Manager authentication modules.

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 drop-down or enter the server's name or IP address.

    To run the installation locally, select `Local installation` from the drop-down.

- **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 Active Directory domain

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Active Directory environment. The following describes the steps for initial configuration of a synchronization project. For more information, see Setting up synchronization.

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.

Information required to set up a synchronization project

> **IMPORTANT:** The domain controller and the domain must be resolved by DNS query for successful authentication. If the DNS cannot be resolved, the target system connection is refused.

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

Table 5: Information required to set up a synchronization project

Data	Explanation
Full domain name	Full domain name.
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 Active Directory on page 16.
DNS name of the domain controller.	Full name of the domain controller for connecting to the synchronization server to provide access to Active Directory objects. Example: `<Name of servers>.<Fully qualified domain name>`
Communications port on the domain controller	Communications port on the domain controller. LDAP default communications port is 389.
Authentication type	You can only connect to a target system if the correct type of authentication is selected. The **Secure** authentication type is used by default. For more information about authentication types, see the MSDN Library.
Synchronization server for Active Directory	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 must be installed on the synchronization server with the Active Directory connector.

Data	Explanation
	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: **Active Directory connector** • Machine role: **Server | Job Server | Active Directory** For more information, see System requirements for the Active Directory synchronization server on page 21.
One Identity Manager database connection data	• Database server • Database name • SQL login and password • 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. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed and an authentication method is set up • Active Directory connector is installed • Target system specific components are 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 server as remote connection server as well by installing the RemoteConnectPlugin.

Data	Explanation
	For more information, see Establishing remote connections.

Creating an initial synchronization project for Active Directory domains

IMPORTANT: The domain controller and the domain must be resolved by DNS query for successful authentication. If the DNS cannot be resolved, the target system connection is refused.

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 Active Directory 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. In the **Installation overview > Data synchronization** section, select the **Target system type Active Directory** and click **Run**.

   This starts the Synchronization Editor's project wizard.

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

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

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

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

Select the **Connect using remote connection server** and enter the remote connection properties.

Remote connection properties

- **Access parameters**

  - **Server**: Full server name or IP address of the server.

    To select an existing Job server as the remote connection server, click ⚒ and select the server from the drop-down. This displays all the Job servers that have the **One Identity Manager Service installed** server function selected.

  - **Port**: Port that is configured for the RemoteConnectPlugin.

- **Authentication**

  If **SecretAuthentication** is configured for the RemoteConnectPlugin:

  - **Secret**: Secret used by the Synchronization Editor to authenticate on the RemoteConnectPlugin.

  If **ADGroupAuthentication** is configured for the RemoteConnectPlugin, no data is required.

- **Options**

  - **Request timeout**: Maximum time allowed for a server query in seconds. If the time is exceeded, the request is canceled.

  - **Accept self-signed certificates**: Specifies whether self-signed certificates can be accepted.

5. On the **Domain selection** page, specify the Active Directory domain to synchronize.

   - Select the domain in the **Domain** list or enter the full domain name.

6. Enter the user account for accessing the domain on the **Credentials** page. This user account is used to synchronize Active Directory objects.

   a. To use a specified user account, enter the user account and password for logging into the target system.

      - OR -

      If you left this empty, the user account of the currently logged in user is used. In the case of synchronization, this is the user account that the One Identity Manager Service is running under. For more information about which permissions are required, see Users and permissions for synchronizing with Active Directory on page 16.

      > **NOTE:** If you do not enter a user account, the current user account is also used in the Synchronization Editor during configuration.
      >
      > The user account used with the Synchronization Editor may differ from the One Identity Manager Service's user account. In this case, it is recommended you use the **RemoteConnectPlugin**. This ensures that the same

> user account is used during configuration with the Synchronization Editor as is used in the service context.

    b. Click **Test** in the **Verify credentials** pane to test the connection to the domain.

7. Enter the domain controller for synchronization on the **Configure connection options** page and set the connection options.

- In the **Binding options** view, you define the authentication type for login to the target system. The `Secure` authentication type is used by default.

- In the **Enter or select domain controller** view, you define the domain controller.

    a. In the **Domain controller** drop-down, select an existing domain controller or enter the full name of the domain controller directly.

    b. In the **Port** input field, enter the communications post on the domain controller. LDAP default communications port is `389`.

    c. With the **Use SSL** option, define whether a secure connection should be used.

    d. Click **Test** to test the connection. The system tries to establish a connection to the domain controller.

8. Specify additional synchronization settings on the **Connector features** page. Configure the following settings.

Table 6: Additional settings

Property	Description
When restoring objects with the same distinguished name or GUID from the recycle bin.	Specifies whether deleted Active Directory objects are taken into account on insertion. Set this option if, when adding an object, the system first checks whether the object is in the Active Directory recycling bin and must be restored.
Allow read and write access to Remote Access Service (RAS) properties.	Specifies whether Remote Access Service (RAS) properties are synchronized. If the option is not set, default values are taken for synchronization. However, no properties are written or read. You can set these options at a later date.
Allow read and write access to the terminal service properties.	Specifies whether terminal server properties are synchronized. If the option is not set, default values are taken for synchronization. However, no properties are written or read. You can set these options at a later date.

> **NOTE:** The import of terminal server properties and RAS properties may slow down synchronization.

9. (Optional) On the **Additional Active Directory schema settings** page you can specify whether to modify the schema used by synchronization. You can add additional auxiliary classes to structural classes. The extension methods apply to the structural class and its derived classes. This configuration is only possible in expert mode.

10. On the last page of the system connection wizard, you can save the connection data.

    - Set the **Save connection data on local computer** 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.

11. 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.

12. 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.

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

Table 7: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.
	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`.
	NOTE: If you initially select this option, no write operations are possible in the target system. If you want to use this synchronization project later to publish changes to the

Option	Meaning
	target system, you have two options: a. Manually configure all required elements of the synchronization configuration (mapping, workflows and others). - OR - b. Create a new synchronization project to replace the previous one. Note that only one synchronization project can be set up for each base object.
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 schema classes whose schema types have write access.

14. 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.

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

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

    - An application role is created for the synchronization project owners with the name of the synchronization project. The identity that creates the synchronization project and the target system managers automatically become members of this application role.

      Assign additional members if required.

    - 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 in days.

Target system managers and synchronization project owners for Active Directory

To edit the synchronization configuration and the synchronized data with role-based login to the One Identity Manager tools, use the application roles for synchronization project owners and the target system managers. As soon as you have created a synchronization project, you can assign identities to these application roles.

Target system managers

Members of the **Target systems | Active Directory** default application role are permitted to edit all Active Directory objects in One Identity Manager. You can restrict this to specific domains by assigning child application roles to the domains. For more information, see Target system managers for Active Directory on page 208 and General main data for Active Directory domains on page 128.

Synchronization project owners

When a new synchronization project is created, an application role is automatically created for the owners of this synchronization project. Members of this application role configure the synchronization and edit synchronization templates in the Synchronization Editor. The following identities are automatically members of this application role:

- The synchronization project creator
- All target system managers of all base objects created in the synchronization project

Owners can edit the members of their application role in the Manager. In the Synchronization Editor, you can change the application role that is assigned to the synchronization project.

For more information, see Active Directory synchronization project owners on page 210.

Adjusting the synchronization configuration for Active Directory environments

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

You must customize the synchronization configuration to be able to regularly compare the database with the Active Directory 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.

- 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.

- To specify which Active Directory 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.

- 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, see Configuring synchronization.

Configuring synchronization in Active Directory 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 Active Directory 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 startup configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related topics

-

Configuring synchronization of several Active Directory domains

In some circumstances, it is possible to use a synchronization project to synchronize different Active Directory 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 Active Directory connector.
   - Declare the connection parameters. The connection parameters are saved in a special variable set.

   A startup 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 Active Directory domains on page 35

Supporting POSIX extensions

One Identity Manager support synchronization of POSIX properties for user accounts, contacts, and groups.

Corresponding synchronization steps are already provided in workflows in the default template for synchronization projects. These synchronization steps are created if the **posixAccount** and **posixGroup** schema classes exist in the schema. By default, the synchronization steps are disabled and must be enabled if required. Use the workflow wizard in the Synchronization Editor for this. For more information, see Editing synchronization steps.

Related topics

- POSIX properties for Active Directory user accounts on page 161
- POSIX properties for Active Directory contacts on page 177
- POSIX properties for Active Directory groups on page 184

Changing system connection settings of Active Directory 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.

Related topics

- Active Directory connector settings on page 234

Editing Active Directory domain 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 startup 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 Active Directory 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 > Startup configurations** category.
9. Select a startup 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, see Using variables and variable sets and Setting up base objects.

Editing target system connection properties

You can also use the system connection wizard to change the connection parameters. 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 connection parameters using 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.

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.
4. Edit the mapping.

   For more information, see Setting up mappings.

> **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.

Active Directory supports revision filtering. The Active Directory objects' Update Sequence Number (USN) is used as revision counter. The Update Sequence Number (USN) is a sequential number that is incremented when changes are made to Active Directory objects. An Active Directory object has its own USN on each domain controller. During synchronization, the highest USN of the rootDSE to be found on the domain controller is stored as revision in the One Identity Manager database (table `DPRRevisionStore`, column `value`). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is synchronized the next time, the Active Directory objects' USN is compared with the revision saved in the One Identity Manager database. This involves finding object pairs where one has a newer USN than the last time it was synchronized. Thus, only objects that have changed since the last synchronization are updated.

Synchronization is even faster if the change information on the schema type also takes deleted objects into account. If a schema type's objects were neither added, changed nor deleted, the synchronization step can be skipped. Objects must not be loaded for comparison. Active Directory provides the information about whether objects in the synchronized domain were added, changed, or deleted.

To use optimized revision filtering

- In the Designer, set the **Common | TableRevision** configuration parameter.

  Now each time a table changes, the table's revision date updates. This information is stored in the `QBMTableRevision` table, `RevisionDate` column. In this way, One Identity Manager identifies whether a table object has been added, changed, or deleted.

Synchronization with revision filtering compares a table's revision date and the domain's change information against the revision saved in the One Identity Manager database. If the revision date is older, no objects have been changed in this table since the previous synchronization. If the change information of the domain is also older, no objects in this domain have been changed since the previous synchronization. Therefore, synchronization does not carry out this step for the affected table. If the revision date or change information of the domain is newer, synchronization does carry out this step and the changed objects are determined as described above.

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 startup 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` drop-down.

To permit revision filtering for a startup configuration

- In the Synchronization Editor, open the synchronization project.
- Edit the startup configuration properties. Select the **Use revision filter** item from the `Revision filtering` drop-down.

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

> **NOTE:** If the **Common | TableRevision** is not set, all revision data in the `QBMTableRevision` table is deleted.

For more information, see How does revision filtering work.

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 Active Directory group (`Group`)
- 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 **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Active Directory** 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: `ADSAccountInADSGroup`, `ADSGroupInADSGroup`, and `ADSMachineInADSGroup`

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 `ADSAccountInADSGroup` assignment table:
>
> ```
> exists (select top 1 1 from ADSGroup g
>        where g.UID_ADSGroup = i.UID_ADSGroup
>        and <limiting condition>)
> ```

For more information, see Synchronizing and provisioning memberships.

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, see Include custom tables in the synchronization.

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

1. In the Manager, select the **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Active Directory** 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_ADSDomain).XObjectKey`
8. Save the changes.

Related topics

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 **Active Directory connector** server function to the Job server.

   All Job servers must access the same Active Directory 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, see Properties of base objects.

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, see Load balancing during provisioning and single object synchronization.

Related topics

- Job server for Active Directory-specific process handling on page 213

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 startup sequence to run synchronization. In a startup sequence, you can combine startup configurations from different synchronization projects and specify the order in which they are run.

For more information, see Defining startup sequences.

Related topics

- Pausing handling of target system specific processes (Offline mode) on page 55

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 > Startup configurations** category.
3. Select a startup 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 > Startup configurations** category.
3. Select a startup 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 startup 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 startup configurations that are used in startup sequences are not started individually at the same time. Assign startup sequences and startup configurations different schedules.
- Starting another synchronization process with different startup 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 startup configuration.
  - Use the schedule to ensure that the startup configurations are run in sequence.
  - Group startup configurations with the same start up behavior.

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 startup 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**.

Related topics

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

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 **Active Directory** 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 synchronizing member lists

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.

Related topics

- Configuring single object synchronization on page 44

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 **Active Directory > Target system synchronization: Active Directory** category.

   The navigation view lists all the synchronization tables assigned to the `Active Directory` 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.

> **TIP:**
>
> ***To display the 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. For memberships, select the object whose properties you want to display.

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 8: 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 (XOrigin>1) 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 **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Active Directory** 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 50

Managing Active Directory user accounts and Active Directory contacts through account definitions

In the default installation, after synchronizing, identities are automatically created for user accounts and contacts. If an account definition for the domain is not known at the time of synchronization, user accounts and contacts are linked to identities. However, account definitions are not assigned. The user accounts and contacts are therefore in a **Linked** state.

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

To manage user accounts and contacts 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 **Active Directory > User accounts > Linked but not configured > <domain>** category.

      - OR -

      In the Manager, select the **Active Directory > Contacts > Linked but not configured > <domain>** category.

   b. Select the **Assign account definition to linked accounts** task.

   c. In the **Account definition** drop-down, select the account definition.

   d. Select the user accounts that contain the account definition.

   e. Save the changes.

Related topics

- Account definitions for Active Directory user accounts and Active Directory contacts on page 58

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.

  For more information, see Simulating synchronization.

- Analyzing synchronization

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

  For more information, see Help for analyzing synchronization issues.

- 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.

  For more information, see Displaying synchronization logs and Configuring logs in One Identity Manager.

- 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, see Handling unexpected interruption of synchronization.

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, see Pausing handling of target system specific processes.

Related topics

- Deactivating synchronization on page 47

Managing Active Directory 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 an Active Directory 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, see Basic mechanisms for identity and user account administration.

Account definitions for Active Directory user accounts and Active Directory contacts

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.

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

For more information, see Using account definitions to create user accounts.

You can use account definitions to create Active Directory contacts for identities.

One Identity Manager 10.0 Administration Guide for Connecting to
Active Directory | **58**
Managing Active Directory user accounts and identities

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 **Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Click (**New**) in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Related topics

- Main data for account definitions on page 60
- Editing account definitions on page 59
- Assigning manage levels to account definitions on page 64

Editing account definitions

You can edit the main data of account definitions.

To edit an account definition

1. In the Manager, select the **Active Directory > 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 60
- Creating account definitions on page 59
- Assigning manage levels to account definitions on page 64

Main data for account definitions

Enter the following data for an account definition:

Table 9: 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 or contacts.
	For Active Directory user accounts, select **ADSAccount**. For Active Directory contacts, select **ADSContact**.
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 Active Directory domains.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts or contacts.
Risk index	Value for evaluating the risk of assigning the account 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 Risk assessment.
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	Specifies whether the account definition is automatically

Property	Description
identities	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 or contact remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account or the associated contact 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 or contact remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account or the associated contact 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 or contact remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account or the associated contact 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 or contact remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account or the associated contact is deleted.

Property	Description
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.

- 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.

For more information, see Account definitions and manage levels.

To edit a manage level

1. In the Manager, select the **Active Directory > 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

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.

To create a manage level

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

2. Click (**New**) in the result list.

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

4. Save the changes.

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 **Active Directory > 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 10: 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:

Property	Description
	• **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, for example, if the container for a user account formed using the identity's department, cost center, location, or business role and which default values will be used if no IT operating data can be found through the 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.

- Container
- Home server
- Profile server
- Terminal home server

- Terminal profile server
- Container for disabled user accounts
- Groups can be inherited
- Identity
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **Active Directory > 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 drop-down, you can select the columns that use the `TSB_ITDataFromOrg` script in their template.

     For more information, see Templates and processes for implementing account definitions.
   - **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 | ADS | Accounts | MailTemplateDefaultValues** configuration parameter.
5. Save the changes.

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: Mapping IT operating data

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.

For more information, see Determining valid IT operating data for the target systems.

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. Open the drop-down by clicking the arrow.

        b. Select the table that maps the target system or the `TSBAccountDef` table for 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 drop-down, you can select the columns that use the `TSB_ITDataFromOrg` script in their template.

  For more information, see Templates and processes for implementing account definitions.

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

4. Save the changes.

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 **Active Directory > 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.

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, see Preparing hierarchical roles for company resource assignments.

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 **Active Directory > 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.

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 **Active Directory > 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.

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 **Active Directory > 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.

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 **Active Directory > 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.

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 **Active Directory > 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 the system role assignment.
>
> *To remove an assignment*
>
> - Select the system role and double-click ✓.

5. Save the changes.

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. To assign the account definition to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
5. To assign the account definition to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.
6. Save the changes.

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

1. In the Manager, select the **Active Directory > 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. To assign the account definition to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.

5. To assign the account definition to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.

6. 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. To remove the account definition from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.

5. To remove the account definition from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.

6. Save the changes.

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

1. In the Manager, select the **Active Directory > 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. To remove the account definition from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.

5. To remove the account definition from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.

6. 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 **Active Directory > 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, see Assigning and removing products.

Assigning account definitions to Active Directory 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 **Active Directory > Domains** category.

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

3. From the **Account definition (initial)** drop-down, select the account definition for
 user accounts.

4. From the **Contact definition (initial)** drop-down, select the account definition
 for contacts.

5. From the **Mail contact definition (initial)** drop-down, select the account definition
 for mail contacts.

6. From the **Mail user definition (initial)** drop-down, select the account definition for mail users.

7. Save the changes.

Related topics

- Assigning identities automatically to Active Directory user accounts on page 78

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 **Active Directory > 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 **Active Directory > 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 **Active Directory > 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 **Active Directory > 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 information, see Unsubscribing products.

    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 **Active Directory > 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 **Active Directory > 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** drop-down, 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 **Active Directory > 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 **Active Directory > 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 Active Directory 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, see Assigning identities automatically to user accounts.

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 | ADS | PersonAutoFullsync** configuration parameter and select the required mode.

- If you want identities to be assigned outside synchronization, in the Designer, set the **TargetSystem | ADS | PersonAutoDefault** configuration parameter and select the required mode.

- In the **TargetSystem | ADS | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to identities shall take place.

  Example:

  ```
  ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $
  ```

  > **TIP:** You can edit the value of the configuration parameter in the **Exclude list for automatic identity assignment** dialog.
  >
  > ***To edit the exclude list for automatic identity assignment***
  >
  > 1. In the Designer, edit the **PersonExcludeList** configuration parameter.
  > 2. Click **...** next to the **Value** field.
  >
  >   This opens the **Exclude list for Active Directory user accounts** dialog.
  > 3. To add a new entry, click **Add**.
  >
  >   To edit an entry, select it and click **Edit**.
  > 4. Enter the name of the user account that does not allow identities to be assigned automatically.
  >
  >   Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.
  > 5. To delete an entry, select it and click **Delete**.
  > 6. Click **OK**.

- Use the **TargetSystem | ADS | 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 Active Directory user accounts and Active Directory contacts through account definitions on page 53.

Related topics

Editing search criteria for automatic identity assignment

NOTE: One Identity Manager supplies a default mapping for the 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 `ADSDomain` 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.

To specify criteria for identity assignment

1. In the Manager, select the **Active Directory > 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 11: Default search criteria for user accounts and contacts

Apply to	Identity column	Column for user account/contact
Active Directory user accounts	Central user account (CentralAccount)	Login name (pre Win2000) (SAMAccountName)
Active Directory contacts	Central user account (CentralAccount)	Name (Cn)

5. Save the changes.

For more information, see Define search criteria for identity assignment.

Related topics

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

> **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** drop-down, and select a manage level in the **Assign this account manage level** drop-down.

    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 drop-down.

    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** drop-down, and select a manage level in the **Assign this account manage level** drop-down.

    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 Active Directory 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 **Active Directory > 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 and editing Active Directory user accounts on page 145

Changing manage levels for Active Directory contacts

The **Unmanaged** manage level is used when you create contacts through automatic identity assignment. You can change the contact's manage level later.

To change the manage level for a contact

1. In the Manager, select the **Active Directory > Contacts** category.

2. Select the contact in the result list.

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

4. In the **Manage level** drop-down, on the **General** tab, select the manage level.

5. Save the changes.

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 12: 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).

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 Active Directory user accounts and Active Directory contacts on page 58

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 an administrative user account 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 **Active Directory > 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 **Active Directory > 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 an administrative user account for multiple identities

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

Prerequisites

- 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 **Active Directory > 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** drop-down, select `Shared identity`.

2. Link the user account to an identity.

   a. In the Manager, select the **Active Directory > 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** drop-down, 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 **Active Directory > 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.

Related topics

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 | ADS | Accounts | PrivilegedAccount | SAMAccountName_ PrefixTargetSystem** configuration parameter.
> - To use a postfix for the login name, in the Designer, set the **TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_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

Updating identities when Active Directory user account are modified

In One Identity Manager, modifications to identity properties are forwarded to the associated user accounts and subsequently provisioned in the target system. In certain circumstances, it may be necessary to forward user account modifications in the target system to identity properties in One Identity Manager.

Example: Changes to user accounts in the target system

During testing, user accounts from the target system are only read into One Identity Manager and identities created. User account administration (creating, modifying, and deleting) should be done later through One Identity Manager. During testing, user accounts are modified further in the target system, which can lead to drifts in user account properties and identity properties. Due to this, user account modifications loaded on resynchronization should be temporarily published to identities who are already created. This means data is not lost when user account administration is put into effect through One Identity Manager.

To update identities when user accounts are modified

- In the Designer, set the **TargetSystem | ADS | PersonUpdate** configuration parameter.

Modifications to user accounts are loaded into One Identity Manager during synchronization. These modifications are forwarded to the associated identities through subsequent scripting and processing.

NOTE:

- When making changes to user accounts, the identities are only updated for user accounts with the **Unmanaged** manage level and that are linked to an identity.

- Only the identity created by the modified user account is updated. The data source from which the identity was created is shown in the **Import data source** property. If other user accounts are assigned to the identity, changes to these user accounts do not cause the identity to be updated.

- For identities who do not yet have the **Import data source** set, the user account's target system is entered as the data source for the import during the first update of the connected user account.

User account properties are mapped to identity properties using the `ADS_PersonUpdate_ADSAccount` script. Contact properties are mapped to identity properties using the `ADS_PersonUpdate_ADSContact` script. To make the mapping easier to customize, the scripts are overwritable.

To customize, create a copy of the script and start the script coding follows:

`Public Overrides Function ADS_PersonUpdate_ADSAccount(ByVal UID_Account As String, OldAccountDN As String, ProcID As String)`

`Public Overrides Function ADS_PersonUpdate_ADSContact(ByVal UID_Account As String, OldAccountDN As String, ProcID As String)`

This redefines the script and overwrites the original. The process does not have to be changed in this case.

Automatic creation of departments and locations based on user account information

You can create new departments and locations in One Identity Manager based on user account department and location data. Furthermore, departments, and locations are assigned to identities of the user accounts as primary department and primary location. These identities can obtain their company resources through these assignments if One Identity Manager is configured correspondingly.

Prerequisites for using this method

Identities must be created automatically when user accounts are added or modified. At least one of the following configuration parameters must be activated and the corresponding method implemented.

- **TargetSystem | ADS | PersonAutoDefault:** Automatic identity assignment for user accounts added to the database outside synchronization based on the given mode.

- **TargetSystem | ADS | PersonAutoFullsync**: Based on the given mode, automatic identity assignment is carried out on user accounts created or updated in the database by synchronization.

- **TargetSystem | ADS | PersonUpdate**: Identities are updated continuously from linked user accounts.

To implement this method

- In the Designer, set the **TargetSystem | ADS | AutoCreateDepartment** configuration parameter to generate departments from the user account information.

- In the Designer, set the **TargetSystem | ADS | AutoCreateLocality** configuration parameter to generate locations from the user account information.

Related topics

- Further data for identifying Active Directory user accounts on page 159
- Assigning identities automatically to Active Directory user accounts on page 78
- Updating identities when Active Directory user account are modified on page 89

Specifying deferred deletion for Active Directory user accounts and Active Directory contacts

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 `ADSAccount` and the `ADSContact` tables.

- 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 `ADSAccount` and `ADContact` tables.

Example: Script for object-specific deferred deletion

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 = TimeSpan.FromDays(10)

End If
```

For more information, see Specifying deferred deletion for objects.

Managing memberships in Active Directory groups

Active Directory user accounts, Active Directory contacts, and Active Directory computers can be grouped into Active Directory groups that can be used to regulate access to resources.

In One Identity Manager, you can assign Active Directory groups directly to user accounts, contacts, and 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.

Assigning Active Directory groups to Active Directory user accounts, Active Directory contacts, and Active Directory computers

Active Directory groups can be assigned directly or indirectly to Active Directory user accounts, Active Directory contacts, and Active Directory computers.

Identities (workdesks or devices) and Active Directory groups are grouped into hierarchical roles in the case of indirect assignment. The number of Active Directory 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 Active Directory user account, the Active Directory user account is added to the Active Directory group.

- If you add an identity to roles and that identity owns an Active Directory contact, the Active Directory contact is added to the Active Directory group.

- If you add a device to roles, the Active Directory computer that references the device is added to the Active Directory groups.

- If a device owns a workdesk and you add the workdesk to roles, the Active Directory computer, which references this device, is also added to all Active Directory groups of the workdesk's roles.

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

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

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

For more information, see Basics for mapping company structures in One Identity Manager, Preparing products for requesting, and Managing system roles.

Prerequisites for indirect assignment of Active Directory groups

Identities (workdesks or devices) and Active Directory groups are grouped into hierarchical roles in the case of indirect assignment. When assigning Active Directory groups indirectly, check the following settings and modify them if necessary.

Prerequisites for indirect assignment of Active Directory groups to identities' Active Directory user accounts and Active Directory contacts

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

Prerequisites for indirect assignment of Active Directory groups to Active Directory computers

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

Prerequisites for indirect assignment to Active Directory groups to Active Directory computers through workdesks

1. Assignment of workdesks and groups is permitted for the role class (department, cost center, location, or business role).

2. The computer is connected to a device labeled as PC or server. This 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 information, see Basic principles for assigning company resources.

Related topics

- Creating and editing Active Directory user accounts on page 145
- General main data of Active Directory user accounts on page 146
- Creating and editing Active Directory contacts on page 171
- General main data for Active Directory contacts on page 172
- Active Directory computers on page 192
- Main data for Active Directory computers on page 193

Assigning Active Directory groups to departments, cost centers and locations

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

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

1. In the Manager, select the **Active Directory > 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 Active Directory groups** task.
4. In the **Add assignments** pane, assign groups.

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

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

5. Save the changes.

Related topics

Assigning Active Directory 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 it is assigned to user accounts, contacts, and computers through this business role.

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

1. In the Manager, select the **Active Directory > 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 Active Directory 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

- Prerequisites for indirect assignment of Active Directory groups on page 94

Adding Active Directory 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 Active Directory user accounts owned by these identities inherit the group.

If you assign a system role to workdesks, all Active Directory computers associated with this workdesk inherit the group.

> **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 Managing system roles.

To assign a group to system roles

1. In the Manager, select the **Active Directory > 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 the system role assignment.
   >
   > **To remove an assignment**
   >
   > - Select the system role and double-click ✅.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Active Directory groups on page 94

Adding Active Directory 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 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 **Active Directory > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Active Directory groups** (role-based login) category.

2. In the result list, select the group.

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

4. To assign the group to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, double-click on the shelves.

5. To assign the group to IT Shop templates, select the **IT Shoptemplates** tab and, in the **Add assignments** section, double-click on the templates.

6. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager, select the **Active Directory > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Active Directory groups** (role-based login) category.

2. In the result list, select the group.

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

4. To remove the group from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.

5. To remove the group from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.

6. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **Active Directory > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Active Directory 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, see Assigning and removing products.

Related topics

- Prerequisites for indirect assignment of Active Directory groups on page 94
- General main data of Active Directory groups on page 182
- Adding Active Directory groups automatically to the IT Shop on page 100

Adding Active Directory groups automatically to the IT Shop

To add groups automatically to the IT Shop

1. In the Designer, set the **QER | ITShop | AutoPublish | ADSGroup** configuration parameter.

2. In the Designer, set the **QER | ITShop | AutoPublish | ADSGroup | ExcludeList** configuration parameter and specify the Active Directory groups that are not to be added automatically to the IT Shop.

   Example:

   ```
   .*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS
   ```

3. (Optional) In the Designer, set the **QER | ITShop | AutoPublish | ADSGroup | AutoFillDisplayName** configuration parameter.

   If the configuration parameter is set, a display name is be created for Active Directory groups if no display name exists yet. The display name of necessary to display the group in the Web Portal, for example.

4. Compile the database.

The system entitlements are added automatically to the IT Shop from now on.

The following steps are run to add a group to the IT Shop.

1. A service item is determined for the system entitlement.

   The service item is tested for each system entitlement and modified if required. The name of the service item corresponds to the name of the system entitlement.

   - The service item is modified if the system entitlement has a service item.
   - System entitlements without a service item are allocated a new service item.

2. The service item is assigned to one of the default service categories.

3. An application role for product owners is determined and the service item is assigned.

   Product owners can approve requests for membership in these system entitlements. By default, the account manager of a system entitlement is determined as the product owner.

   > **NOTE:** The application role for the product owner must be added under the **Request & Fulfillment | IT Shop | Product owner** application role.

   - If the account manager of the system entitlement is already a member of an application role for product owners, this application role is assigned to the service item. Therefore, all members of this application role become product owners of the system entitlement.
   - If the account manager of the system entitlement is not yet a member of an application role for product owners, a new application role is created. The name of the application role corresponds to the name of the account manager.
     - If the account manager is a user account or a contact, the user account's identity or the contact's identity is added to the application role.
     - If it is a group of account managers, the identities of all this group's user accounts are added to the application role.
   - If the system entitlement does not have an account manager, the **Request & Fulfillment | IT Shop | Product owner | Without owner in AD** default application role is used.

4. The system entitlement is labeled with the **IT Shop** option and assigned to the **Active Directory groups** IT Shop shelf in the **Identity & Access Lifecycle** shop.

Subsequently, the shop's customers can request memberships in system entitlement through the Web Portal.

NOTE: When a system entitlement is irrevocably deleted from the One Identity Manager database, the associated service item is also deleted.

Related topics

- Adding Active Directory groups to the IT Shop on page 99

Assigning Active Directory user accounts directly to Active Directory 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.

To assign user accounts directly to a group

1. In the Manager, select the **Active Directory > 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.

NOTE: The primary group of a user account is already assigned and is marked as `Does not apply yet`. Edit the user account's main data to change its primary group.

Related topics

- Assigning Active Directory groups directly to Active Directory user accounts on page 103 Assigning Active Directory groups to business roles on page 97
- Adding Active Directory groups automatically to the IT Shop on page 100

Assigning Active Directory groups directly to Active Directory user accounts

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

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

To assign groups directly to user accounts

1. In the Manager, select the **Active Directory > 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.

> **NOTE:** The primary group of a user account is already assigned and is marked as `Does not apply yet`. Edit the user account's main data to change its primary group.

Related topics

Assigning Active Directory contacts directly to Active Directory groups

Groups can be assigned directly or indirectly to a contact. Indirect assignment is done by allocating the identity and groups into company structures such as departments, cost centers, locations, or business roles. If the identity has a contact in Active Directory, the groups in the role are inherited by this contact.

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

To assign a group directly to contacts

1. In the Manager, select the **Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Assign contacts** task.

4. In the **Add assignments** pane, assign the contacts.

   > **TIP:** In the **Remove assignments** pane, you can remove contact assignments.
   >
   > ### To remove an assignment
   >
   > - Select the contact and double-click ⊘.

5. Save the changes.

Related topics

Active Directory Assign groups directly to Active Directory Contacts

Groups can be assigned directly or indirectly to a contact. Indirect assignment is done by allocating the identity and groups into company structures such as departments, cost centers, locations, or business roles. If the identity has a contact in Active Directory, the groups in the role are inherited by this contact.

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

To assign groups directly to a contact

1. In the Manager, select the **Active Directory > Contacts** category.

2. Select the contact 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 Active Directory groups to Active Directory user accounts, Active Directory contacts, and Active Directory computers on page 93

Assigning Active Directory computers directly to Active Directory groups

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

To assign a group directly to computers

1. In the Manager, select the **Active Directory > 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.

> **NOTE:** The primary group of a computer is already assigned and is marked as `Does not apply yet`. Edit the computer's main data to change its primary group.

Related topics

- Assigning Active Directory groups directly to Active Directory computers on page 105
- Main data for Active Directory computers on page 193

Assigning Active Directory groups directly to Active Directory computers

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

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

To assign a computer directly to groups

1. In the Manager, select the **Active Directory > Computers** category.

2. Select the computer in the result list.

3. Select **Assign groups**.

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.

> **NOTE:** The primary group of a computer is already assigned and is marked as `Does not apply yet`. Edit the computer's main data to change its primary group.

Related topics

Effectiveness of membership in Active Directory 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 `ADSAccountInADSGroup` and `BaseTreeHasADSGroup` tables by the `XIsInEffect` column.

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 13: Specifying excluded groups (`ADSGroupExclusion` table)

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

Table 14: 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 15: 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.

- Mutually exclusive groups belong to the same domain

To exclude a group

1. In the Manager, select the **Active Directory > 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.

Active Directory group inheritance based on categories

Groups and be selectively inherited by user accounts and contacts in One Identity Manager. The groups and user accounts (contacts) are divided into categories in the process. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains tables that map the user accounts (contact) and the groups. Specify your categories for user account (contacts) in the table for user accounts (contacts). Enter your categories for groups in the group table. Each table contains the **Position 1** to **Position 36** category positions.

Every user account (contact) can be assigned to one or more categories. Each group can also be assigned to one or more categories. If at least one user account (contact) category position matches an assigned structural profile, the structural profile is inherited by the user account (contact). If the group or user account (contact) is not in classified into categories, the group is also inherited by the user account (contact).

> **NOTE:** Inheritance through categories is only taken into account when groups are assigned indirectly through hierarchical roles. Categories are not taken into account when assigning groups to user accounts and contacts.

Table 16: Category examples

Category position	Categories for user accounts	Categories for groups
1	Default user	Default entitlements
2	System users	System user entitlements
3	System administrator	System administrator entitlements

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: Assignment overview

- 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 17: Meaning of icons in the report toolbar

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

Login credentials for Active Directory 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.

Password policies for Active Directory 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.

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, see Password policies for identities.

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, see Password policies for identities.

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.

The **Active Directory password policy** is predefined for Active Directory. You can apply this password policy to Active Directory user accounts passwords (ADSAccount.UserPassword) of an Active Directory domain or an Active Directory 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.

> **NOTE:** One Identity Manager password policies, global account policy settings for the Active Directory domain, and Active Directory account policies are all taken into account when verifying user passwords.
>
> Ensure that the password policy does not violate the target system's requirements.

Related topics

- Global account policies for Active Directory domains on page 130
- Active Directory account policies for Active Directory domains on page 134

Using password policies

The **Active Directory password policy** is predefined for Active Directory. You can apply this password policy to Active Directory user accounts passwords (`ADSAccount.UserPassword`) of an Active Directory domain or an Active Directory 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.

> **NOTE:** One Identity Manager password policies, global account policy settings for the Active Directory domain, and Active Directory account policies are all taken into account when verifying user passwords.
>
> Ensure that the password policy does not violate the target system's requirements.

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 Active Directory container.
4. Password policy of the user account's Active Directory 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 **Active Directory > 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. Open the drop-down by clicking the arrow.
     2. Select one of the following references:

- 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 **Active Directory > 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** drop-down, select the new password policy you want to apply.
6. Save the changes.

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 **Active Directory > Basic configuration data > Password policies** category.
2. Click (**New**) in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

Using 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 **Active Directory > 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.

General main data of password policies

Enter the following main data of a password policy.

Table 18: 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.

ONE IDENTITY

Policy settings

Define the following settings for a password policy.

Table 19: 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. **NOTE:** If, during synchronization, a more restrictive value for an Active Directory domain's global account policy is found than the one on the One Identity Manager password policy, this value is the one that will be applied to the domain's One Identity Manager password policy. If this One Identity Manager password policy is used for other domains the value also applies to these domains.
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 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.
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.

Property	Meaning
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. **NOTE:** If, during synchronization, a more restrictive value for an Active Directory domain's global account policy is found than the one on the One Identity Manager password policy, this value is the one that will be applied to the domain's One Identity Manager password policy. If this One Identity Manager password policy is used for other domains the value also applies to these domains.
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.

Character classes for passwords

Specify which characters are permitted for a password.

Table 20: Character classes for passwords

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

Property	Meaning
	• 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 letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.

Property	Meaning
letters	
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.

Script for checking passwords

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example: 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 **Active Directory > 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. (Optional) On the **Scripts** tab, in the **Additional requirements** field, enter the description of the additional requirements for the password that are checked by the script.

   f. Save the changes.

Related topics

- Script for generating a password on page 122

Script for generating a password

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

ONE IDENTITY

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 **Active Directory > 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

- Script for checking passwords on page 121

Editing the password exclusion list

You can add terms to a exclusion list to stop them from being used in passwords.

> **NOTE:** The exclusion list applies globally to all password policies.

To add a term to the exclusion list

1. In the Designer, select the **Base data > Security settings > Password exclusion list** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude.
3. Save the changes.

Verifying passwords

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

To verify if a password conforms to the password policy

1. In the Manager, select the **Active Directory > 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 password generation

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

To generate a password that conforms to the password policy

1. In the Manager, select the **Active Directory > 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 Active Directory user accounts

You have the following possible options for issuing an initial password for a new Active Directory user account:

- 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 | ADS | 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 Active Directory user accounts on page 113

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:

ONE IDENTITY

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see Setting up the email notification system.

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 Central password of an identity.

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 Determining the language for identities.

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 | ADS | Accounts | InitialRandomPassword** configuration parameter.

2. In the Designer, set the **TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.

3. In the Designer, set the **TargetSystem | ADS | 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 | ADS | 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 Active Directory objects in One Identity Manager

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

Active Directory domains

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

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

To edit main data of an Active Directory domain

1. In the Manager, select the **Active Directory > 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.

Related topics

- Synchronizing single objects on page 49

General main data for Active Directory domains

Enter the following general main data.

Table 21: Domain main data

Property	Description
Domain	NetBIOS domain name. This corresponds to the pre-Windows 2000 domain names. The domain name cannot be changed later.
Parent domain	Parent domain for mapping a hierarchical domain structure. The full name and the defined name are automatically updated through templates.
Domain subtype	Active Directory functional level. There are several features available in Active Directory at functional level. Refer to the documentation for the appropriate Windows to find out which functional levels are supported by the domain controller's Windows Server operating system to be implemented. Following functional levels are supported in One Identity Manager: - Windows Server 2003 native - Windows Server 2003 mixed - Windows Server 2008 - Windows Server 2008 R2 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2025
Display name	Name used to display the domain in the user interface. This is preset with the domain NetBIOS name; however, the display name can be changed.
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 definition is given. This is the case on initial synchronization, for example.
Contact definition (initial)	Initial account definition for creating contacts. These account definitions

Property	Description
	are used if automatic assignment of identities to contacts is used for this domain, resulting in administered user accounts (**Linked configured** state). The account definition's default manage level is applied.
	Contacts are only linked to the identity (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role in which target system managers are specified for the domain. Target system managers only edit the objects from domains that are assigned to them. Therefore, each domain can have a different target system manager assigned to it.
	Select the One Identity Manager application role whose members are responsible for administration of this domain. Use the ⊞ button to add a new application role.
Synchronized by	Type of synchronization through which the data is synchronized between the domain and One Identity Manager. You can no longer change the synchronization type once objects for these domains are present in One Identity Manager.

If you create a domain with the Synchronization Editor,
`One Identity Manager` is used.

Table 22: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Active Directory connector	Active Directory 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.

Description	Text field for additional explanation.

Related topics

- Assigning identities automatically to Active Directory user accounts on page 78
- Target system managers for Active Directory on page 208
- Displaying information about the Active Directory forest on page 133

Global account policies for Active Directory domains

When you set up a user account, globally defined account policies and data are applicable for issuing passwords. You can enter these setting against the domain. Account policies apply when user accounts are newly added.

For domains from the functional level `Windows Server 2008 R2` and above, it is possible to define multiple policies. You can also define password policies in One Identity Manager that you can apply to the user account passwords.

> **NOTE:** One Identity Manager password policies, global account policy settings for the Active Directory domain, and Active Directory account policies are all taken into account when verifying user passwords.

Enter the following data for global account policies.

Table 23: Account policies for domains

Property	Description
Minimum password length	Minimum length of the password. Use this option to specify that a password has to be complex. **NOTE:** If, during synchronization, a more restrictive value for an Active Directory domain's global account policy is found than the one on the One Identity Manager password policy, this value is the one that will be applied to the domain's One Identity Manager password policy. If this One Identity Manager password policy is used for other domains the value also applies to these domains.
Minimum password lifetime	Minimum age of the password. Enter the length of time a password has to be used before the user is allowed to change it.
Max. password age	Maximum age of the password. Enter the length of time a password can be used before it expires.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.
Password history	Enter the number of passwords to be saved. For example, if you enter the value **5**, the last 5 passwords for the user are saved. **NOTE:** If, during synchronization, a more restrictive value for an Active Directory domain's global account policy is found than the one on

Property	Description
	the One Identity Manager password policy, this value is the one that will be applied to the domain's One Identity Manager password policy. If this One Identity Manager password policy is used for other domains the value also applies to these domains.
Lock duration [min]	Lock duration in minutes. Enter the time period the account should be locked for before it is automatically reset.
Reset account [min]	Duration in minutes of account reset. Enter the time period that can elapse between two invalid attempts to enter a password before a user account is locked.

Related topics

- Password policies for Active Directory user accounts on page 113
- Active Directory account policies for Active Directory domains on page 134
- Password data for Active Directory user accounts on page 151

Active Directory specific main data for Active Directory domains

Enter the following main data for Active Directory:

Table 24: Active Directory data

Property	Description
Domain name (pre Win2000)	Pre-Windows 2000 computer name.
Full domain name	Name of the domain confirming to DNS syntax. `<name of this domain>.<name of parent domain>.<name of root domain>.`
Account manager	Manager responsible for the domain. ***To specify an account manager*** 1. Open the drop-down by clicking the arrow. 2. Select the table that maps the account manager. 3. In the **Account manager** menu, select the manager.

Property	Description
	4. Click **OK**.
Distinguished name	Distinguished name of the domain. The distinguished name is determined using a template from the full domain name and cannot be edited.
Forest	The name of the forest to which the domain belongs. This name should be given if group memberships are mapped cross-domain.
Enable recycling bin	(As of functional level `Windows Server 2008 R2`) Specifies whether the recycling bin is enabled. The property is imported by the synchronization and should not be edited in One Identity Manager.
Retention period	(As of function level `Windows Server 2008 R2`) Retention period of objects in the recycling bin. The property is imported by the synchronization and should not be edited in One Identity Manager.
Complex passwords	Specifies whether complex passwords are implemented in the domain. Complex passwords must fulfill certain minimum prerequisites.
	For domains from the functional levels `Windows Server 2008 R2` and above, it is possible to define this setting using account policies.
Default home drive	Default home drive to be connected when a user logs in.
Structural object class	Structural object class representing the object type. By default, the domains in One Identity Manager are created using the object class `DOMAINDNS`.
Object class	List of classes defining the attributes for this object. The object classes listed are read in from the database during synchronization with the Active Directory environment. You can also enter object classes in to the input field.

Related topics

- Validity of group memberships on page 185
- Procedure for deleting Active Directory user accounts in One Identity Manager on page 166
- Active Directory account policies for Active Directory domains on page 134
- Preparing a home server and profile server for creating user directories on page 219

Defining categories for the inheritance of Active Directory groups

Groups and be selectively inherited by user accounts and contacts in One Identity Manager. The groups and user accounts (contacts) are divided into categories in the process. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains tables that map the user accounts (contact) and the groups. Specify your categories for user account (contacts) in the table for user accounts (contacts). Enter your categories fro groups in the group table. Each table contains the **Position 1** to **Position 36** category positions.

To define a category

1. In the Manager, select the **Active Directory > Domains** category.

2. Select the domain in the result list.

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

4. Select the **Categories** tab.

5. Expand the root in the respective table.

6. To enable the category, double-click ⊗.

7. Enter a category name for user accounts, contacts, and groups in your login language.

8. Save the changes.

Related topics

- Active Directory group inheritance based on categories on page 109

Displaying information about the Active Directory forest

The information about the forest is required in One Identity Manager to map trusted domains and group memberships across domains.

The information about the Active Directory forest is loaded into One Identity Manager during synchronization.

To display information about a forest

1. In the Manager, select the **Active Directory > Forest** category.

2. Select a forest in the result list.

3. To display a domain's forest, select the **Forest overview** task.

4. To display a forest's main data, select the **Change main data** task.

Related topics

Entering and testing trusted Active Directory domains

For an explanation of the concept of trusts in Active Directory, refer to your Windows Server documentation. Users can access resources in other domains depending on the domain trusts.

- Explicit trusts are loaded into Active Directory by synchronizing with One Identity Manager. Domains which are trusted by the currently synchronized domains are found.
- To declare implicit two-way trusts between domains within an Active Directory forest in One Identity Manager, ensure that the parent domain is entered in all child domains.

To enter the parent domain

1. In the Manager, select the **Active Directory > Domains** category.
2. Select the domain in the result list.
3. Select the **Change main data** task.
4. Enter the parent domain.
5. Save the changes.

   Implicit trusts are created automatically.

To test trusted domains

1. In the Manager, select the **Active Directory > Domains** category.
2. Select the domain in the result list.
3. Select **Specify trust relationships**.

   This shows domains that trust the selected domain.

Active Directory account policies for Active Directory domains

Set up global account policies for a domain. This information is declared in the domain as default settings. For domains from the functional levels `Windows Server 2008 R2` and above, it is possible to define multiple account policies. This allows individual users and

groups to be subjected to stricter account policies as intended for global groups. Refer to your Active Directory documentation for more information about the concept of fine-grained password policies under Windows Server.

You can also define password policies in One Identity Manager that you can apply to the user account passwords.

> **NOTE:** One Identity Manager password policies, global account policy settings for the Active Directory domain, and Active Directory account policies are all taken into account when verifying user passwords.

Related topics

- Assigning Active Directory account policies to Active Directory user account and Active Directory groups on page 137
- Password policies for Active Directory user accounts on page 113
- Global account policies for Active Directory domains on page 130

Creating and editing Active Directory account policies

Account policies are loaded into the One Identity Manager database during synchronization. You have the option to edit existing account policies and add new ones.

To enter main data of an account policy

1. In the Manager, select the **Active Directory > Account policies** category.
2. Select the account policy in the result list and run the **Change main data** task.

   - OR -

   Click (**New**) in the result list.
3. Edit the account policy's main data.
4. Save the changes.

Related topics

- General main data for an Active Directory account policy on page 136
- Guidelines for Active Directory account guidelines on page 136

General main data for an Active Directory account policy

Enter the following general main data.

Table 25: General main data of an account policy

Property	Description
Name	Account policy name
Domain	Active Directory domain for which the account policy is available.
Distinguished name	Distinguished name of the account policy. The distinguished name is formed based on rules and is made up of the name of the account policy, the system container for password policies **Password Settings Container**, and the domain.
Display name	Display name to display in the One Identity Manager tools.
Simple display	Display name for systems that cannot interpret all the characters of normal display names.
Description	Text field for additional explanation.

Related topics

- Guidelines for Active Directory account guidelines on page 136

Guidelines for Active Directory account guidelines

Enter the following settings for the policy.

Table 26: Main data for a policy definition

Property	Description
Lock duration [min]	Lock duration in minutes. Enter the time period the account should be locked for before it is automatically reset.
Reset account [min]	Duration in minutes of account reset. Enter the time period that can elapse between two invalid attempts to enter a password before a user account is locked.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is locked.
Max. password age	Maximum age of the password. Enter the length of time a password can be used before it expires.

Property	Description
Minimum password lifetime	Minimum age of the password. Enter the length of time a password has to be used before the user is allowed to change it.
Minimum password length	Minimum length of the password. Use this option to specify that a password has to be complex.
Password history	Enter the number of passwords to be saved. For example, if you enter the value **5**, the last 5 passwords for the user are saved.
Ranking	Ranking for password settings. If several account polices are assigned to a user account or a group, the account policy is used that has the lowest value.
Complex passwords	Specifies how complicated the password has to be. Complex passwords must fulfill certain minimum prerequisites. For more information, see the documentation for your Windows Server.
Save passwords with reversible encryption	Details for encrypting passwords. By default, passwords that are saved in Active Directory are encrypted. When you use this option, passwords are saved in plain text and can be restored again.

Related topics

- General main data for an Active Directory account policy on page 136

Assigning Active Directory account policies to Active Directory user account and Active Directory groups

If several account policies are assigned to one user account, the actual account policy is found using specific rules. If there are no special account policy the domain setting apply. Refer to the concept of fine-grained password guidelines under Active Directory in the documentation for your Windows Server for information about the calculation rules.

To specify account policies for user accounts

1. In the Manager, select the **Active Directory > Account policies** category.

2. Select the account policy in the result list.

3. Select in 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.

To specify account policies for groups

1. In the Manager, select the **Active Directory > Account policies** category.
2. Select the account policy 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.

Editing the synchronization project for an Active Directory 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 **Active Directory > 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 Active Directory environments on page 35

Monitoring the number of memberships in Active Directory groups and Active Directory containers

Table 27: Effective configuration parameters

Configuration parameter	Meaning
TargetSystem	ADS	MemberShipRestriction	Container	Number of Active Directory objects allowed per container before warning email is sent.
TargetSystem	ADS	MemberShipRestriction	Group	Number of Active Directory objects allowed per group before warning email is sent.
TargetSystem	ADS	MemberShipRestriction	MailNotification	Default mail address for sending warning emails.

A mechanism to monitor user account memberships to limit the number of members in groups and containers,

- The `ADSAccountInADSGroup` and `ADSAccount`tables are monitored with respect to the number of user account memberships in a group and the number of user accounts in a container.

- The `ADSContactInADSGroup` and `ADSContact` tables are monitored with respect to the number of contact memberships in a group and the number of contacts in a container.

- The `ADSGrouInADSGroup` and `ADSGroup` tables are monitored with respect to the number of contact memberships in a group and the number of groups in a container.

- The `ADSMachineInADSGroup` and `ADSMachine` tables are monitored with respect to the number of computer memberships in a group and the number of computers in a container.

> **NOTE:** The primary groups of Active Directory objects are not taken into account when membership per group is calculated.

Thresholds are set using configuration parameters. If the values in the parameters are exceeded, a warning message is sent to a defined mail address. The warning is only generated the first time the threshold is exceeded. This prevents warnings being send to the given address each time the threshold is exceeded, which could occur during synchronization for example.

> **Example: Monitoring group memberships**
>
> The threshold value for the number of objects in a `Members` group is limited to ten members (**TargetSystem | ADS | MemberShipRestriction | Group=10**). The `Members` group currently contains ten user accounts. When an 11th user account is added, a warning is generated and sent by email to the given address. When further user accounts are added, however, no more warning emails are sent.

Active Directory container structures

Containers are represented by a hierarchical tree structure. The containers that already exist can be loaded from the Active Directory environment into the One Identity Manager database by synchronization. System containers, which are entered into the One Identity Manager database are labeled correspondingly.

Related topics

Creating and editing Active Directory containers

Containers are loaded from Active Directory into the One Identity Manager database during synchronization. You can create new containers or edit existing ones.

To create a container

1. In the Manager, select the **Active Directory > Container** category.
2. Click ⬛ (**New**) in the result list.
3. Edit the container's main data.
4. Save the changes.

To edit a container

1. In the Manager, select the **Active Directory > 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

- Main data for Active Directory containers on page 141

Main data for Active Directory containers

Enter the following main data for a container.

Table 28: Main data for a container

Property	Description
Name	Container name.
Distinguished name	Container's distinguished name. The distinguished name for the new container is made up of the container name, the object class, the parent container, and the domain, and it cannot be modified.
Structural object class	Structural object class representing the object type.
Object class	List of classes defining the attributes for this object. The object classes listed are read in from the database during synchronization with the Active Directory environment. You can also enter object classes in to the input field. Other properties can be edited depending on the object class. **NOTE:** New containers should be set up as organizational units (`ORGANIZATIONALUNIT` object class). Organizational units (for example, branches, or departments) are used organize Active Directory objects, such as users, groups, and computers, in a logical way and therefore make administration of the objects easier. Organizational units can be managed in a hierarchical container structure.
Domain	Container domain
Parent container	Parent container for mapping a hierarchical container structure. The distinguished name is automatically updated using templates.
Account manager	Manager responsible for the container. ***To specify an account manager*** 1. Open the drop-down by clicking the arrow. 2. Select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.

Property	Description
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.
Street	Street or road.
Zip code	Zip code.
Location	Location.
State	State.
Country ID	The country ID.
Description	Text field for additional explanation.
Extended Function	Filter criteria for other representations of the container. Containers marked with this option are only shown in the Active Directory user account and computer manager when advanced mode console view is active.
Protected from accidental deletion	Specifies whether to protect the container against accidental deletion. If the option is set, the permissions for deleting the container are removed in Active Directory. The container cannot be deleted or moved.

Related topics

- Target system managers for Active Directory on page 208

Assigning extended properties to Active Directory 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, see Extended properties and property groups and Setting up extended properties.

To specify extended properties for a container

1. In the Manager, select the **Active Directory > 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.

Deleting Active Directory containers

Containers are deleted permanently from the One Identity Manager database and from Active Directory.

> NOTE: Containers with the **Protected from accidental deletion** option set, cannot be deleted.

To delete an Active Directory container

1. In the Manager, select the **Active Directory > Container** category.
2. Select the container in the result list.
3. Delete the container by using 🗑.
4. Confirm the security prompt with **Yes**.

Moving an Active Directory container

> NOTE:
>
> - Containers can only be moved within a domain.
> - Containers with the **Protected from accidental deletion** option set, cannot be deleted.

To move a container

1. In the Manager, select the **Active Directory > Container** category.
2. Select the container in the result list.
3. Select the **Change main data** task.
4. Select the **Change Active Directory container** task.
5. Confirm the security prompt with **Yes**.

6. Select the new container from the **Containers** drop-down on the **General** tab.

7. Save the changes.

Related topics

- Main data for Active Directory containers on page 141

Displaying the Active Directory 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 **Active Directory > Container** category.

2. Select the container in the result list.

3. Select the **Active Directory container overview** task.

Active Directory user accounts

You manage user account in One Identity Manager with Active Directory. A user account is a security principal in Active Directory. That means a user account can log in to the domain. A user account receives access to network resources through its group memberships and permissions.

Related topics

- Managing Active Directory user accounts and identities on page 57
- Supported user account types on page 84
- Login credentials for Active Directory user accounts on page 113
- Synchronizing single objects on page 49

Creating and editing Active Directory user accounts

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.

To create a user account

1. In the Manager, select the **Active Directory > 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.

To edit main data of a user account

1. In the Manager, select the **Active Directory > 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.

To manually assign a user account for an identity

1. In the Manager, select the **Identities > Identities** category.
2. Select the identity in the result list.
3. Select the **Assign Active Directory user accounts** task.
4. Assign a user account.
5. Save the changes.

Related topics

- Account definitions for Active Directory user accounts and Active Directory contacts on page 58

General main data of Active Directory user accounts

Table 29: Configuration parameters for setting up user accounts

Configuration parameter	Meaning
TargetSystem | ADS | Accounts | TransferJPegPhoto	Specifies whether changes to the identity's picture are published in existing user accounts. The picture is not part of default synchronization. It is only published when an identity's main data is changed.

Enter the following general main data.

Table 30: General 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 drop-down. The drop-down 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 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

Property	Description
	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 (`XOrigin=1`).
Manage level	Manage level of the user account. Select a manage level from the drop-down. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the drop-down.
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.
Middle name	User's middle 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

Property	Description
	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.
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.
Name	User account identifier. The identifier is made up of the user's 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.
Domain	Domain in which the user account is created.
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.
Primary group	User account's primary group. Synchronization with the Active Directory environment assigns the user account to the **Domain Users** group by default. Only groups that are assigned to the user account are available as primary groups.
Login name (pre Win2000)	Login name for the previous version of Active Directory. If you assigned an account definition, the login name (pre Win2000) is made up of the identity's central user account depending on the manage level of the user account.
User login name	User account login name. User login names that are formatted like this correspond to the User Principal Name (UPN) in Active Directory.
	If you have already established the container and entered the login name (pre Win2000), the user login name is created following the formatting rule as shown:
	`<login name (pre Win2000)>@<AD domain name>`
Email address	User account 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.
Additional email addresses	Other email addresses for the user account.
Account expiry	Account expiry date. Specifying an expiry data for the account has the

Property	Description
date	effect that the login for this user account is locked 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.
Structural object class	Structural object class representing the object type. Possible values: • `USER`: Default object class for user accounts. • `INETORGPERSON` : Object class used by other LDAP and X.500 directory services for mapping user accounts. • `POSIXACCOUNT`: Object class for user accounts with additional POSIX (Portable Operating System Interface) properties. • `MSDS-DELEGATEDMANAGEDSERVICEACCOUNT`: Object class for delegated Managed Service Accounts (dMSA).
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 Risk assessment.
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 drop-down.
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. • `Service identity`: Service account.
Privileged user account.	Specifies whether this is a privileged user account.

Property	Description
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.
Preferred user account	Preferred user account when an identity has several user accounts in Active Directory.
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 deactivated> option.
Account locked	Specifies whether the user account is locked. Depending on the configuration, the user account in the Active Directory environment is locked after multiple incorrect password attempts. You can lock the user account again in the Manager using the **Unlock user account** task. If the user account is linked to an identity, the user account is unlocked when a new central password is set for the identity. This behavior is controlled by the **TargetSystem	ADS	Accounts	UnlockByCentralPassword** configuration parameter. For more information, see Central password of an identity.
Protected from accidental deletion	Specifies whether to protect the user account against accidental deletion. If the option is set, the permissions for deleting the user account are removed in Active Directory. The user account cannot be deleted or moved.

Related topics

- Account definitions for Active Directory user accounts and Active Directory contacts on page 58
- Active Directory group inheritance based on categories on page 109
- Managing Active Directory user accounts and identities on page 57
- Supported user account types on page 84
- Disabling Active Directory user accounts on page 163
- Unlocking Active Directory user accounts on page 168
- Assigning identities automatically to Active Directory user accounts on page 78
- Prerequisites for indirect assignment of Active Directory groups on page 94

Password data for Active Directory user accounts

Enter the password data for the system user ID.

> **NOTE:** One Identity Manager password policies, global account policy settings for the Active Directory domain, and Active Directory account policies are all taken into account when verifying user passwords.

> **NOTE:** The **TargetSystem | ADS | Accounts | NotRequirePassword** configuration parameter specifies whether a password is required when creating new Active Directory user accounts in One Identity Manager. If the configuration parameter is not set, entry of a password that meets the defined password guidelines is requested when a new Active Directory user account is created. If the configuration parameter is set, it is not necessary to specify a password when creating new Active Directory user accounts. In the Designer, you can edit the configuration parameter as required.

Table 31: User account password data

Property	Description
Password	Password for the user account. The identity's central password can be mapped to the user account password. For more information, see Central password of an identity. 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.
Password confirmation	Reconfirm password.
Password last changed	Date of last password change. The date is read in from the Active Directory system and cannot be changed.
Password never expires	Specifies whether the password expires. This option is usually used for service accounts. It overwrites the maximum lifetime of a password and the **Change password at next logon** option.
Cannot change password	Specifies whether the password can be changed. This option is normally set for user accounts that are used by several users.
Change password at next login	Specifies whether the user must change their password the next time they log in.

Property	Description
	TIP: To enable this option every time new user accounts are created, set the **TargetSystem | ADS | Accounts | UserMustChangePassword** configuration parameter.
Save passwords with reversible encryption	Details for encrypting the password. By default, passwords that are saved in Active Directory are encrypted. When you use this option, passwords are saved in plain text and can be restored again.
SmartCard required to log on	Data required for logging in with a SmartCard. Set this option to save public and private keys, passwords, and other personal information for this Active Directory user account. For the user to be able to log in to the network, the user's computer must be equipped with a smart card reader and the user must have a personal identification number (PIN).
Account trusted for delegation purposes	Data required for delegation. Set this option so that a user can delegate the responsibility for administration and management of a partial domain to another Active Directory user account or another group.
Cannot delegate account	Data required for delegation. Set this option when this user account may not be assigned for delegation purposes from another user account.
Account uses DES encryption	Data required for encryption. Set this option if you would like to enable Data Encryption Standard (DES) support.
Kerberos preauthentication not required	Specifies whether Kerberos pre-authentication is required. Set this option when the user account uses a different implementation of the Kerberos protocol.

Related topics

Active Directory user account home directory and profile directory

Enter the data for the user's home and profile directories. When you enter a profile directory, a new user profile is created through One Identity Manager Service that is loaded over the network when the user logs on.

> **NOTE:** If the **QER | Person | User | ConnectHomeDir** configuration parameter is set, some of the following data for the home directory is formed automatically. In the Designer, you can set the configuration parameter as required.

Table 32: Main data for a user directory

Property	Description
Home server	Home server. You can select the home server depending on the number of home directories per home server that already exist (according to the database). If you assigned an account definition, the home server is determined from the current IT operating data for the assigned identity depending on the manage level.
Home share	The share that is stored under the user's home directory on the home server. Default is `HOMES`.
Home directory path	Name of the home directory for the user under the home share. By default, the login name (pre Windows 2000) is used to format the home directory path.
Home shared as	Home directory share. This share is formatted using the default home directory path.
Home drive	The drive to be connected when the user logs in. The default domain home drive is used.
Home directory	The user's home directory. The given home directory is automatically added and shared by the One Identity Manager Service.
Size home directory [MB]	Size of the home directory in MB. Find the size of the home directory by running the schedule supplied by default. In the Designer, configure and enable the **Load size of home folders for user accounts** schedule.
Maximum home storage space [MB]	Maximum size for the home directory on the home server in MB.
Profile server	Profile server. If you assigned an account definition, the profile server is determined from the current IT operating data for the assigned identity depending on the manage level.

Property	Description
Profile share	The share that is stored under the user's profile directory on the profile server. Default is **PROFILES**.
Profile shared as	Profile directory share.
Profile directory path	Name of the profile directory for the user under the profile share. By default, the login name (pre Windows 2000) is used to format the profile directory path.
Login script	Name of the login script. If the script is in a subdirectory of the login script path (normally `Winnt\Sysvol\domain\scripts`), you need enter the subdirectory as well. The given login script is run when the user logs in.

Related topics

- Preparing a home server and profile server for creating user directories on page 219

Login credentials for Active Directory user accounts

Enter the following login credentials.

Table 33: Credentials

Property	Description
Last login	Date of last login. The date is read in from the Active Directory system and cannot be changed manually.
Login workstation	Workstation on which the user can log in. A user can log in on all workstations by default.
	Select the button next to the input field to activate it and add workstations. Use the button to remove workstations from the list.
Login times	Times and days on which the user is allowed to be logged in. By default, login is permitted at all hours and every day of the week. If a user is logged in, the login is disconnected at the end of the valid login period.
	The calendar shows a 7-day week, each box represents one hour. The configured login times are shown in color, respectively. If a box is filled, login is allowed. If the box is empty, login is denied.
	To specify login times
	- Select a time period with the mouse or keyboard.
	- Select **Assign** to enable login in the selected period.

Property	Description
	• Select **Remove** to deny login in the selected period.
	• Select **Reverse** to invert the selected period.
	• Use the arrow keys to reset or repeat a selection.

Dial-in access using Remote Access Service (RAS) for Active Directory user accounts

> **NOTE:** Remote Access Service (RAS) properties are only synchronized and provisioned if the **Enable RAS properties** option is set.

Allocate remote dial-up permissions for the user account in the network and specify the callback option. The following data can be edited depending on the selected domain mode (mixed or native).

Enter the following main data:

Table 34: Remote access service

Property	Description
Dial-up permitted	Specifies whether the user may dial up the network. Permitted values are:
	• `Allow access`: This permits the user to dial up the network.
	• `Deny access`: This specifies that you deny the user the dial-in to the network.
	• `Control access using remote access policy`: This data specifies that access to the network is controlled over RAS guidelines. RAS guidelines are usually used to apply the same access permissions to several Active Directory user accounts.
No callback	The callback function is switched off by this option.
Set by caller	The server expects the user to input the number that they can be called back on.
Always callback	The server tries to call the user back over the given number.
Verifying caller ID	A predefined number with which the user should dial into the network.
Static IP address	A fixed IP address assigned to the user.
Static routes	Target network IP addresses, network addresses and metrics for

Property	Description
with IP address, network address and metric	dialing in over fixed routes.

Related topics

- Synchronizing an Active Directory environment on page 15

Terminal server connection data for Active Directory user accounts

> **NOTE:** Terminal server properties are only synchronized and provisioned if the **Enable terminal server properties** option is set.

Enter the following data for adding a user profile, which will be made available for logging the Active Directory user account on to a terminal server. A profile directory can be provided, which is available to the user to log on to a terminal server for terminal server sessions. A home directory can be added on the terminal server in the same way.

> **NOTE:** If the **QER | Person | User | ConnectHomeDir** configuration parameter is set, some of the following data for the home directory is formed automatically. In the Designer, you can set the configuration parameter as required.

Table 35: Main data for a terminal server

Property	Description
Login permitted on terminal server	Specifies whether terminal server login is allowed. Enable this option to allow a user to log on to a terminal server.
Use own configuration	Specifies whether a startup program can be defined. Enable this option to specify a program, which should be started when you log on to the terminal server and enter the program's command line and working directory. > **NOTE:** If this data is inherited from the client, disable this option.
Command line	Command line to start the program.
Working directory	Working directory of program to start.

Property	Description
Connect client drives at login	Specifies whether client drive connections should automatically be restored when logging into a terminal server.
Connect client printers at login	Specifies whether client printer connections should automatically be restored when logging on to a terminal server.
Client default printer	Specifies whether default printer connections should automatically be restored when logging into a terminal server.
Active session limit [min]	Maximum connection time in minutes. After the time is exceeded the connection to the terminal server is detached or ended.
End disconnected session [min]	Time period in minutes for maintaining a disconnected connection.
Idle session limit [min]	Maximum time without client activity before the connection is detached or ended.
Connect disconnected session from previous client	Specifies whether a disconnected session can be restored from an arbitrary client computer.
End session if connection is interrupted	Specifies whether a session should be returned to a disconnected state if the connection is interrupted.
Enable remote control	Specifies whether remote monitoring or remote control is enabled for this session.
Get permission of user	Specifies whether permission needs to be obtained for the user to monitor the session.
Display user session	Specifies whether to monitor the user session
Interact with session	Specifies whether the user to be monitored can input data into the session over the keyboard or mouse.
Profile server	Profile server. If you assigned an account definition, the profile server is determined from the current IT operating data for the assigned identity depending on the manage level.
Profile share	The share that is stored under the user's profile directory on the profile server. Default is **TPROFILES**.
Profile directory path	Name of the profile directory for the user under the profile share. By default, the login name (pre Windows 2000) is used to format the profile directory path.

Property	Description
Profile path	The full path to the user's profile directory.
Home server	Home server. If you assigned an account definition, the profile server is determined from the current IT operating data for the assigned identity depending on the manage level.
Home share	The share that is stored under the user's home directory on the home server. Default is `THOMES`.
Home directory path	Name of the home directory for the user under the home share. By default, the login name (pre Windows 2000) is used to format the home directory path.
Shared as	Home directory share. This share is formatted using the default home directory path.
Home drive	The drive to be connected when the user logs in. The default domain home drive is used.
Home directory	Home directory. The given home directory is automatically added and shared by the One Identity Manager Service.

Related topics

Extension data for Active Directory user accounts

Enter the user-defined Active Directory schema extensions for the user account.

Table 36: Extension data

Property	Description
Extensions data	Custom extension data in binary format.
Attribute extension 01 - attribute extension 15	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Further data for identifying Active Directory user accounts

Enter the following address data used by this user account for contacting the identity.

Table 37: Main data for identification

Property	Description
Office	Office. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Street	Street or road. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Mailbox	Mailbox. 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.
City	City. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. Locations can be automatically generated and identities assigned based on the town.
State	State. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
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.
Department	Identity's department If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. Departments can be automatically generated and identities assigned based on the department data.
Job description	Job description. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Identity's ID.	Identity's unique marker, for example their ID.
Personnel number	Number for identifying the identity, in addition to their ID.
Account manager	Manager responsible for the user account. ***To specify an account manager*** 1. Open the drop-down by clicking the arrow. 2. Select the table that maps the account manager. 3. In the **Account manager** menu, select the manager.

4. Click **OK**.

Related topics

- Automatic creation of departments and locations based on user account information on page 91

Contact information for Active Directory user accounts

Enter the data used by this user account for contacting the identity by telephone.

Table 38: Contact data

Property	Description
Phone	Telephone 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.
Fax	Fax 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.
Website	Website.
IP telephone number	IP telephone number.
Comment	Text field for additional explanation.

POSIX properties for Active Directory user accounts

User accounts with the `POSIXACCOUNT` object class also have the following properties mapped.

Table 39: POSIX properties

Property	Description
GID number	ID of the primary user group in the domain.
Gecos	Additional information, such as full name or phone numbers.
Login shell	Name and path of the login shell.
Unix home directory	Full path of the Unix home directory.
UID Posix	Unique ID within the domain.
UID number	Unique ID in the Unix system.

Related topics

- Supporting POSIX extensions on page 37

Assigning Active Directory account policies to Active Directory user accounts

For domains from the `Windows Server 2008 R2` functional level and above, it is possible to define additional password policies in addition to the default password policies. This allows individual users and groups to be subjected to stricter account policies as intended for global groups.

To specify account policies for a user account

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign account policies** task.
4. In the **Add assignments** pane, assign account policies.

   > **TIP:** In the **Remove assignments** pane, you can remove account policy assignments.

> *To remove an assignment*
> - Select the account policy and double-click ⊘.

5. Save the changes.

Related topics

Assigning secretaries to Active Directory user accounts

Assign a secretary to a user account. The secretary is displayed in the email recipient's properties in Microsoft Outlook.

To assign a secretary to a user account

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign secretary** task.
4. Select the table which contains the user from the drop-down **Table** at the top of the form. You have the following options:
   - Active Directory user accounts
   - Active Directory contacts
   - Active Directory groups
5. In the **Add assignments** pane, assign secretaries.

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

6. Save the changes.

Assigning extended properties to Active Directory 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, see Extended properties and property groups and Setting up extended properties.

To specify extended properties for a user account

1. In the Manager, select the **Active Directory > 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 Active Directory 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 `ADSAccount.AccountDisabled` column.

> **NOTE:** To move user accounts to a special container when they are being disabled, maintain the **Container for disabled user accounts** (`ADSAccount.UID_ADSContainerDisabled`) in the IT operating data.
>
> If a user account that is managed by an account definition is disabled, the container is determined using the IT operating data and the user account is moved to that container.

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 **Active Directory > 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.

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 **Active Directory > 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, see Deactivating and deleting identities and user accounts.

Related topics

- Account definitions for Active Directory user accounts and Active Directory contacts on page 58
- Creating manage levels on page 63
- Creating mapping rules for IT operating data on page 65
- Deleting and restoring Active Directory user accounts on page 165

Deleting and restoring Active Directory user accounts

> **NOTE:**
> - Containers with the **Protected from accidental deletion** option set, cannot be deleted.
> - As long as an account definition still applies to an identity, 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.
> - When you delete a user account, an Active Directory SID entry is created in One Identity Manager.
> - When you configure the synchronization project you define whether, when adding or restoring an Active Directory object in One Identity Manager, the system should first check if the object is in the Active Directory recycling bin and can be restored.

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 prompt the user account is marked for deletion in One Identity Manager.

To delete a user account

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Click (**Delete**) in the result list.
4. Confirm the security prompt with **Yes**.

Deferred deletion is taken into account if a user account is being deleted. 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. You can reenable the user accounts up until deferred deletion runs.

If the **QER | Person | User | DeleteOptions | ReapplyTemplatesOnRestore** is set, the template is applied again when reenabling a user account marked for deletion that is managed through an account definition. This means that properties dependent on the IT operating data are automatically recreated according to the current configuration.

To restore a user account

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.

Related topics

Procedure for deleting Active Directory user accounts in One Identity Manager

Objects in Active Directory such as user accounts, are issued with a unique identification number that is also linked to permissions.

For domains with a functional level lower than `Windows Server 2008 R2`, the ID and the associated permissions are irreversibly lost when the user accounts are deleted in Active Directory. This makes it difficult to restore user accounts.

User accounts in domains with a `Windows Server 2008 R2` functional level or higher can be deleted using the recycling bin. This moves the users to the recycle bin and from where they can be restored within a defined period without loss of IDs or permissions.

> **NOTE:** When you configure the synchronization project you define whether, when adding or restoring an Active Directory object in One Identity Manager, the system should first check if the object is in the Active Directory recycling bin and can be restored.

One Identity Manager uses various methods for deleting user accounts.

Deleting without an Active Directory recycle bin

This method can be applied to all domains that:

- Have a functional level lower than `Windows Server 2008 R2` and therefore no recycling bin is available.

  - OR -

- Have a functional level of `Windows Server 2008 R2` or higher but the recycling bin is not activated.

After you have confirmed the security prompt the user account is marked for deletion in One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the Active Directory depending on the deferred deletion setting.

Deleting with the Active Directory recycle bin

This method is used for domains with a `Windows Server 2008 R2` functional level or higher, in which the recycling bin is activated.

After you have confirmed the security prompt the user account is marked for deletion in One Identity Manager. The user account is locked in One Identity Manager and is permanently deleted from the One Identity Manager database once the deferred deletion time has expired. In Active Directory, the user account is moved into the recycling bin and is finally deleted from Active Directory once the deferred deletion time has expired. The retention time for objects in the recycling bin is entered in the domain in the **Retention period** property.

Related topics

- Creating a synchronization project for initial synchronization of an Active Directory domain on page 24
- Active Directory specific main data for Active Directory domains on page 131
- Specifying deferred deletion for Active Directory user accounts and Active Directory contacts on page 92

Handling of user directories when deleting Active Directory user accounts

When a user accounts is deleted the configuration parameter defining handling of user directories is taken into account. In the Designer, check the configuration parameters and modify them as necessary to suit your requirements.

Table 40: Configuration parameters for deleting user accounts

Configuration parameter	Effect when set
QER | Person | User | DeleteOptions	This configuration parameter to control behavior when users are deleted
QER | Person | User | DeleteOptions | FolderAnonymPre	If the delete options specify that a directory or a share should not be deleted, it is renamed and the given prefix is applied.
QER | Person | User | DeleteOptions | HomeDir	Deletes the user home directory.
QER | Person | User | DeleteOptions | HomeShare	Deletes the user home share.
QER | Person | User | DeleteOptions | ProfileDir	Deletes the user profile directory.
QER | Person | User |	Deletes the user profile share.

Configuration parameter	Effect when set
DeleteOptions | ProfileShare	
QER | Person | User | DeleteOptions | TerminalHomeDir	Deletes the user terminal home directory.
QER | Person | User | DeleteOptions | TerminalHomeShare	Deletes the user terminal home share.
QER | Person | User | DeleteOptions | TerminalProfileDir	Deletes the user terminal profile directory.
QER | Person | User | DeleteOptions | TerminalProfileShare	Delete the user terminal profile share.

Unlocking Active Directory user accounts

If the password is entered incorrectly several times (configuration dependent), the user account is locked in Active Directory.

If the user account is linked to an identity, the user account is unlocked when a new central password is set for the identity. This behavior is controlled by the **TargetSystem | ADS | Accounts | UnlockByCentralPassword** configuration parameter. For more information, see Central password of an identity.

To unlock a user account manually

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **Unlock user account** task.
5. Confirm the security prompt with **OK**.

   The user account is unlocked by the One Identity Manager Service.

Related topics

- Creating and editing Active Directory user accounts on page 145

Moving Active Directory user accounts

> **NOTE:**
> - User accounts with the **Protected from accidental deletion** option set, cannot be deleted.
> - To move a user account to another domain, make sure that the user account is assigned to the primary group only. You should remove all other group memberships before you move them. If you move a user account to another container within a domain, you must not remove the group memberships.
> - If you move a user account with an account definition to another domain, you must also remove the account definition from the user account.

To move a user account to another container

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **Change Active Directory container** task.
5. Confirm the security prompt with **Yes**.
6. Select the new container from the **Containers** drop-down on the **General** tab.
7. Save the changes.

To move a user account to another domain

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **Change Active Directory domain** task.
5. In the **Move to other domain** dialog, select a **Target domain** and a **Target container** and click **Ok**.
6. Confirm the security prompt with **OK**.

Related topics

- General main data of Active Directory user accounts on page 146

Displaying the Active Directory 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 **Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Active Directory user account overview** task.

Displaying Microsoft Entra ID user accounts for Active Directory user accounts

> **NOTE:** This function is only available if the Microsoft Entra ID Module is installed.

You can display the Microsoft Entra ID user account for an Active Directory user account on the overview form.

To display the Microsoft Entra ID user account for an Active Directory user account

1. In the Manager, select the **Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Active Directory user account overview** task.

   The **Microsoft Entra ID user account** form element shows which user account is linked to it.

For more information, see Microsoft Entra ID user accounts.

Active Directory contacts

A contact is a non-security principal. That means a contact cannot log into a domain. For example, a contact represents a user out the organization and is mainly used for distribution groups or email purposes.

Related topics

- Managing Active Directory user accounts and identities on page 57
- Managing memberships in Active Directory groups on page 93
- Synchronizing single objects on page 49

Creating and editing Active Directory contacts

A contact can be connected to an identity in One Identity Manager. You can also manage contacts separately from identities.

> **NOTE:**
>
> - It is recommended to use account definitions to set up contacts for company identities. If an account definition is used to set up a contact, some of the main data described in the following is composed of the identity's main data using templates. The amount of data, in this case, is based on the default manage level of the account definitions. The templates supplied should be customized as required.
> - If identities receive their contacts through account definitions, the identities must have a central user account and obtain their IT operating data through assignment to a primary department, primary location or a primary cost center.

To create a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Click (**New**) in the result list.
3. Edit the contact's main data.
4. Save the changes.

To edit a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list and run the **Change main data** task.
3. Edit the contact's main data.
4. Save the changes.

To manually assign or create a contact for an identity

1. In the Manager, select the **Identities > Identities** category.
2. Select the identity from the result list and run the **Assign Active Directory contacts** task.

3. Assign a contact.

4. Save the changes.

Related topics

- Account definitions for Active Directory user accounts and Active Directory contacts on page 58

General main data for Active Directory contacts

Enter the following general main data.

Table 41: General main data

Property	Description
Identity	Identity that uses the contact.
	- An identity is already entered if the contact was generated by an account definition.
	- If you are using automatic identity assignment, when you save the contact, the system searches for an associated identity and adds it to the contact.
	- If you create the contact manually, you can select the identity from the drop-down.
	The drop-down 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, the contact might be locked or deleted depending on the configuration.
	NOTE: To enable working with identity types, the identities and the contacts also need identity types. You can only link contacts that have an identity type assigned to them, to identities of the same identity type.
No link to an identity required	Specifies whether the contact is intentionally not assigned an identity. The option is automatically set if a contact 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 contact does not need to be linked with an identity (for example, if

Property	Description
	several identities use the contact).
	If attestation approves these contacts, these contacts will not be submitted for attestation in the future. In the Web Portal, contact 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 contact. Possible values: • `By administrator`: The option was set manually by the administrator. • `By attestation`: The contact was attested. • `By exclusion criterion`: The contact is not associated with an identity due to an exclusion criterion. For example, the contact is included in the exclude list for automatic identity assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the contact was created. Use the account definition to automatically populate contact main data and to specify a manage level for the contact. One Identity Manager finds the IT operating data of the assigned identity and uses it to populate the corresponding fields in the contact. **NOTE:** The account definition cannot be changed once the contact has been saved. To create the contact manually through an account definition, enter an identity in the **Identity** field. You can select all the account definitions assigned to this identity and through which no contact has been created for this identity.
Manage level	Contact's manage level. Select a manage level from the drop-down. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the drop-down.
First name	The contact'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 contact'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 contact's initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Title	Contact's academic title. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.

Property	Description
Display name	The contact's display name. The display name is made up of the contact's first and last names.
Structural object class	Structural object class representing the object type. Possible values: • **CONTACT**: Default object class for contacts. • **POSIXACCOUNT**: Object class for contacts with additional POSIX (Portable Operating System Interface) properties.
Name	The contact's identifier. The identifier is made up of the contact's first and last names.
Distinguished name	Contact's distinguished name. The distinguished name is formatted from the contact's identifier and the container and cannot be changed.
Domain	Domain in which to create the contact.
Container	Container in which to create the contact. 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. The distinguished name for the contact is determined by a template when the container is selected.
Email address	Contact's 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.
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 Risk assessment.
Category	Category for the contact to inherit groups. Groups and be selectively inherited by contacts. To do this, the groups and contacts are divided into categories. Select one or more categories from the drop-down.
Description	Text field for additional explanation.
Identity type	Contact's type of identity. **NOTE:** To enable working with identity types, the identities and the user accounts also need identity types. You can only link user accounts that have an identity type assigned to them, to identities of the same identity type.
Groups can be inherited	Specifies whether the identity's groups are inherited. If this option is set, contacts inherit groups through hierarchical roles. If you add an identity with a contact to an apartment, for example, and you have assigned groups to this department, the contact inherits the

Property	Description
	groups.
Protected from accidental deletion	Specifies whether to protect the contact against accidental deletion. If the option is set, the permissions for deleting the contact are removed in Active Directory. The contact cannot be deleted or moved.

Related topics

- Account definitions for Active Directory user accounts and Active Directory contacts on page 58
- Supported user account types on page 84
- Managing Active Directory user accounts and identities on page 57
- Active Directory group inheritance based on categories on page 109

Contact data for Active Directory contacts

Enter the data used by this contact for contacting the identity by telephone.

Table 42: Contact data

Property	Description
Phone	Telephone number.
Phone private	Private telephone number.
Fax	Fax number.
Mobile phone	Mobile number.
Pager	Pager number.
Website	Website.
IP telephone number	IP telephone number.
Comment	Text field for additional explanation.

Further data for identifying Active Directory contact

Enter the following address data used by this contact for contacting the identity.

Table 43: Main data for identification

Property	Description
Office	Office.
Street	Street or road.
Mailbox	Mailbox.
Zip code	Zip code.
City	City.
State	State.
Country ID	The country ID.
Company	Identity's company.
Department	Identity's department
Job description	Job description.
Identity's ID.	Identity's unique marker, for example their ID.
Account manager	Manager responsible for the contact. ***To specify an account manager*** 1. Open the drop-down by clicking the arrow. 2. Select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.

Extension data for Active Directory contacts

Enter the custom Active Directory schema extensions for the contact.

Table 44: Extensions data

Property	Description
Extensions data	Custom extension data in binary format.

Property	Description
Attribute extension 01 - attribute extension 15	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

POSIX properties for Active Directory contacts

Contacts with the `POSIXACCOUNT` object class also have the following properties mapped.

Table 45: POSIX properties

Property	Description
GID number	ID of the primary user group in the domain.
Gecos	Additional information, such as full name or phone numbers.
Login shell	Name and path of the login shell.
Unix home directory	Full path of the Unix home directory.
UID Posix	Unique ID within the domain.
UID number	Unique ID in the Unix system.

Related topics

Assigning secretaries to Active Directory contacts

Assign a secretary to a contact. The secretary is displayed in the email recipient's properties in Microsoft Outlook.

To assign a secretary to a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list.
3. Select the **Assign secretary** task.

4. Select the table which contains the user from the **Table** drop-down at the top of the form. You have the following options:

- Active Directory user accounts
- Active Directory contacts
- Active Directory groups

5. In the **Add assignments** pane, assign secretaries.

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

6. Save the changes.

Assigning extended properties to Active Directory contacts

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, see Extended properties and property groups and Setting up extended properties.

To assign extended properties for a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

5. Save the changes.

Deleting and restoring Active Directory contacts

One Identity Manager uses various methods to delete contacts. For more information, see Procedure for deleting Active Directory user accounts in One Identity Manager on page 166.

> **NOTE:**
>
> - Contacts with the **Protected from accidental deletion** option set, cannot be deleted.
> - As long as an account definition for an identity is valid, the identity retains the contact that was created by it. If the account definition assignment is removed, the contact created through this account definition, is deleted.

In the Manager, delete contacts that were not created using an account definition, via the result list or the menu bar. After you have confirmed the security prompt the contact is marked for deletion in One Identity Manager.

To delete a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list.
3. Click (**Delete**) in the result list.
4. Confirm the security prompt with **Yes**.

Deferred deletion is taken into account if a contact is being deleted. You can use deferred deletion to specify how long the contacts remain in the database after deletion is triggered before they are finally removed. You can reenable the contacts up until deferred deletion runs.

If the **QER | Person | User | DeleteOptions | ReapplyTemplatesOnRestore** is set, the template is applied again when reenabling a contact marked for deletion that is managed through an account definition. This means that properties dependent on the IT operating data are automatically recreated according to the current configuration.

To restore a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list.
3. Click in the result list.

Related topics

- General main data for Active Directory contacts on page 172
- Specifying deferred deletion for Active Directory user accounts and Active Directory contacts on page 92

Moving Active Directory contacts

> **NOTE:**
> - Contacts can only be moved within a domain.
> - Contacts with the **Protected from accidental deletion** option set, cannot be deleted.

To move a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list.
3. Select the **Change main data** task.
4. Select the **Change Active Directory container** task.
5. Confirm the security prompt with **Yes**.
6. Select the new container from the **Containers** drop-down on the **General** tab.
7. Save the changes.

Related topics

- General main data for Active Directory contacts on page 172

Displaying the Active Directory contact overview

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

To obtain an overview of a contact

1. In the Manager, select the **Active Directory > Contacts** category.
2. Select the contact in the result list.
3. Select the **Active Directory contact overview** task.

Active Directory groups

Read the documentation for your Active Directory for an explanation of group concepts under Windows Server.

In Active Directory, contacts, computers, and groups can be collected into groups for which the access to resources can be regulated not only within a domain but across domains.

We distinguish between two group types:

- Security groups

  Permissions are granted through security groups. User accounts, computers, and other groups are added to security groups and which makes administration easier. Security groups are also used for email distribution groups.

- Distribution groups

  Distribution groups can be used as mail-enabled distribution groups. Distribution groups do not have any security.

In addition, a group area is defined for each group type. Permitted group types are:

- Universal

  Groups within this scope are described as universal groups. Universal groups can be used to make cross-domain permissions available. Universal group members can be user accounts and groups from all domains in one domain structure.

- Local domain

  Groups in this scope are described as groups of the local domain. Local groups are used when permissions are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.

- Global

  Groups within this scope are described as global groups. Global groups can be used to make cross-domain permissions available. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.

Related topics

- Managing memberships in Active Directory groups on page 93
- Validity of group memberships on page 185
- Synchronizing single objects on page 49

Creating and editing Active Directory groups

Groups are loaded into One Identity Manager by synchronization. You can set up new groups or edit existing groups.

To create a group

1. In the Manager, select the **Active Directory > Groups** category.
2. Click (**New**) in the result list.

3. On the main data form, edit the main data of the group.

4. Save the changes.

To edit group main data

1. In the Manager, select the **Active Directory > 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.

General main data of Active Directory groups

Enter the following general main data.

Table 46: General main data

Property	Description
Name	Name of the group. The group identifier is used to form the group name for previous **group name (pre Win2000)** versions.
Domain	Domain in which to create the group.
Container	Container in which to create the group.
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.
Display name	Name for displaying the group in the user interface of One Identity Manager tools.
Group name (pre Win2000)	Name of the group for the previous versions. The group name is taken from the group identifier.
Structural object class	Structural object class representing the object type. Possible values: • `GROUP`: Default object class for groups. • `POSIXGROUP`: Object class for groups with additional POSIX (Portable Operating System Interface) properties.
Object class	List of classes defining the attributes for this object. The object classes listed are read in from the database during synchronization with the Active Directory environment. However, in the input field, you can add object classes and auxiliary classes that are used by other LDAP and X.500 directory services.

Property	Description
Account manager	Manager responsible for the group. ***To specify an account manager*** 1. Open the drop-down by clicking the arrow. 2. Select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.
Group manager can update members list.	Specifies whether the account manager can change the memberships for this group.
Protected from accidental deletion	Specifies whether to protect the group against accidental deletion. If the option is set, the permissions for deleting the group are removed in Active Directory. The group cannot be deleted or moved.
Email address	Group's email address
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, see Risk assessment.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts and contacts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the drop-down.
Description	Text field for additional explanation.
Remark	Text field for additional explanation. Abbreviations for combinations of group type and group area are added in the comment and should not be changed.
Security group	Group type. Authorizations are issued through security groups. User accounts, computers, and other groups are added to security groups and which makes administration easier. Security groups are also used for email distribution groups.
Distribution group	Group type. Distribution groups can be used as email distribution groups. Distribution groups do not have any security.
Universal group	Group scope. Universal groups can be used to make cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
Local group	Group scope. Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user

Property	Description
	accounts, computers, or groups in any domain.
Global group	Group scope. Global groups can be used to make cross-domain authorizations available. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.
IT Shop	Specifies whether the group can 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. 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.
Service item	Service item data for requesting the group through the IT Shop.
Read-only memberships	Specifies whether memberships are read-only. For example, dynamic groups. The memberships are regulated by the target system. Manual changes to memberships in One Identity Manager are not permitted.

Related topics

- Active Directory group inheritance based on categories on page 109

Extension data for Active Directory groups

Enter the custom Active Directory schema extensions for the group.

Table 47: Extension data

Property	Description
Attribute extension 01 - attribute extension 15	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

POSIX properties for Active Directory groups

The following additional properties are mapped for groups with the `POSIXGROUP` object class.

Table 48: POSIX properties

Property	Description
GID number	Group ID in the domain.

Related topics

- Supporting POSIX extensions on page 37

Validity of group memberships

There are different assignments to groups possible depending on the construction of the domain structure and the domain trusts. For more information about permitted group memberships, see the documentation for your Windows Server.

Ensure the following if you want to map group memberships using forests:

- The trusted domains are known.
- The name of the forest is entered in the domain.

In the following tables, the groups, user accounts, contacts, and computers permitted in One Identity Manager listed in groups.

Legend for the tables:

- G = Global
- U = Universal
- L = Local

Table 49: Group memberships permitted within a domain

Target Group		Member in target group						User account	Contact	Compute-r
		Group								
		Distribution			Security					
		G	U	L	G	U	L			
Distri-bution	Global	x			x			x	x	x
	Universal	x	x		x	x		x	x	x
	Local	x	x	x	x	x	x	x	x	x
Security	Global	x			x			x	x	x
	Universal	x	x		x	x		x	x	x
	Local	x	x	x	x	x	x	x	x	x

Table 50: Group memberships permitted within a hierarchical domain structure

Target Group		Member in target group						User account	Contact	Compute-r
		Group								
		Distribution			Security					
		G	U	L	G	U	L			
Distri-bution	Global								x	
	Universal	x	x		x	x		x	x	x
	Local	x	x		x	x		x	x	x
Security	Global									
	Universal	x	x		x	x		x	x	x
	Local	x	x		x	x		x	x	x

Table 51: Group memberships permitted within a forest

Target Group		Member in target group						User account	Contact	Compute-r
		Group								
		Distribution			Security					
		G	U	L	G	U	L			
Distri-bution	Global									
	Universal									
	Local	x	x		x	x		x		x
Security	Global									
	Universal									
	Local	x	x		x	x		x		x

Table 52: Group memberships permitted between forests

Target Group		Member in target group						User account	Contact	Compute-r
		Group								
		Distribution			Security					
		G	U	L	G	U	L			
Distri-bution	Global									
	Universal									
	Local	x	x		x	x		x		x
Security	Global									
	Universal									
	Local	x	x		x	x		x		x

Related topics

- Entering and testing trusted Active Directory domains on page 134
- Active Directory specific main data for Active Directory domains on page 131

Adding Active Directory groups to Active Directory 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 **Active Directory > 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 **Active Directory > 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.

Related topics

- Validity of group memberships on page 185

Assigning Active Directory account policies to Active Directory groups

For domains from the functional level `Windows Server 2008 R2` and above, it is possible to define additional password policies in addition to the default password policies. This allows individual users and groups to be subjected to stricter account policies as intended for global groups.

To specify account policies for a group

1. In the Manager, select the **Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Assign account policies** task.

4. In the **Add assignments** pane, assign account policies.

   > **TIP:** In the **Remove assignments** pane, you can remove account policy assignments.
   >
   > ### To remove an assignment
   >
   > - Select the account policy and double-click ⊘.

5. Save the changes.

Related topics

Assigning secretaries to Active Directory groups

Assign a secretary to the group. The secretary is displayed in the email recipient's properties in Microsoft Outlook.

To assign a secretary to a group

1. In the Manager, select the **Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Assign secretaries** task.
4. Select the table which contains the user from the **Table** drop-down at the top of the form. You have the following options:
   - Active Directory user accounts
   - Active Directory contacts
   - Active Directory groups
5. In the **Add assignments** pane, assign secretaries.

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

6. Save the changes.

Assigning extended properties to Active Directory 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, see Extended properties and property groups and Setting up extended properties.

To specify extended properties for a group

1. In the Manager, select the **Active Directory > 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.

Deleting Active Directory groups

Groups are deleted permanently from the One Identity Manager database and from Active Directory. When a group is deleted, an entry is created in One Identity Manager for the Active Directory SID.

> **NOTE:**
>
> - Groups with the **Protected from accidental deletion** option set, cannot be deleted.
> - When a group is deleted, an entry is created in One Identity Manager for the Active Directory SID.

To delete an Active Directory group

1. In the Manager, select the **Active Directory > Groups** category.

2. Select the group in the result list.

3. Click (**Delete**) in the result list.

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

Related topics

- General main data of Active Directory groups on page 182
- Active Directory security IDs on page 195

Moving Active Directory groups

> **NOTE:**
>
> - Groups can only be moved within a domain.
> - Groups with the **Protected from accidental deletion** option set, cannot be deleted.

To move a group

1. In the Manager, select the **Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. Select the **Change Active Directory container** task.
5. Confirm the security prompt with **Yes**.
6. Select the new container from the **Containers** drop-down on the **General** tab.
7. Save the changes.

Related topics

- General main data of Active Directory groups on page 182

Displaying the Active Directory 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 **Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Active Directory group overview** task.

   The **Microsoft Entra ID group** form element shows which group is linked to it.

Displaying Microsoft Entra ID groups for Active Directory groups

NOTE: This function is only available if the Microsoft Entra ID Module is installed.

The Microsoft Entra ID group linked to an Active Directory group is displayed on the overview form.

To display the Microsoft Entra ID group for an Active Directory group

1. In the Manager, select the **Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Active Directory group overview** task.

    The **Microsoft Entra ID group** form element shows which group is linked to it.

For more information, see Microsoft Entra ID groups.

Active Directory computers

Computers and servers are loaded into One Identity Manager by synchronization. You can create new computers or edit existing ones.

To create a computer

1. In the Manager, select the **Active Directory > Computers** category.

2. Click ▣ (**New**) in the result list.

3. Edit the computer's main data.

4. Save the changes.

To edit computer main data

1. In the Manager, select the **Active Directory > Computers** category.

2. In the result list, select the computer and run the **Change main data** task.

3. Edit the computer's main data.

4. Save the changes.

Related topics

- Managing memberships in Active Directory groups on page 93
- Synchronizing single objects on page 49

Main data for Active Directory computers

Enter the following data for a computer.

Table 53: Computer main data

Property	Description
Device	The computer is connected to this device. Specify a new device using the ![icon] button next to the drop-down. For more information, see Managing devices and workdesks.
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.
Primary group	Computer's primary group. Then, only groups that are already assigned to the computer can be selected.
Account manager	Manager responsible for the computer. **To specify an account manager** 1. Open the drop-down by clicking the arrow. 2. Select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.
Computer name (pre Win2000)	Pre-Windows 2000 computer name. Name of the computer for the previous version of Windows 2000.
DNS host name	DNS name of the computer.
Function	Function of the computer in the network. The functions `Workstation`, `Server` and `Domain Controller` are available for selection.
Operating system	Operating system identifier.
Operating system version	Version number of the operating system.
Service pack operating system	Service pack identifier.

Property	Description
Hotfix operating system	Hotfix identifier.
Protected from accidental deletion	Specifies whether to protect the computer against accidental deletion. If the option is set, the permissions for deleting the computer are removed in Active Directory. The computer cannot be deleted or moved.

Performing computer diagnostics

You can use the following tasks to run a diagnosis if the computer can be found on the network and if you have sufficient access permissions.

To run diagnostics for a computer

1. In the Manager, select the **Active Directory > Computers** category.
2. Select the computer and run the required diagnosis task from the task view.
    *   **Diagnosis - browse**: This opens a Windows Explorer window. All shares for the selected computer are shown.
    *   **Diagnosis - Windows diagnosis**: This opens the computer's system information (`winmsd.exe` or `msinfo32.exe`).
    *   **Windows computer administration**: This opens the Microsoft Management console for computer administration for the selected computer. For example, here you can see the result log or the local user administration.

Moving an Active Directory computer

> **NOTE:**
>
> *   Computers can only be moved within a domain.
> *   Computers with the **Protected from accidental deletion** option set, cannot be deleted.

To move a computer

1. In the Manager, select the **Active Directory > Computers** category.
2. Select the computer in the result list.
3. Select the **Change main data** task.
4. Select the **Change Active Directory container** task.

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

6. Select the new container from the **Containers** drop-down on the **General** tab.

7. Save the changes.

Related topics

- Main data for Active Directory computers on page 193

Displaying the Active Directory 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 **Active Directory > Computers** category.

2. Select the computer in the result list.

3. Select the **Active Directory computer overview** task.

Active Directory security IDs

The security ID (SID) is used in One Identity Manager to identify user accounts and groups from other domains. This is required, amongst other things, for synchronizing group memberships of two domains. Furthermore, the SID is used to find access permission at file system level.

Example: Group membership assignment by SIDs

Domain A is synchronized with One Identity Manager. Domain B is not synchronized at first. The domains are in a trust relationship. There are user accounts of domain A and domain B in groups of domain A.

Group memberships are identified when domain A is synchronized. User accounts from domain A are assigned based on their identifier. The SIDs are found for user accounts from domain B and entered in One Identity Manager.

If Active Directory domain B is synchronized at later, the user accounts are identified based on their SIDs and the user accounts are assigned directly to the groups in domain B. The SID is removed from One Identity Manager database.

To display security IDs

- In the Manager, select the **Active Directory > Active Directory SIDs** category.

> **NOTE:** When you delete an Active Directory object, a SID entry is created in One Identity Manager.

Active Directory printers

All shared printers of a domain are loaded into One Identity Manager during synchronization and cannot be edited.

To display a printer

1. In the Manager, select the **Active Directory > Printer** category.
2. In the result list, select a printer then select the **Change main data** task.

The following main data is displayed:

Table 54: Printer main data

Property	Description
Printer name	Name of the printer.
Driver	Printer driver identifier.
Active Directory computers	Computer or server to which the printer is connected.
Full server name	Full name of the server to which the printer is connected.
Server	Server's short name.
Port	Printer connection.
UNC name	Universal Naming Convention (UNC) address of the printer.
Location description	Text field for additional explanation.
Description	Text field for additional explanation.
Duplex	Specifies whether double sided printing is supported.
Color	Specifies whether color is supported.
Supports sorter	Specifies whether the printer supports sorting.
Pages per minute	Printer speed in page per minute.
Max. resolution	Maximum printer resolution in dpi.

Property	Description
[dpi]	
Max. horizontal resolution	Maximum printer resolution along the X-axis (width).
Max. vertical resolution	Maximum printer resolution along the Y-axis (height).
Spare field no. 01 ... Spare field no. 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Related topics

- Synchronizing single objects on page 49

Active Directory sites

Sites are a group of computers based on networking information. In Active Directory, sites data is used to control replication between domain controllers.

The information about Active Directory sites is loaded into One Identity Manager during synchronization and cannot be edited.

To display site information

1. In the Manager, select the **Active Directory > Sites** category.
2. Select the site in the result list.
3. To display a site's server, select the **Location overview** task.
4. To display a site's main data, select the **Change main data** task.

The following main data is displayed:

Table 55: Site main data

Property	Description
Name	Site name.
Canonical name	The site's canonical name
Description	Text field for additional explanation.
Location description	Text field for additional explanation.
Forest	The name of the Forest to which this site belongs.
Subnets	IP address range at this site.

Reports about Active Directory 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 Active Directory.

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

Table 56: 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 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.

Report	Published for	Description
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. For more information, see Analyzing role memberships and identity assignments.
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 entitlements	Domain	This report contains all user accounts with an above average number of system 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

Report	Published for	Description
		(**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 57: Additional reports for the target system

Report	Description
Active Directory user account and group administration	This report contains a summary of user account and group distribution in all domains. In the Manager, find the report in the **My One Identity Manager** category. In the Manager web application, find the report in the **Favorites** section.
Data quality summary for Active Directory user accounts	This report contains different evaluations of user account data quality in all domains. In the Manager, find the report in the **My One Identity Manager** category. In the Manager web application, find the report in the **Favorites** section.

Related topics

- Overview of all assignments on page 111

Handling of Active Directory objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

For more information, see Working with the 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.

  For more information, see Attestation and recertification.

- 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.

  For more information, see Compliance rules and identity audit.

  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.

  For more information, see Company policies in One Identity Manager.

- 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.

  For more information, see Risk assessment.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the identities, user accounts, and their entitlements and risks.

Related topics

Default solutions for requesting Active Directory groups and group memberships

In One Identity Manager, standard products and default approval workflows are provided for requesting Active Directory groups and membership in these groups through the IT Shop. Permissions in this target system are therefore issued by defined approval processes. In the Web Portal, product owners and target system managers can edit properties of these groups and request changes.

For more information, see Requests for Active Directory groups.

Adding Active Directory groups

By requesting this standard product, you can add new security groups or distribution groups in the Active Directory. The requester provides information about the name, container, and domain, if known, of the request. Based on this information, the target system manager specifies the container in which the group will be added and grants approval for the request. The group is created in One Identity Manager and published to the target system.

Prerequisite

- Identities are assigned to the **Target systems | Active Directory** application role.

If the **QER | ITShop | AutoPublish | ADSGroup** configuration parameter is set, the group is added to the IT Shop and the assigned to the shelf **Identity & Access Lifecycle | Active Directory groups**. The group is assigned to the service category **Security group** or **Distribution group** respectively.

Table 58: Default objects for requesting an Active Directory group

Products	Creating an Active Directory security group
	Creating an Active Directory distribution group
Service category	Active Directory groups
Shelf	Identity & Access Lifecycle > Group Lifecycle
Approval policies/approval workflows	Approval of Active Directory group create requests

Related topics

- Adding Active Directory groups automatically to the IT Shop on page 100

Changing Active Directory groups

Product owners and target system managers can request updates to the group type and group scope of Active Directory groups in the Web Portal. The target system manager must grant approval for these changes. The changes are published in the target system.

Prerequisites

- The group can be requested in the IT Shop.
- Identities are assigned to the **Target systems | Active Directory** application role.

Table 59: Default objects for changing an Active Directory group

Product	Modifying an Active Directory group
Service category	Not assigned
Shelf	Identity & Access Lifecycle > Group Lifecycle
Approval policies/approval workflows	Approval of Active Directory group change requests

Deleting Active Directory groups

Product owners and target system managers can request deletion of an Active Directory group in the Web Portal. The product owner or target system manager must grant deletion approval. The group is deleted in One Identity Manager and the change is published in the target system.

Prerequisites

- The group can be requested in the IT Shop.
- Identities are assigned to the **Target systems | Active Directory** application role.

Table 60: Default objects for deleting an Active Directory group

Product	Deleting an Active Directory group
Service category	Not assigned
Shelf	Identity & Access Lifecycle > Group Lifecycle
Approval policies/approval workflows	Approval of Active Directory group deletion requests

Active DirectoryRequesting Groups Memberships

Product owners and target system managers can request members for groups in these shelves in the Web Portal. The respective product owner or target system manager must grant approval for this modification. The changes are published in the target system.

Table 61: Default objects for requesting group memberships

Shelves:	Identity & Access Lifecycle > Active Directory groups

Approval policies/approval workflows	Approval of Active Directory group membership requests

Related topics

- Adding Active Directory groups automatically to the IT Shop on page 100
- Adding Active Directory groups on page 203

Basic data for managing an Active Directory environment

To manage an Active Directory 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 Active Directory user accounts and Active Directory contacts on page 58.

- Password policy

  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 Active Directory user accounts on page 113.

- Initial password for new user accounts

  You have the different options for issuing an initial password for user accounts. Enter a password or use a random generated initial password when you create a user account.

  For more information, see Initial password for new Active Directory user accounts on page 125.

- Email notifications about credentials

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

  For more information, see Email notifications about login data on page 125.

- User account names

    To assign permissions to directories and files, it is sometimes necessary to define user account names such as **Administrators** or **Domain Users** in specific languages.

    For more information, see User account names on page 207.

- 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 50.

- 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 Target system managers for Active Directory on page 208.

- Servers

    Servers must be informed of your server functionality in order to handle Active Directory-specific processes in One Identity Manager. These may be the synchronization server, home server, or profile server, for example.

    For more information, see Job server for Active Directory-specific process handling on page 213.

- Extended properties

    Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager. You can assign extended properties to system entitlements and user accounts. For example, use them in the rule conditions for compliance rules.

    For more information, see Extended properties for Active Directory system entitlements on page 225.

User account names

To assign permissions to directories and files, it is sometimes necessary to define user account names such as **Administrators** or **Domain Users** in specific languages.

> **NOTE:** Default language for user account names is English.

To edit user account names

1. In the Manager, select the **Active Directory > Basic configuration data > User account names** category.

2. Select an item in the result list. Select the **Change main data** task.

   - OR -

   Click ⊞ (**New**) in the result list.

3. Enter the English name for the user account. Translate the given text using the 🌐 button.

4. Save the changes.

Target system managers for Active Directory

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 One Identity Manager application roles.

Implementing application roles for target system managers

1. One Identity Manager basic functionality administrators specify identities as 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.

   > **NOTE:** If no identities are assigned to a child application role for target system administrators, the identities of the parent application role are granted the permissions.

Table 62: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Active Directory** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete the 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. • 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. In the Manager, log in as a basic functionality administrator (**Base roles \| 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 > Active Directory** 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 **Active Directory > 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 **Active Directory > 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** drop-down.

    - OR -

    Next to the **Target system manager** drop-down, click 🔳 to create a new application role.

    a. Enter the application role name and assign the **Target systems | Active Directory** 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

Active Directory synchronization project owners

Synchronization project owners configure synchronization and edit synchronization templates in the Synchronization Editor. Application roles for synchronization project owners are created automatically when new synchronization projects are created.

Generated application roles have the following properties:

- **Application role**: Display name of the synchronization project
- **Parent application roles**: Custom | Synchronization
- **Directly assigned identities**: Creator of the synchronization project

- **Identities assigned by dynamic role**: Target system managers of all the synchronization project base objects

The generated application roles are immediately assigned to the synchronization projects. Use them to edit synchronization projects by logging in to the Synchronization Editor using role-based credentials. If base objects are subsequently added to the synchronization project, the assigned target system managers automatically become owners of the synchronization project through the dynamic role.

Adapt application roles to meet your requirements. For example:

- Assign identities directly to application roles
- Exclude identities from dynamic roles
- Change the condition for calculating the dynamic role

Implementing application roles for target system owners

1. The One Identity Manager administrator for basic functionality specifies identities as custom application role administrators.

2. These administrators include identities in the default application role for synchronization project owners.

   These owners can create initial synchronization projects and assign identities to child application roles.

To define initial identities as administrators for custom application roles

1. In the Manager, log in as a basic functionality administrator (**Base roles | Administrators** application role).

2. Select the **One Identity Manager Administration > Custom > Administrators** category.

3. Select the **Assign identities** task.

4. Assign the identity you want and save the changes.

To add the first identities to the default application as synchronization project owners

1. Log in to the Manager as an administrator for custom application roles (**Custom | Administrators** application role).

2. Select the **One Identity Manager Administration > Custom > Synchronization** category.

3. Select the **Assign identities** task.

4. Assign the identities you want and save the changes.

Changing synchronization project owners

As soon as a synchronization project has been created, you can authorize more identities to be owners.

To permit identities to be owners of a synchronization project

1. Log in to the Manager as the synchronization project owner.

2. Select the application role in the **Active Directory > Basic configuration data > Synchronization project owners** category.

3. To assign identities directly, select the **Assign identities** task.

   - Assign identities or remove directly assigned identities and save the changes.

4. To edit the dynamic role, select the **Application role overview** task.

   a. Select the dynamic role on the overview form.

   b. To edit the exclusion list of the dynamic role, select the **Exclude identities** task.

   c. To change the dynamic role condition, select the **Change main data** task.

   d. Save the changes.

Create additional application roles for the owners manually under the **User-specific | Synchronization** application role.

To create an application role for owners

1. Log in to the Manager as an administrator of custom tasks (**Custom | Administrators** application role).

2. Select the **One Identity Manager Administration > Custom > Synchronization** category.

3. Click ⬛ in the result list.

4. Enter the application role main data.

5. Save the changes.

6. Assign identities to the application role.

For more information, see Creating and editing application roles, Creating and editing dynamic roles for application roles, and Dynamic roles.

Owners can change the application role that is assigned to the synchronization project.

To change the owner application role of a synchronization project

1. Log in to the Synchronization Editor as the synchronization project owner.

2. Open the synchronization project.

3. On the start page, in the **General** section, click **Edit**.

4. In the **Owner (application role)** drop-down, select the application role.

   > **NOTE:** The change can only be saved if the logged in identity is a member of the assigned application role.

5. Click **OK**.

6. Save the changes.

For more information, see General properties of a synchronization project.

> **NOTE:** A dynamic role determines the members of generated application roles. The dynamic role condition establishes the connection to the synchronization project for which an application role was created. Therefore, reuse of generated application roles for other synchronization projects is not recommended.

Job server for Active Directory-specific process handling

Servers must be informed of your server functionality in order to handle Active Directory-specific processes in One Identity Manager. These may be the synchronization server, home server, or profile server, for example.

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, see Setting up Job servers.

- In the Manager, select an entry for the Job server in the **Active Directory > Basic configuration data > Server** category and edit the Job server main data.

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

> **NOTE:** One Identity Manager must be installed, configured, and running in order for a server to perform its functions in the One Identity Manager Service network. For more information, see Installing and configuring the One Identity Manager Service.

To edit a Job server and its functions

1. In the Manager, select the **Active Directory > 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.

Related topics

General main data of Job servers

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

The following properties are displayed for Job servers.

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

Table 63: 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>`
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.
Local Active Directory DC	You can enter a domain controller that is physically nearby for home servers or profile servers on a member server. The Active Directory is accessed over it when jobs are being processed. If no server is entered the main domain controller for the domain is used.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.

Property	Meaning
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Max. number of homes	Maximum number of home directories to maintain if the server is a home server. This number is compared with the number of (according to the database) existing home directories on the server (<Homes created>) when a new home directory is added for a user. If this number is less than the given maximum number of directories, the home can be added. Otherwise the addition of a new home directory is forbidden.
Homes created	Number of homes directories already in existing on the home server.
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.
Max. home storage space [MB]	Maximum permitted storage in MB for home directories on the home server. This is taken into account when the home directory is allocated.
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

Property	Meaning
	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 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 Emergency stop.
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.

Property	Meaning
	For more information, see Pausing handling of target system specific processes.
No automatic software update	Specifies whether to exclude the server from automatic software updating.
	NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
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

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 64: Permitted server functions

Server function	Remark
Active Directory connector	Server on which the Active Directory connector is installed. This server synchronizes the Active Directory target system.
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

Server function	Remark
	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.
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	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 on which the One Identity Manager Service handles email notifications.
Default report server	Server on which reports are generated.
PowerShell connector	The server can run PowerShell.

Related topics

- General main data of Job servers on page 214

Preparing a home server and profile server for creating user directories

Home and profile servers are expected when user account home and profile directories are added.

To declare home and profile servers

- In the Designer, set the **TargetSystem | ADS | AutoCreateServers** and **TargetSystem | ADS | AutoCreateServers | PreferredLanguage** configuration parameters.

  If these configuration parameters are set, entries for missing home servers and profile servers are created automatically when user accounts are synchronized.

- OR -

1. In the Manager, select the **Active Directory > 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 the **Home server** and **Profile server** server functions.
6. Save the changes.

You may use other settings for create home and profile directories.

- If you want a user's home directory to be linked at the time of login, in the Designer, set the **QER | Person | User | ConnectHomeDir** configuration parameter.
- To create the user profile in the user's home directory, in the Designer, set the **QER | Person | User | PropertyMapping | ProfileFromHome** configuration parameter.
- You can use a batch file for creating the home directory, the result of which determines whether the home directory is enabled.
- You can create a template structure on the profile server that is used in the process of creating the profile directory.
- Home and profile directory permissions can be granted through the One Identity Manager Service.

Creating home directories using batch files

To satisfy specific demands of individual network environments, you can use a batch file, which is run when you create a home directory with One Identity Manager Service. Whether the home directory is ultimately enabled depends on the result of running the batch file.

To use this function, a Netlogon share must exist on all home servers. Subdirectories are added in the Netlogon share, which correspond to the NetBIOS names of the domain. If there is a batch file in this directory with the name `HomePre.CMD`, it is run before the home directory is added. If the batch file ends in failure (that means Errorlevel <> 0), the home directory is not added.

Pass the following command line parameters to the batch file `HomePre.CMD` to be used during the run (in the given order; database column names are used):

`SAMAccountName (from table ADSAccount)`

`Ident_Domain (from table ADSAccount)`

`Ident_Server (from table QBMServer)`

`SharedAs (from table ADSAccount)`

`HomeDirPath (from table ADSAccount)`

`HomeShare (from table ADSAccount)`

You can run another batch file again after adding a home directory. This must be kept in the same place as before and have the name `HomePost,CMD`. You pass the parameters in the same way as `HomePre.CMD`. Merely, the exit code (Errorlevel) is not handled.

Example: Batch calls to create a home

A user account **Test1** is created in the domain **Dom2**. Its home directory should be created on the server **Serv3** in the shared drive **Share7** with the name **TestHome6** and be released as **TestShare5**. On the running home server **ServHome** the files `HomePre.CMD` and `HomePost.CMD` are found in the `\\ServHome\Netlogon\Dom2` directory.

Batch call before creating the home directory:

`\\ServHome\Netlogon\Dom2\HomePre.CMD Test1 Dom2 Serv3 TestShare5 TestHome6 Share7`

If the batch run returns an exit code 0, the home directory is created. Otherwise, the process is stopped with a log message.

Batch call after creating the home directory:

```
\\ServHome\Netlogon\Dom2\HomePost.CMD Test1 Dom2 Serv3 TestShare5
TestHome6 Share7
```

Supporting multiple profile directories

The different Windows operating system versions use different repositories for roaming user profiles. For more information about storing roaming user profiles, see the MicrosoftTechNet Library.

To map the roaming user profile in One Identity Manager.

- Provide a template structure for the user profile on the profile server.

  Example of a template structure for user profiles on a profile server

  ```
  PROFILE
        UserProfile
              All required folders/files
        UserProfile.V2
              All required folders/files
        UserProfile.V3
              All required folders/files
        UserProfile.V4
              All required folders/files
  ```

- In the Designer, set the **TargetSystem | ADS | Accounts | ProfileFixedString** configuration parameter and define the part of the user profile directory that you want to attach to the default profile path. The default value is `UserProfile`.

As a result, the directory paths for the user profiles are mapped as follows in the default installation.

- If the profile directory is created in the home directory:

  `\\Servername\HOMES\Username$\PROFILES\UserProfile`

- If the profile directory is not created in the home directory:

  `\\Servername\PROFILES\Username\UserProfile`

The following directories exist after handling the processes.

- If the profile directory is created in the home directory:

  `\\Servername\HOMES\Username$\PROFILES\UserProfile`

  `\\Servername\HOMES\Username$\PROFILES\UserProfile.v2`

```
\\Servername\HOMES\Username$\PROFILES\UserProfile.v3

\\Servername\HOMES\Username$\PROFILES\UserProfile.v4
```

- If the profile directory is not created in the home directory:

```
\\Servername\PROFILES\Username\UserProfile

\\Servername\PROFILES\Username\UserProfile.v2

\\Servername\PROFILES\Username\UserProfile.v3

\\Servername\PROFILES\Username\UserProfile.v4
```

The directory paths for the repository on the terminal server are mapped in the same way.

- In this case, in the Designer, change the **TargetSystem | ADS | Accounts | TProfileFixedString** configuration parameter accordingly.

- Specify in this configuration parameter the part of the user profile directory path which is appended to the default profile path on a terminal server. The default value is `UserProfile`.

Home and profile directory access permissions

Table 65: Configuration parameters for setting up user directories

Configuration parameter	Meaning
QER	Person	User	AccessRights	Configuration of permissions for accessing user directories.

> **NOTE:** To assign permissions to directories and files, it is sometimes necessary to define user account names such as **Administrators** or **Domain Users** in specific languages. The default language for the user accounts names is English.

> **NOTE:** Ensure that the subdirectories under the root directories, such as the home directory, do not inherit permissions for the **Everyone** user group. Otherwise, there is a possibility that the user group obtains unwanted permissions on all home directories.

To grant access permissions for the home directory

- In the Designer, set the **QER | Person | User | AccessRights | HomeDir** and its configuration subparameters, then enter the access permissions in the configuration parameters.

  Granting access permissions to the home directory is done by the One Identity Manager Service.

Table 66: Configuration parameters for home directory access permissions

Configuration parameter	Effect when set
QER | Person | User | AccessRights | HomeDir	Configuration of access permissions for the user's home directory. To set the permissions, the configuration parameter and subparameters need to be set.
QER | Person | User | AccessRights | HomeDir | User	Defines the user's home directory permissions. Default: **+r+w-x**

To grant access permission for the profile directory

- In the Designer, set the **QER | Person | User | AccessRights | ProfileDir** configuration parameter and its configuration subparameters, and enter the access permissions in the configuration parameters.

  Granting access permissions to the profile directory is done by the One Identity Manager Service.

Table 67: Configuration parameters for profile directory access permissions

Configuration parameter	Effect when set
QER | Person | User | AccessRights | ProfileDir	Configuration of access permissions for the user's profile directory. To set the permissions, the configuration parameter and subparameters need to be set.
QER | Person | User | AccessRights | ProfileDir | User	Defines the user's profile directory permissions. Default: **+r+w-x**

To grant access permissions for the home directory on a terminal server

- In the Designer, set the **QER | Person | User | AccessRights | TerminalHomeDir** and its configuration subparameters, and enter the access permissions in the configuration parameters.

  Granting access permissions to the home directory is done by the One Identity Manager Service.

Table 68: Configuration parameters for access permissions to the home directory on a terminal server

Configuration parameter	Effect when set
QER | Person | User | AccessRights | TerminalHomeDir	Configuration of access permissions for an Active Directory user account's terminal server home directory. To set the permissions, the configuration parameter and subparameters need to be set.
QER | Person | User | AccessRights | TerminalHomeDir | User	Defines the user's terminal server home directory permissions. Default: **+r+w-x**

To grant access permissions for the profile directory on a terminal server

- In the Designer, set the **QER | Person | User | AccessRights | TerminalProfileDir** and its configuration subparameters, and enter the access permissions in the configuration parameters.

  Granting access permissions to the profile directory is done by the One Identity Manager Service.

Table 69: Configuration parameters for access permissions to the profile directory on a terminal server

Configuration parameter	Effect when set
QER | Person | User | AccessRights | TerminalProfileDir	Configuration of access permissions for an Active Directory user account's terminal server profile directory. To set permissions, the configuration parameter and subparameters need to be set.
QER | Person | User | AccessRights | TerminalProfileDir | User	Terminal server profile directory permissions. Default: **+r+w-x**

Related topics

- User account names on page 207

Extended properties for Active Directory system entitlements

Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager. You can assign extended properties to system entitlements and user accounts. For example, use them in the rule conditions for compliance rules.

For more information, see Extended properties and property groups and Setting up extended properties.

To assign extended properties

1. First, set up a property group, under which the extended properties will be grouped.

   - In the Manager, select the **Active Directory > Basic configuration data > Extended properties** category.

2. Set up the extended properties in the property group.

   - In the Manager, select the **Active Directory > Basic configuration data > Extended properties > <property group>** category.

3. Assign the extended properties to the system entitlements.

Related topics

- Assigning extended properties to Active Directory user accounts on page 163
- Assigning extended properties to Active Directory containers on page 142
- Assigning extended properties to Active Directory groups on page 189

Configuration parameters for managing an Active Directory environment

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

Table 70: Configuration parameters

Configuration parameters	Description
QER | ITShop | AutoPublish | ADSGroup	Preprocessor relevant configuration parameter for automatically adding Active Directory groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. 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.
QER | ITShop | AutoPublish | ADSGroup | AutoFillDisplayName	The configuration parameter specifies whether the template should be applied to the `ADSGroup.DisplayName` column.
QER | ITShop | AutoPublish | ADSGroup | ExcludeList	List of all Active Directory groups that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_ IUSRS`
TargetSystem | ADS	Preprocessor relevant configuration parameter for controlling database model components for Active Directory target system administration. If the parameter is set, the target system

Configuration parameters	Description
	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.
TargetSystem	ADS	Accounts	Allows configuration of user account data.
TargetSystem	ADS	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	ADS	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 configuration parameter **TargetSystem	ADS	DefaultAddress**.
TargetSystem	ADS	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	ADS	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	ADS	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	ADS	Accounts	NotRequirePassword	Specifies whether a password is required when creating new Active Directory user accounts in One Identity Manager. If the configuration parameter is not set, entry of a password that meets the defined password guidelines is requested when a new Active Directory user account is created. If the configuration parameter is set, it is not necessary to specify a password when creating new Active Directory user accounts.
TargetSystem	ADS	Accounts		Allows configuration of privileged Active Directory user account settings.

Configuration parameters	Description
PrivilegedAccount	
TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_ Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem | ADS | Accounts | PrivilegedAc- count | SAMAccountName_ Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem | ADS | Accounts | ProfileFixedString	Fixed string appended to the default profile path of a user profile.
TargetSystem | ADS | Accounts | TransferJPegPhoto	Specifies whether changes to the identity's picture are published in existing user accounts. The picture is not part of default synchronization. It is only published when an identity's main data is changed.
TargetSystem | ADS | Accounts | TransferSIDHistory	Specifies whether the SID history is loaded from the target system.
TargetSystem | ADS | Accounts | TSProfileFixedString	Fixed string appended to the default profile path of a user profile on a terminal server.
TargetSystem | ADS | Accounts | UnlockByCentralPasswo rd	Specifies whether the identity's Active Directory user account is unlocked when the central password is synchronized.
TargetSystem | ADS | Accounts | UserMustChangePassw ord	Specifies whether the **Change password at next login** option is enabled when a new user account is created.
TargetSystem | ADS | AuthenticationDomains	Domains to be used by the manual Active Directory authentication module to authenticate users. The list is processed in the same sequence as given in the configuration parameter. This list should only contain domains to be synchronized. The domain name is entered as used when logging in to user accounts, either with the down-level login name

ONE IDENTITY

Configuration parameters	Description
	(domain\username) or the user principal name (username@domain). Multiple domains are specified in a list separated by a pipe character (|).
	Example:
	mydomain|myotherdomain
	For more information, see One Identity Manager authentication modules.
TargetSystem | ADS | AutoCreateDepartment	Specifies whether departments are automatically created when user accounts are modified or synchronized.
TargetSystem | ADS | AutoCreateLocality	Specifies whether locations are automatically created when user accounts are modified or synchronized.
TargetSystem | ADS | AutoCreateHardwaretype	Specifies whether corresponding device types are created automatically in the database for imported printer objects.
TargetSystem | ADS | AutoCreateServers	Specifies whether entries for missing home servers and profile servers are created automatically when user accounts are synchronized.
TargetSystem | ADS | AutoCreateServers | PreferredLanguage	Language of automatically created servers.
TargetSystem | ADS | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | ADS | HardwareInGroupFromOrg	Specifies whether computers are added to groups based on group assignment to roles.
TargetSystem | ADS | 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 | ADS | MembershipAssignCheck	Specifies whether membership validity is verified on saving when group memberships are assigned in the One Identity Manager database.
	Disable this configuration parameter if several trusted domains with access across memberships are managed in the database.
TargetSystem | ADS | MemberShipRestriction	General configuration parameter for restricting membership in Active Directory.

ONE IDENTITY

Configuration parameters	Description
TargetSystem | ADS | MemberShipRestriction | Container	Number of Active Directory objects allowed per container before warning email is sent.
TargetSystem | ADS | MemberShipRestriction | Group	Number of Active Directory objects allowed per group before warning email is sent.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Default mail address for sending warning emails.
TargetSystem | ADS | PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem | ADS | PersonAutoDisabledAccounts	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem | ADS | PersonAutoFullSync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem | ADS | PersonExcludeList	Listing of all user account without automatic identity assignment. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.* |SUPPORT_.*|.* | $`
TargetSystem | ADS | PersonUpdate	Specifies whether identities are updated if their user accounts are changed. This configuration parameter is set to allow ongoing update of identities from associated user accounts.
TargetSystem | ADS | ReplicateImmediately	Speeds up synchronization of modifications between two domain controllers When set, the accumulated modifications in Active Directory are immediately replicated between domain controllers.

Default project template for Active Directory

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.

The project template uses mappings for the following schema types.

Table 71: Mapping Active Directory schema types to tables in the One Identity Manager schema

Schema type in Active Directory	Table in the One Identity Manager Schema
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
forest (virtual schema type)	ADSForest
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
organizationalUnit	ADSContainer
posixContact	ADSContact
posixGroup	ADSGroup

Schema type in Active Directory	Table in the One Identity Manager Schema
posixUser	ADSAccount
printQueue	ADSPrinter
serverInSite	ADSMachineInADSSite
site	ADSSite
trustedDomain	DomainTrustsDomain
user	ADSAccount

Processing methods of Active Directory system objects

The following table describes permitted editing methods for Active Directory schema types and the necessary restrictions for processing the system objects.

Table 72: Methods available for processing Active Directory schema types

Type	Read	Add	Delete	Refresh
Domain (`domainDNS`)	Yes	No	No	Yes
Forest (`forest`)	Yes	No	No	No
Password policies (`msDS-PasswordSettings`)	Yes	Yes	Yes	Yes
Trusted domain (`trustedDomain`)	Yes	No	No	No
Container (`container`)	Yes	Yes	Yes	Yes
Container (`builtInDomain`)	Yes	Yes	Yes	Yes
Container (`organizationalUnit`)	Yes	Yes	Yes	Yes
User accounts (`user, posixUser`)	Yes	Yes	Yes	Yes
User accounts (`inetOrgPerson`)	Yes	Yes	Yes	Yes
Contacts (`contact, posixContact`)	Yes	Yes	Yes	Yes
Groups (`group, posixGroup`)	Yes	Yes	Yes	Yes
Computer, server (`computer`)	Yes	Yes	Yes	Yes
Computer: location assignments (`serverInSite`)	Yes	No	No	No
Location (`site`)	Yes	No	No	No
Printer (`printQueue`)	Yes	No	No	No

Active Directory connector settings

The following settings are configured for the system connection with the Active Directory connector.

Table 73: Active Directory connector settings

Setting	Meaning
Domain	Full domain name. Variable: `CP_ADRootdn`
User account	User account for logging in to the target system. Variable: `CP_BASELoginaccount` If the currently logged in user account is used, leave this field empty. The user account running under the One Identity Manager Service requires the permissions described in Users and permissions for synchronizing with Active Directory on page 16. **NOTE:** If you do not enter a user account, the current user account is also used in the Synchronization Editor during configuration. This user account may be different to the One Identity Manager Service's user account In this case, it is recommended you use the **RemoteConnectPlugin**. This ensures that the same user account is used during configuration with the Synchronization Editor as is used in the service context.
Password	The user account's password. Variable: `CP_BASEPassword`
Authentication type	Authentication type for target system login. The **Secure** authentication type is used by default. Variable: `CP_ADAuthentication`
Domain controller	Full name of the domain controller for connecting to the

Setting	Meaning
	synchronization server to provide access to Active Directory objects.
	Example:
	`<Name of servers>.<Fully qualified domain name>`
	Variable: `CP_ADServer`
Port	Communications port on the domain controller.
	Default value: **389**
	Variable: `CP_ADPort`
Use SSL	Specifies whether to use a secure connection.
When restoring objects with the same distinguished name or GUID from the recycle bin.	Specifies whether deleted Active Directory objects are taken into account on insertion.
	Set this option if, when adding an object, the system first checks whether the object is in the Active Directory recycling bin and must be restored.
	Default: **False**
	Variable: `CP_ADEnableTombstone`
Allow read and write access to Remote Access Service (RAS) properties.	Specifies whether Remote Access Service (RAS) properties are synchronized.
	Default: **False**
	Variable: `CP_ADEnableras`
Allow read and write access to the terminal service properties.	Specifies whether terminal server properties are synchronized.
	Default value: **True**
	Variable: `CP_ADEnableterminal`
Extensions	(Expert mode only) The schema used in synchronization can be customized by adding additional auxiliary classes to structural classes. The extension methods apply to the structural class and its derived classes.

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

risk index 146

set up 145

terminal server profile 156

town 91, 159

unlock 146, 168

update identity 89

wizard 162

workstation 154

architecture overview 10

B

base object 38, 44

C

calculation schedule 46

deactivate 47

configuration parameter 226

convert connection parameter 38

D

direction of synchronization

direction target system 24, 35

in the Manager 24

E

email notification 125

exclusion definition 106

extended property 225

F

firewall configuration 19

G

group

change 202-203

delete 204

request 202-203

H

home server 219

home directory 219-222

HomePost.cmd 220

HomePre.cmd 220

I

identity 84

identity assignment

automatic 78

manual 81

remove 81

search criteria 80

table column 80

installation prerequisites

firewall 19

ports 19

IT operating data

change 68

IT Shop shelf

assign account definition 73

J

Job server

edit 21

load balancing 45

V

variable set 38

   active 39