One Identity Manager 8.1.5

Administration Guide for Connecting to Active Directory

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

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

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

One Identity Manager Administration Guide for Connecting to Active Directory
Updated - 09 July 2021, 11:43
Version - 8.1.5

Contents

1

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 employees with the user accounts required to allow you to use different mechanisms for connecting employees to their user accounts. You can also manage user accounts independently of employees and therefore 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.

Architecture overview

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

- Active Directory domain controller

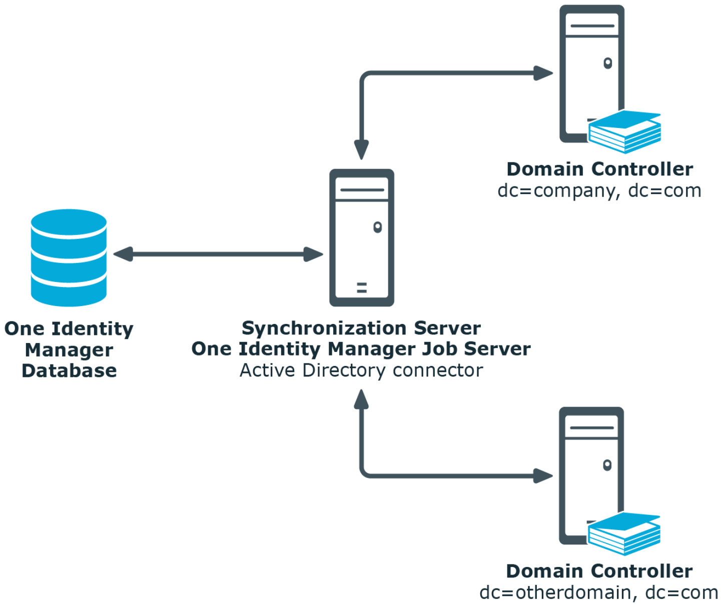
  Domain controller against which the Active Directory objects are synchronized. The synchronization server connects to this server in order to access the Active Directory objects.

- Synchronization server

  The synchronization server for synchronizing data between One Identity Manager and 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

User	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive.

User	Tasks
	- Authorize other employees to be target system administrators. - Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | 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 target system objects like user accounts or groups. - Edit password policies for the target system. - Prepare groups to add to the IT Shop. - Can add employees who have an other identity than the **Primary identity**. - Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. - Edit the synchronization's target system types and outstanding objects. - Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	- Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. - Create system users and permissions groups for non role-based login to administration tools in the Designer as required. - Enable or disable additional configuration parameters in the Designer as required. - Create custom processes in the Designer as required. - Create and configure schedules as required. - Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role:

User	Tasks
	- 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.

2

Setting up Active Directory synchronization

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

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.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with Active Directory on page 14
- Communications ports and firewall configuration on page 17
- Setting up the synchronization server on page 18
- Creating a synchronization project for initial synchronization of an Active Directory domain on page 21
- Disabling synchronization on page 38
- Customizing the synchronization configuration on page 28

- Configuration parameters for managing an Active Directory environment on page 193
- Default project template for Active Directory on page 198

Users and permissions for synchronizing with Active Directory

The following users are involved 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 authorizations for full synchronization of Active Directory objects with the supplied One Identity Manager default configuration. • Member of the Active Directory group **Domain administrators** NOTE: In a hierarchical domain structure, the user account of the One Identity Manager Service child domain must be a member of the **Enterprise Admins**. We cannot recommend any practical minimum configuration with different permissions in terms of user administration from a member of the group **Domain administrators**.
One Identity Manager Service user account	The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires access permissions to the internal web service. NOTE: If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems)

User	Permissions
	• `%ProgramFiles%\One Identity` (on 64-bit operating systems) Setting Remote Access Service (RAS) properties requires Remote Procedure Calls (RPC) which are executed 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.
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to execute synchronization with an application server.

Necessary access rights explained

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

- Read
- Write

If the base object is the domain object, these access rights are required for reading and setting domain properties like, for example, password guidelines.

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

- Create All Child Objects
- Delete All Child Objects

In order to enable 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 property **Password cannot be changed**), 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 access rights 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

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

Modifying a DACL 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 DACL, 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 change the DACL 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.

Notes for read permissions

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 access rights and by taking appropriate precautions when importing.

Notes on the One Identity Manager Active Directory edition

For the One Identity Manager Active Directory edition, full **Read** permissions are required, as well as permissions for creating, changing, and deleting groups.

Communications ports and firewall configuration

One Identity Manager is made up of several components that can be executed 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
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.
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.
445	Microsoft-DS Active Directory, Windows shares. Required for synchronization (TCP/UDP)
53	Domain Name System (DNS), mainly through UDP. Required for access to the Active Directory total structure.
636	Lightweight Directory Access Protocol using TLS/SSL (LDAP S). Required for access to the Active Directory total structure.
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 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 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 or later

  > NOTE: Take the target system manufacturer's recommendations into account.
- One Identity Manager Service, Active Directory connector
  - Install One Identity Manager components with the installation wizard.
    1. Select the **Select installation modules with existing database** option.
    2. Select the **Server | Job server | Active Directory** machine role.

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

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

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

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

> NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from

> the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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

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

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

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

       - OR -

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

    b. Enter the following data for the Job server.

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

         Syntax:

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

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

4. On the **Machine roles** page, select **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 detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.

- For a direct connection to the database:
    a. Select **Process collection | sqlprovider**.
    b. Click the **Connection parameter** entry, then click the **Edit** button.
    c. Enter the connection data for the One Identity Manager database.
- For a connection to the application server:
    a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
    b. Click the **Connection parameter** entry, then click the **Edit** button.
    c. Enter the connection data for the application server.
    d. Click the **Authentication data** entry and click the **Edit** button.
    e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files.
10. On the **Select private key file** page, select the file with the private key.

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

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

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

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

Creating a synchronization project for initial synchronization of an 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 detailed information about setting up synchronization, see the One Identity Manager Target System Synchronization Reference Guide.

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

Have the following information available for setting 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.

Table 4: Information required for setting up a synchronization project

Data	Explanation
Full domain name	Full domain name. Example: `Docu.Testlab.dd`
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 14.
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: `Server.Doku.Testlab.dd`
Communications port on the domain	Communications port on the domain controller. LDAP default communications port is 389.

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td>controller</td><td></td></tr>
<tr><td>Authentication type</td><td>You can only connect to a target system if the correct type of authentication is selected. The <b>Secure</b> authentication type is used by default.
For more information about authentication types, see the MSDN Library.</td></tr>
<tr><td>Synchronization server for Active Directory</td><td>All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.
The One Identity Manager Service must be installed on the synchronization server with the Active Directory connectorActive Roles.
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.
<b>Table 5: Additional properties for the Job server</b>
<table>
<tr><th>Property</th><th>Value</th></tr>
<tr><td>Server function</td><td>Active Directory connector</td></tr>
<tr><td>Machine role</td><td>Server/Jobserver/Active Directory</td></tr>
</table>
For more information, see Setting up the synchronization server on page 18.</td></tr>
<tr><td>One Identity Manager database connection data</td><td>• Database server
• Database
• SQL Server login and password
• Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td></tr>
<tr><td>Remote connection server</td><td>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is</td></tr>
</table>

Data	Explanation
	not possible from the workstation, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed • 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 as remote connection server at the same time, by simply installing the **RemoteConnectPlugin** as well. For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

To set up an initial synchronization project for Active Directory domains

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

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

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

   This starts the Synchronization Editor's project wizard.

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

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

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

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

4. On the **Domain selection** page, specify the Active Directory domain to synchronize.
   - Select the domain in the **Domain** list or enter the full domain name.
5. 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. The user account requires the permissions described under Users and permissions for synchronizing with Active Directory on page 14.

      > 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.
6. 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** menu, 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.
7. Specify additional synchronization settings on the **Connector features** page. Enter 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 are a later date.
Allow read and write access to the terminal service properties.	Specifies whether Remote Access Service (RAS) 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 are a later date.

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

8. 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.

9. 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.

10. 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

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

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

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

    a. Click + to add a new Job server.

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

    c. Click **OK**.

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

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

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

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

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

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

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

    NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project**

> **automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

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

NOTE:

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

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

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **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** menu, select the account definition.

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

    e. Save the changes.

Related topics

- Setting up the synchronization server on page 18
- Users and permissions for synchronizing with Active Directory on page 14
- Displaying synchronization results on page 28
- Customizing the synchronization configuration on page 28
- Speeding up synchronization with revision filtering on page 32
- Default project template for Active Directory on page 198
- Account definitions for Active Directory user accounts on page 42
- Automatic assignment of employees to Active Directory user accounts on page 127

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

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

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

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

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

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

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.

Customizing the synchronization configuration

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 master system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing methods, for example.
- 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.

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

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

Detailed information about this topic

- Configuring synchronization in Active Directory domains on page 30
- Configuring synchronization of different Active Directory domains on page 30
- Updating schemas on page 31

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

To create a synchronization configuration for synchronizing Active Directory domains

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

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

Related topics

- Configuring synchronization of different Active Directory domains on page 30

Configuring synchronization of different Active Directory domains

Prerequisites

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

To customize a synchronization project for synchronizing another domain

1. Prepare a user account with sufficient permissions for synchronizing in the other domain.
2. Open the synchronization project in the Synchronization Editor.

3. Create a new base object for the other domains. Use the wizard to attach a base object.
    - In the wizard, select the Active Directory connector and declare the connection parameters. The connection parameters are saved in a special variable set.

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

Related topics

- Configuring synchronization in Active Directory domains on page 30

Updating schemas

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

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

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

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

To update a system connection schema

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

- OR -

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

3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

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

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

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

Speeding up synchronization with revision filtering

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

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.

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

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

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

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

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.

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

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

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

- The synchronization log has already been deleted.

  - OR -

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

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

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

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

> TIP:
>
> ***To display object properties of an outstanding object***
>
> a. Select the object on the target system synchronization form.
>
> b. Open the context menu and click **Show object**.

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

Table 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. The **Outstanding** label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

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

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

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

To add custom tables to target system synchronization

1. In the Manager, select the **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.

> 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.

Configuring the provisioning of memberships

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

- Memberships are saved in the target system as an object property in list form (Example: List of user accounts in the `Members` property of an Active Directory `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.
    - This option can only be enabled for assignment tables that have a base table with an `XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically (for example, `ADSAccountInADSGroup`, `ADSGroupInADSGroup` and `ADSMachineInADSGroup`).
5. Click **Merge mode**.
6. Save the changes.

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

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

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

To restore the default condition

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

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

Accelerating provisioning and single object synchronization

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

> NOTE: You should not implement load balancing for provisioning or single object synchronization on a permanent basis. Parallel processing of objects might result in dependencies not being resolved because referenced objects from another Job server have not been completely processed.
>
> Once load balancing is no longer required, ensure that the synchronization server executes the provisioning processes and single object synchronization.

To configure load balancing

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

    - Assign the **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 about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- Editing a server on page 75

Help for the analysis of synchronization issues

You can generate a report for analyzing problems that arise during synchronization, inadequate performance for example. The report contains information such as:

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

To generate a synchronization analysis report

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Help | Generate synchronization analysis report** menu item and click **Yes** in the security prompt.

   The report may take a few minutes to generate. It is displayed in a separate window.
3. Print the report or save it in one of the available output formats.

Disabling synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Related topics

- Creating a synchronization project for initial synchronization of an Active Directory domain on page 21

Basic data for managing an Active Directory environment

To manage an Active Directory environment in One Identity Manager, the following basic data is relevant.

- Configuration parameter

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

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

  For more information, see Configuration parameters for managing an Active Directory environment on page 193.

- Account definitions

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

  For more information, see Account definitions for Active Directory user accounts on page 42.

- Password policy

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

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

For more information, see Password policies for Active Directory user accounts on page 60.

- Initial password for new user accounts

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

  For more information, see Initial password for new Active Directory user accounts on page 71.

- 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 71.

- User account names

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

  For more information, see User account names on page 72.

- Target system types

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

  For more information, see Post-processing outstanding objects on page 33.

- Target system managers

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

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

  For more information, see Target system managers on page 73.

- Server

  Servers must know 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 Editing a server on page 75.

Account definitions for Active Directory user accounts

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

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

For detailed information about account definitions, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating an account definition
- Setting up manage levels
- Creating a formatting rule for IT operating data
- Collecting IT operating data
- Assigning account definitions to employees
- Assigning account definitions to a target system

Creating an account definition

To create a new account definition

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

   -OR-

   Click 🗋 in the result list.
3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- Master data for an account definition on page 43

Master data for an account definition

Enter the following data for an account definition:

Table 9: Master data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. Leave empty for Active Directory domains.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can also be assigned directly to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee

Property	Description
to employees	not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Setting up manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

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

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

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

To assign manage levels to an account definition

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

   - OR -

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

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

To edit a manage level

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

   - OR -

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

Related topics

- Master data for manage levels on page 46

Master data for manage levels

Enter the following data for a manage level.

Table 10: Master data for manage levels

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

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

Creating a formatting rule for IT operating data

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

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

- Active Directory container
- Active Directory home server
- Active Directory profile server
- Active Directory terminal home server
- Active Directory terminal profile server
- 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 and enter the following data.

Table 11: Mapping rule for IT operating data

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

4. Save the changes.

Related topics

- Collecting IT operating data on page 49

Collecting IT operating data

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

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

Example

Normally, each employee in department A obtains a default user account in the domain A. In addition, certain employees in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. Specify the "Department" property in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

To define IT operating data

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

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

Table 12: IT operating data

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

4. Save the changes.

Related topics

- Creating a formatting rule for IT operating data on page 47

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To execute the template

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

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

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

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

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

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

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 54
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 55
- Adding account definitions in the IT Shop on page 56
- Assigning account definitions to a target system on page 57

Assigning account definitions to departments, cost centers, and locations

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.

Related topics

- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 54
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 55
- Adding account definitions in the IT Shop on page 56

Assigning an account definition to business roles

Installed modules:	Business Roles Module

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, assign business roles.

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

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning account definitions to all employees on page 54
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 55
- Adding account definitions in the IT Shop on page 56

Assigning account definitions to all employees

To assign an account definition to all employees

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 master data** task.
4. On the **General** tab, enable the **Automatic assignment to employees** option.

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

5. Save the changes.

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

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 55
- Adding account definitions in the IT Shop on page 56

Assigning account definitions directly to employees

To assign an account definition directly to employees

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 employees** task.
4. In the **Add assignments** pane, add employees.

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

> ***To remove an assignment***
>
> - Select the employee and double-click ✓.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 54
- Assigning account definitions to system roles on page 55
- Adding account definitions in the IT Shop on page 56

Assigning account definitions to system roles

Installed modules:	System Roles Module

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

To add account definitions to a system role

1. In the Manager, select the **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 assigned system roles.
   >
   > ***To remove an assignment***
   >
   > - Select the system role and double-click ✓.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 54
- Assigning account definitions directly to employees on page 54
- Adding account definitions in the IT Shop on page 56

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 employees using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

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

To add an account definition to the IT Shop

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

   - OR -

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

To remove an account definition from individual IT Shop shelves

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

   - OR -

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

To remove an account definition from all IT Shop shelves

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

   - OR -

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

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

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

Related topics

- Master data for an account definition on page 43
- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 54
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 55

Assigning account definitions to a target system

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

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

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

To assign the account definition to a target system

1. In the Manager, select the domain in the **Active Directory | Domains** category.
2. Select the **Change master data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. From the **Contact definition (initial)** menu, select the account definition for contacts.
5. From the **E-mail contact definition (initial)** menu, select the account definition for email contacts.
6. From the **E-mail user definition (initial)** menu, select the account definition for email users.
7. Save the changes.

Detailed information about this topic

- Automatic assignment of employees to Active Directory user accounts on page 127

Deleting an account definition

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
   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 master data** task.
   d. On the **General** tab, disable the **Automatic assignment to employees** option.
   e. Save the changes.
2. Remove direct assignments of the account definition to employees.
   a. In the Manager, select the **Active Directory | Basic configuration data | Account definitions | Account definitions** category.
   b. Select an account definition in the result list.
   c. Select the **Assign to employees** task.
   d. In the **Remove assignments** pane, remove the employees.
   e. Save the changes.

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

    a. In the Manager, select the **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.

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

    d. Save the changes.

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

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

   To remove an account definition from all IT Shop shelves

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

       - OR -

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

    b. Select an account definition in the result list.

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

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

    e. Click **OK**.

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

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

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

    b. Select an account definition in the result list.

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

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

    e. Save the changes.

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

    a. In the Manager, select the domain in the **Active Directory | Domains** category.

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

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

    d. Save the changes.

8. Delete the account definition.

    a. In the Manager, select the **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.

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 employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

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

Detailed information about this topic

- Predefined password policies on page 61
- Using password policies on page 62
- Editing password policies on page 64
- Custom scripts for password requirements on page 67
- Password exclusion list on page 70
- Checking a password on page 70
- Testing password generation on page 70

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

> NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.1.5, the configuration parameter settings for forming passwords are passed on to the target system-specific 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.

Related topics

- Global account policies for an Active Directory domain on page 89
- Active Directory account policies for Active Directory domains on page 94

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

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

To reassign a password policy

1. In the Manager, select the **Active Directory | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.

3. Select the **Assign objects** task.
4. Click **Add** in the **Assignments** section and enter the following data.

Table 13: Assigning a password policy

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

5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **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** menu, select the new password policy you want to apply.
6. Save the changes.

Editing password policies

To edit a password policy

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

   - OR -

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

Detailed information about this topic

- General master data for password policies on page 64
- Policy settings on page 65
- Character classes for passwords on page 66
- Custom scripts for password requirements on page 67

General master data for password policies

Enter the following master data for a password policy.

Table 14: Master data for a password policy

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

Policy settings

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

Table 15: Policy settings

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

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

Character classes for passwords

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

Table 16: Character classes for passwords

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

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

Custom scripts for password requirements

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

Detailed information about this topic

- Script for checking passwords on page 67
- Script for generating a password on page 68

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 of a script that checks a password

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

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

      Dim pwd = spwd.ToInsecureArray()

      If pwd.Length>0

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

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

            End If

      End If

      If pwd.Length>2

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

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

            End If

      End If

End Sub
```

To use a custom script for checking a password

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

Related topics

- Script for generating a password on page 68

Script for generating a password

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

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

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

     Dim pwd = spwd.ToInsecureArray()

     ' replace invalid characters at first position

     If pwd.Length>0

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

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

          End If

     End If

End Sub
```

To use a custom script for generating a password

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

Related topics

- Script for checking passwords on page 67

Password exclusion list

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

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

To add a term to the restricted list

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

Checking a password

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

To check if a password conforms to the password policy

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

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

Testing password generation

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

To generate a password that conforms to the password policy

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

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

   This generates and displays a password.

Initial password for new Active Directory user accounts

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

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

Related topics

- Password policies for Active Directory user accounts on page 60
- Email notifications about login data on page 71

Email notifications about login data

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

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

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

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

To send initial login data by email

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

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

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

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

User account names

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

NOTE: Default language for user account names is English.

To edit user account names

1. Select **Active Directory | Basic configuration data | User account name**.
2. Select an item in the result list. Select the **Change master data** task.

   - OR-

   Click 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

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

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

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

Implementing application roles for target system managers

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

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

Table 17: 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.

User	Tasks
	- Create, change, or delete target system objects like user accounts or groups. - Edit password policies for the target system. - Prepare groups to add to the IT Shop. - Can add employees who have an other identity than the **Primary identity**. - Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. - Edit the synchronization's target system types and outstanding objects. - Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

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

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

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

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

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

To specify target system managers for individual domains

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

   - OR -

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

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

   b. Click **OK** to add the new application role.
6. Save the changes.
7. Assign employees to this application role who are permitted to edit the domain in One Identity Manager.

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

Related topics

- One Identity Manager users for managing Active Directory on page 10
- General master data for Active Directory domains on page 87
- Master data for an Active Directory container on page 178

Editing a server

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 detailed information, see *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **Active Directory | Basic configuration data | Server** category and edit the Job server master data category.

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 started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

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 master data** task.
4. Edit the Job server's master data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master data for a Job server on page 76
- Specifying server functions on page 79
- Preparing a home server and profile server for creating user directories on page 81

Master data for a Job server

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

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

Table 18: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of server>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.

Property	Meaning
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.
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	Maximum permitted storage in MB for home directories on the home server. This is taken into account when the home directory is allocated.

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

Property	Meaning
update	
Software update running	Specifies whether a software update is currently running.
Last fetch time	Last time the process was collected.
Last timeout check	The time of the last check for loaded process steps with a dispatch value that exceeds the one in the **Common | Jobservice | LoadedJobsTimeOut** configuration parameter.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 79

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 19: 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 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.

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

Related topics

- Master data for a Job server on page 76

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. Select the **Active Directory | Basic configuration data | Servers** category.
2. Select the Job server entry in the result list.
3. Select the **Change master data** task.
4. Edit the Job server's master data.
5. Select the **Assign server functions** task and specify 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.

Related topics

- Creating home directories using batch files on page 82
- Supporting multiple profile directories on page 83
- Home and profile directory access permissions on page 84
- Master data for a Job server on page 76
- Specifying server functions on page 79

Creating home directories using batch files

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

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 executing 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 execution returns an exit code 0, the home directory is created. Otherwise, the process is aborted 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 exact information about storing roaming profile, 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 20: Configuration parameters for setting up user directories

Configuration parameter	Meaning
QER | Person | User | AccessRights	This configuration parameter allows configuration of access permissions to user directories.

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

To grant access permissions to a home directory

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

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

Table 21: Configuration parameters for home directory access permissions

Configuration parameter	Effect when set
QER | Person | User | AccessRights | HomeDir	Configuration of access permissions of the user's home directory. To set the permissions, the configuration parameter and subparameters must be set.
QER | Person | User | AccessRights | HomeDir | EveryOne	**Everyone** has permissions to access a user's home directory. Default: `-r-w-x`
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 through One Identity Manager Service.

Table 22: Configuration parameters for profile directory access permissions

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

To grant access permissions to 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 through One Identity Manager Service.

Table 23: 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 | EveryOne	**Everyone** has permission to access a user's terminal server home directory. Default: `-r-w-x`
QER | Person | User | AccessRights | TerminalHomeDir | User	Defines the user's terminal server home directory permissions. Default: `+r+w-x`

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

- In the Designer, set the **QER | Person | User | AccessRights | TerminalProfileDir** 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 through One Identity Manager Service.

Table 24: 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 | EveryOne	**Everyone** has permissions to access a user's terminal server profile directory. Default: `-r-w-x`
QER | Person | User | AccessRights | TerminalProfileDir | User	Terminal server profile directory permissions. Default: `+r+w-x`

Related topics

- User account names on page 72

Active Directory domains

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

To edit master data for an Active Directory domain

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

General master data for Active Directory domains

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

Table 25: Domain master 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:

Property	Description
	• Windows Server 2000 (Win2000) • Windows Server 2003 native (Win2003 native) • Windows Server 2003 mixed (Win2003 mixed) • Windows Server 2008 (Win2008) • Windows Server 2008 R2 (Win2008 R2) • Windows Server 2012 (Win2012) • Windows Server 2012 R2 (Win2012 R2) • Windows Server 2016 (Win2016)
Display name	The display name is used to display the domain in the user interface. This is preset with the domain NetBIOS name; however, the display name can be changed.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this domain and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.
Contact definition (initial)	Initial account definition for creating contacts. These account definitions are used if automatic assignment of employees 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 employee (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role in which target system managers are specified for the domain. Target system managers only edit the objects from domains that are assigned to them. Therefore, each domain can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this domain. Use the + button to add a new application role.
Synchronized by	Type of synchronization through which the data is synchronized between the domain and One Identity Manager. You can no longer change the synchronization type once objects for these domains are present in One Identity Manager. If you create a domain with the Synchronization Editor, **One Identity Manager** is used.

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

Table 26: Permitted values

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

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

</td></tr>
<tr><td>Description</td><td>Text field for additional explanation.</td></tr>
</table>

Related topics

- Automatic assignment of employees to Active Directory user accounts on page 127
- Target system managers on page 73
- Information about the Active Directory forest on page 92

Global account policies for an Active Directory domain

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.

Enter the following master data on the **Account policies** tab.

Table 27: 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.
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.

Property	Description
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.
Block duration [min]	Block 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.

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.

Related topics

- Password policies for Active Directory user accounts on page 60
- Active Directory account policies for Active Directory domains on page 94
- Password data for Active Directory user accounts on page 112

Active Directory specific master data for Active Directory domains

Enter the following data on the **Active Directory** tab:

Table 28: 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 default domain` Example

Property	Description
	`Docu.Testlab.dd`
Account manager	Manager responsible for the domain. ***To specify an account manager*** 1. Click → next to the field. 2. In the **Table** menu, select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 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	Specifies whether the recycling bin is enabled (from functional level **Windows Server 2008 R2**). The property is imported by the synchronization and should not be edited in One Identity Manager.
Retention period	Retention period of objects in the recycling bin (from functional level **Windows Server 2008 R2**). 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 more information, see the documentation for implementing Windows Server. 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 152
- Deleting and restoring Active Directory user accounts on page 134

- Active Directory account policies for Active Directory domains on page 94
- Preparing a home server and profile server for creating user directories on page 81

Specifying categories for inheriting 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 31** category positions.

To define a category

1. Select the **Active Directory | Domains** category.
2. Select the domain in the result list.
3. Select the **Change master 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.

Detailed information about this topic

- Active Directory group inheritance based on categories on page 169

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. Select the **Active Directory | Forests** 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 master data, select the **Change master data** task.

Related topics

- Trusted Active Directory domains on page 93
- Validity of group memberships on page 152

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 master 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 which 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.

Detailed information about this topic

- Entering Active Directory account policies on page 94
- Assigning Active Directory account policies to Active Directory user accounts and Active Directory groups on page 96

Related topics

- Password policies for Active Directory user accounts on page 60
- Global account policies for an Active Directory domain on page 89

Entering 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 master data for an account policy

1. Select the **Active Directory | Account policies** category.
2. Select the account policy in the result list and run the **Change master data** task.

   - OR -

   Click **New** in the result list toolbar.
3. Edit the account policy's master data.
4. Save the changes.

Detailed information about this topic

- General master data for an Active Directory account policy on page 95
- How to define a policy on page 95

General master data for an Active Directory account policy

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

Table 29: General master data for 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

- How to define a policy on page 95

How to define a policy

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

Table 30: Master data for a policy definition

Property	Description
Block duration [min]	Block 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

Property	Description
	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 blocked.
Max. password age	Maximum age of the password. Enter the length of time a password can be used before it expires.
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 should be. Complex passwords must fulfill certain minimum prerequisites. For more information, see the documentation for implementing 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 master data for an Active Directory account policy on page 95

Assigning Active Directory account policies to Active Directory user accounts 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. Please refer to your Active Directory documentation on fine-grained account policies under Windows Server for information about the rules for calculating this.

To specify account policies for a user account

1. Select the **Active Directory | Account policies** category.
2. Select the account policy in the result list.
3. Select the **Assign user accounts** task.
4. In **Add assignments** pane, assign user accounts.

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

5. Save the changes.

To specify account policies for a group

1. 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 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.

How to edit a synchronization project

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. Select the **Active Directory | Domains** category.
2. Select the domain in the result list. Select the **Change master data** task.
3. Select the **Edit synchronization project** task.

Related topics

- Customizing the synchronization configuration on page 28

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

Table 31: Effective configuration parameters

Configuration parameter	Meaning
TargetSystem | ADS | MemberShipRestriction | Container	This configuration parameter contains the number of Active Directory objects allowed per container before warning email is sent.
TargetSystem | ADS | MemberShipRestriction | Group	This configuration parameter contains the number of Active Directory objects allowed per group before warning email is sent.
TargetSystem | ADS | MemberShipRestriction | MailNotification	This configuration parameter contain the default email address for sending warnings by email.

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 of monitoring

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.

5

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 receives access to network resources through group membership and access permission.

The managed service accounts introduced in Windows Server 2008 R2 and the group managed service accounts introduced with Windows Server 2012 are not supported in One Identity Manager.

Related topics

- Linking user accounts to employees on page 100
- Supported user account types on page 101
- Entering master data for Active Directory user accounts on page 107

Linking user accounts to employees

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

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

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

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

Related topics

- Entering master data for Active Directory user accounts on page 107
- Account definitions for Active Directory user accounts on page 42
- Automatic assignment of employees to Active Directory user accounts on page 127
- For more detailed information about employee handling and administration, see the *One Identity Manager Target System Base Module Administration Guide*.

Supported user account types

Different types of user accounts, such as default user accounts, administrative user accounts, 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

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

Table 32: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary

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

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

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

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

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

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

- Privileged user account

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

Detailed information about this topic

- Default user accounts on page 103
- Administrative user accounts on page 104

- Providing an administrative user account for one employee on page 104
- Providing an administrative user account for multiple employees on page 105
- Privileged user accounts on page 106

Default user accounts

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

To create default user accounts through account definitions

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

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

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

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

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

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

Related topics

- Account definitions for Active Directory user accounts on page 42

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 employee on page 104
- Providing an administrative user account for multiple employees on page 105

Providing an administrative user account for one employee

Prerequisites

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

To prepare an administrative user account for a person

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

   d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

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

Related topics

- Providing an administrative user account for multiple employees on page 105
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing an administrative user account for multiple employees

Prerequisite

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

To prepare an administrative user account for multiple employees

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

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

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

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

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

Related topics

- Providing an administrative user account for one employee on page 104
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

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

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

To create privileged users through account definitions

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

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

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

- In the mapping rule for the IsPrivilegedAccount column, use the default value **1** and set the **Always use default value** option.
- You can also specify a mapping rule for the IdentityType column. The column owns different permitted values that represent user accounts.
- To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the IsGroupAccount column with a default value of **0** and set the **Always use default value** option.

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

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

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

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

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

- To use a prefix for the login name, in the Designer, set the **TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_Prefix** 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.

Related topics

- Account definitions for Active Directory user accounts on page 42

Entering master data for Active Directory user accounts

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

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

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

To create a user account

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

To edit master data for a user account

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

To manually assign or create a user account for an employee

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

Detailed information about this topic

- General master data of Active Directory user accounts on page 109
- Password data for Active Directory user accounts on page 112
- Profile and home directories on page 114
- Active Directory user account login data
- Remote access service dial-in permissions on page 117
- Connection data for terminal servers on page 118
- Extensions data for an Active Directory user account on page 120
- Further identification data on page 120
- Contact data for an Active Directory user account on page 122

Related topics

- Account definitions for Active Directory user accounts on page 42
- Linking user accounts to employees on page 100
- Supported user account types on page 101

General master data of Active Directory user accounts

Table 33: Configuration parameters for setting up user accounts

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

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

Table 34: General master data for a user account

Property	Description
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click + next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved.
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
First name	The user’s first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user’s last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.

Property	Description
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 employee depending on the manage level of the user account. When the container is selected, the defined name for the user is created using a formatting rule.
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 employee’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: `Logon name (pre Win2000)@ADS Domain name`
Email address	User account email address. If you assigned an account definition, the email address is made up of the employee’s default email address depending on the manage level of the user account.
Additional e-mail addresses	Other email addresses for the user account.
Account expiry date	Account expiry date. Specifying an expiry data for the account has the effect that the logon for this user account is blocked as soon as the given date is exceeded. If you assigned an account definition, the employee’s

Property	Description
	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. By default, you set up user accounts in One Identity Manager with the USER object class. However, the INETORGPERSON object class is also supported, which is used by other LDAP and X.500 directory services for the mapping of user accounts.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative permissions, used by one employee. • **Sponsored identity**: User account that is used for a specific purpose, such as training. • **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • **Service identity**: Service account.
Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.

Property	Description
	- If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Preferred user account	Preferred user account when an employee has several user accounts in Active Directory.
User account is disabled	Specifies whether the user account is disable. If a user account is not required for a period of time, you can temporarily disable the user account by using the <User account is deactivated> option.
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 employee, the user account is unlocked when a new central password is set for the employee. This behavior is controlled by the **TargetSystem | ADS | Accounts | UnlockByCentralPassword** configuration parameter. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Account definitions for Active Directory user accounts on page 42
- Active Directory group inheritance based on categories on page 169
- Linking user accounts to employees on page 100
- Supported user account types on page 101
- Disabling Active Directory user accounts on page 133
- Unlocking Active Directory user accounts on page 123
- Automatic assignment of employees to Active Directory user accounts on page 127

Password data for Active Directory user accounts

Table 35: Configuration parameters for setting up password data

Configuration parameter	Meaning
TargetSystem | ADS | Accounts | NotRequirePassword	The configuration parameter specifies whether a password is required when new Active Directory user accounts are added

Configuration parameter	Meaning
	in One Identity Manager. If the configuration parameter is not set, you are prompted for a password that complies with the defined password policies when a new Active Directory user account is added. If the configuration parameter is set, a password is not required when a new Active Directory user account is added.
TargetSystem | ADS | Accounts | UserMustChangePassword	This configuration parameter defines if the **Change password at next login** option is enabled when a new user account is created.

> 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 master data on the **Password** tab.

Table 36: User account password data

Property	Description
Password	Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use an initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system.
Password confirmation	Reconfirm password.
Password last changed	Data 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. TIP: To enable this option every time new user accounts are created, set the **TargetSystem | ADS | Accounts | UserMustChangePassword** configuration parameter.

Property	Description
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

- Password policies for Active Directory user accounts on page 60
- Initial password for new Active Directory user accounts on page 71
- Global account policies for an Active Directory domain on page 89
- Active Directory account policies for Active Directory domains on page 94
- Assigning Active Directory account policies to an Active Directory user account on page 124

Profile and home directories

Table 37: Configuration parameters for setting up user directories

Configuration parameter	Meaning
QER | Person | User | ConnectHomeDir	This configuration parameter specifies whether the home directory should also be mounted when the user logs in.

Enter the data for the user's home and profile directories.

> 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, set the configuration parameter if necessary.

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.

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

Table 38: Master 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 employee 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 employee depending on the manage level.
Profile share	The share that is stored under the user’s profile directory on the profile server. Default is PROFILES.

Property	Description
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 executed when the user logs in.

Related topics

- Preparing a home server and profile server for creating user directories on page 81

Active Directory user account login data

Enter the following master data on the **Log in** tab.

Table 39: 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. • 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.

Remote access service dial-in permissions

> NOTE: Remote Access Service (RAS) 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 master data on the **RAS** tab.

Table 40: Remote access service

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>Dial-up permitted</td><td>Specifies whether the user may dial up the network. Permitted values are:
<table>
<tr><td>Allow access</td><td>This permits the user to dial up the network.</td></tr>
<tr><td>Deny access</td><td>With this users are not allowed to dial up the network.</td></tr>
<tr><td>Control access through Remote Access Policy</td><td>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.</td></tr>
</table></td></tr>
<tr><td>No callback</td><td>The callback function is switched off by this option.</td></tr>
<tr><td>Set by caller</td><td>The server expects the user to input the number that he can be called back on.</td></tr>
<tr><td>Always callback</td><td>The server tries to call the user back over the given number.</td></tr>
<tr><td>Verifying caller ID</td><td>A predefined number with which the user should dial into the network.</td></tr>
<tr><td>Static IP address</td><td>A fixed IP address assigned to the user.</td></tr>
<tr><td>Static routes with IP address, network address and metric</td><td>Target network IP addresses, network addresses and metrics for dialing in over fixed routes.</td></tr>
</table>

Related topics

- Setting up Active Directory synchronization on page 13

Connection data for terminal servers

Table 41: Configuration parameters for terminal server properties

Configuration parameter	Effect when set
QER | Person | User | ConnectHomeDir	This configuration parameter specifies whether the home directory should also be mounted when the user logs in.

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. If necessary, in the Designer, set the configuration parameter.

Enter the following data on the **Terminal service** tab.

Table 42: Master 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.
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.

Property	Description
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	This option specifies whether remote monitoring or control is enabled for this session.
Get permission of user	You specify 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 person monitoring can input data into the session over the keyboard or the 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 employee 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.
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 employee 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	Name of the home directory for the user under the home share. By

Property	Description
path	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

- Preparing a home server and profile server for creating user directories on page 81

Extensions data for an Active Directory user account

On the **Extensions** tab, you enter the user-defined Active Directory schema extensions for the user account.

Table 43: Extensions 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 identification data

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

Table 44: Master 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

Property	Description
	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 employees 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	Employee's company. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Department	Employee'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 employees 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.
Employee ID	Employee's unique marker, for example their ID.
Employee number	Number for identifying the employee in addition to their ID.
Account manager	Manager responsible for the user account. ***To specify an account manager*** 1. Click → next to the field. 2. In the **Table** menu, 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 132

Contact data for an Active Directory user account

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

Table 45: 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.

Additional tasks for managing Active Directory user accounts

After you have entered the master data, you can run the following tasks.

Overview of Active Directory user accounts

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

To obtain an overview of a user account

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

Changing the manage level of Active Directory user accounts

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

To change the manage level for a user account

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

Related topics

- Entering master data for Active Directory user accounts on page 107

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 employee, the user account is unlocked when a new central password is set for the employee. This behavior is controlled by the **TargetSystem | ADS | Accounts | UnlockByCentralPassword** configuration parameter. For detailed information about an employee’s central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

To unlock a user account manually

1. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. Select the **Unlock user account** task.

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

   The user account is unlocked by One Identity Manager Service.

Related topics

- Entering master data for Active Directory user accounts on page 107

Assigning Active Directory account policies to an Active Directory user account

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. 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 the account policies.

   - OR -

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

Related topics

- Active Directory account policies for Active Directory domains on page 94
- Global account policies for an Active Directory domain on page 89
- Assigning Active Directory account policies directly to an Active Directory group on page 171

Assigning Active Directory groups directly to an Active Directory user account

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

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 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 master data to change its primary group.

Related topics

- Assigning Active Directory groups to Active Directory user accounts, Active Directory contacts, and Active Directory computers on page 154
- Validity of group memberships on page 152
- General master data of Active Directory user accounts on page 109

Assigning secretaries to an Active Directory user account

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. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign secretaries** task.
4. Select the table which contains the user from the menu **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.

   - OR -

In the **Remove assignments** pane, remove secretaries.

6. Save the changes.

Moving an Active Directory user account

> NOTE: User accounts can only be moved within a domain.

To move a user account

1. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master 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** menu on the **General** tab.
7. 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.

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

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

5. Save the changes.

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

Automatic assignment of employees to Active Directory user accounts

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

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

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

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | ADS | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want employees 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 employees shall take place.

  Example:

  ```
  ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $
  ```
- Use the **TargetSystem | ADS | PersonAutoDisabledAccounts** configuration parameter to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the domain. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employees assigned to the domain.

> NOTE:
>
> The following applies for synchronization:
>
> - Automatic employee assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:

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

NOTE:

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

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

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **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** menu, select the account definition.
    d. Select the user accounts that contain the account definition.
    e. Save the changes.

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

Related topics

- Creating an account definition on page 42
- Assigning account definitions to a target system on page 57
- Editing search criteria for automatic employee assignment on page 128

Editing search criteria for automatic employee assignment

The criteria for employee assignments are defined for the domain. In this case, you specify which user account properties must match the employee’s properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (`AccountToPersonMatchingRule`) in the `ADSDomain` table.

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

> NOTE: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.
>
> It is not recommended to make assignments to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user accounts for the respective user account.

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

To specify criteria for employee assignment

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

Table 46: Default search criteria for user accounts and contacts

Apply to	Column for employee	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.

Direct assignment of employees to user accounts based on a suggestion list

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

Table 47: Manual assignment view

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an employee is assigned.
Without employee assignment	This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.

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

To apply search criteria to user accounts

- Click **Reload**.

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

To assign employees directly using a suggestion list

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

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

   – OR –

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

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

To remove assignments

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

       The assigned employees are removed from the selected user accounts.

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

Related topics

- Automatic assignment of employees to Active Directory user accounts on page 127

Updating employees when Active Directory user account are modified

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

Example

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

To update employees 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 employees through subsequent scripting and processing.

> NOTE: When making changes to user accounts, the employees are only updated for user accounts with the **Unmanaged** manage level and that are linked to an employee.

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

User account properties are mapped to employee properties using the `VI_PersonUpdate_ADSAccount` script. Contact properties are mapped to employee properties using the `ADS_PersonUpdate_ADSContact` script. To adjust the mapping more easily, the scripts can be overwritten.

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

```
Public Overrides Function ADS_PersonUpdate_ADSAccount(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 employees of the user accounts as primary department and primary location. These employees can obtain their company resources through these assignments if One Identity Manager is configured correspondingly.

Prerequisites for using this method

Employees 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.

Table 48: Configuration Parameter for Automatic Employee Assignment

Configuration parameter	Effect when set
TargetSystem | ADS | PersonAutoDefault	Automatic employee assignment for user accounts added to the database outside synchronization based on the given mode.
TargetSystem | ADS | PersonAutoFullsync	Automatic employee assignment for user accounts created or updated in the database as a result of the synchronization based on the given mode.

Configuration parameter	Effect when set
TargetSystem | ADS | PersonUpdate	Ongoing update of employee objects 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 identification data on page 120
- Automatic assignment of employees to Active Directory user accounts on page 127
- Updating employees when Active Directory user account are modified on page 131

Disabling Active Directory user accounts

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

Scenario:

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

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

Scenario:

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

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

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

To disable the user account when the configuration parameter is disabled

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

Scenario:

- User accounts not linked to employees.

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

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

For more detailed information about deactivating and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Account definitions for Active Directory user accounts on page 42
- Setting up manage levels on page 45
- Deleting and restoring Active Directory user accounts on page 134

Deleting and restoring Active Directory user accounts

Objects in Active Directorysuch as, for example user accounts, are issued with a unique identification number that is also linked to entitlements. For domains with functional levels below **Windows Server 2008 R2**, when user accounts are deleted in Active Directory, the ID and the associated authorizations are irreversibly lost. This makes it difficult to restore user accounts. For domains from the functional level **Windows Server 2008 R2** and above, user accounts 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 entitlements.

When you configure the synchronization project you define whether, when adding an Active Directory object, 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 below **Windows Server 2008 R2** and therefore no recycling bin is available.

  - OR-

- Have a functional level from **Windows Server 2008 R2** and above but the recycling bin is not activated.

After you have confirmed the security alert, the user account is marked for deletion in One Identity Manager. The user account is locked in One Identity Manager and finally 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 from the functional level **Windows Server 2008 R2**, in which the recycling bin is activated.

After you have confirmed the security alert, the user account is marked for deletion in One Identity Manager. The user account is locked in One Identity Manager and is finally 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.

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

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

To delete a user account

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

To restore a user account

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

When a user accounts is deleted the configuration parameter defining handling of user directories is taken into account.

- Check the configuration parameters and modify them as necessary to suit your requirements.

Table 49: 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 | DeleteOptions | ProfileShare	Deletes the user profile share.
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.

Configuring deferred deletion

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

Related topics

- Disabling Active Directory user accounts on page 133
- Deleting and restoring Active Directory contacts on page 146
- Active Directory security IDs on page 177
- Creating a synchronization project for initial synchronization of an Active Directory domain on page 21
- Active Directory specific master data for Active Directory domains on page 90

6

Active Directory contacts

A contact is a non-security principal. That means a contact cannot log into a domain. A contact, for example, represents a user outside the company and is mainly used for distribution and email purposes.

Related topics

- Entering master data for Active Directory contacts on page 138
- Linking user accounts to employees on page 100
- Supported user account types on page 101

Entering master data for Active Directory contacts

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

> NOTE:
>
> - It is recommended to use account definitions to set up contacts for company employees. If an account definition is used to set up a contact, some of the master data described in the following is composed of the employee's master 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 employees receive their contacts through account definitions, the employees 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 edit contact master data

1. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list and run the **Change master data** task.

   - OR -

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

To manually assign or create a contact for an employee

1. Select the **Employees | Employees** category.
2. Select the employee from the result list and run the **Assign Active Directory contacts** task.
3. Assign a contact.

   - OR -

   Select the **New contact** task and edit the master data.
4. Save the changes.

Detailed information about this topic

- General master data for Active Directory contacts on page 139
- Contact data for Active Directory contacts on page 141
- Further identification data on page 142
- Extensions data for Active Directory contacts on page 143

General master data for Active Directory contacts

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

Table 50: General master data

Property	Description
Employee	Employee who uses the contact. An employee is already entered if the contact was generated by an account definition. If you are using automatic employee assignment, an associated employee is created when you save the contact and added to the contact. If you create the contact manually, you can select an employee in the menu.

Property	Description
Account definition	Account definition through which the contact was created. Use the account definition to automatically populate contact master data and to specify a manage level for the contact. One Identity Manager finds the IT operating data of the assigned employee 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 employee in the **Employee** field. You can select all the account definitions assigned to this employee and through which no contact has been created for this employee.
Manage level	Contact's manage level. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
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.
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. By default, set up contacts with "Contact" in One Identity Manager.
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 employee 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.

Property	Description
Email address	Contact's email address. If you assigned an account definition, the email address is made up of the employee’s default email address depending on the manage level of the user account.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
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 menu.
Description	Text field for additional explanation.
Identity	Contact's type of identity.
Groups can be inherited	Specifies whether the employee's groups are inherited. If this option is set, contacts inherit groups through hierarchical roles. If you add an employee with a contact to an apartment, for example, and you have assigned groups to this department, the contact inherits the groups.

Related topics

- Account definitions for Active Directory user accounts on page 42
- Supported user account types on page 101
- Linking user accounts to employees on page 100
- Active Directory group inheritance based on categories on page 169

Contact data for Active Directory contacts

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

Table 51: Contact data

Property	Description
Phone	Telephone number.
Phone private	Private telephone number.
Fax	Fax number.
Mobile phone	Mobile number.

Property	Description
Pager	Pager number.
Website	Website.
IP telephone number	IP telephone number.
Comment	Text field for additional explanation.

Further identification data

Enter the address data used by this contact for contacting the employee on the **Identification** tab.

Table 52: Master 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	Employee's company.
Department	Employee's department
Job description	Job description.
Employee ID	Employee's unique marker, for example their ID.
Account manager	Manager responsible for the contact. ***To specify an account manager*** 1. Click → next to the field. 2. In the **Table** menu, select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.

Extensions data for Active Directory contacts

On the **Extensions** tab, you enter the user-defined Active Directory schema extensions for the contact.

Table 53: Extensions 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.

Additional tasks for managing Active Directory contacts

After you have entered the master data, you can run the following tasks.

Overview of Active Directory contacts

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

To obtain an overview of a contact

1. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list.
3. Select the **Active Directory contact overview** task.

Changing the manage level of Active Directory contacts

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

To change the manage level for a contact

1. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list.
3. Select the **Change master data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Assigning Active Directory groups directly to an Active Directory contact

Groups can be assigned directly or indirectly to a contact. Indirect assignment is done by allocating the employee and groups into company structures such as departments, cost centers, locations, or business roles. If the employee has a 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. 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 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 154
- Validity of group memberships on page 152

Assigning secretary to an Active Directory contact

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. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list.
3. Select the **Assign secretaries** task.
4. Select the table which contains the user from the **Table** menu 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.

   - OR -

   In the **Remove assignments** pane, remove secretaries.
6. Save the changes.

Moving an Active Directory contact

> Table Cell Outside Table:
> NOTE: Contacts can only be moved within an domain.

To move a contact

1. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list.
3. Select the **Change master 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** menu on the **General** tab.
7. 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.

To assign extended properties for a contact

1. 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.

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

Deleting and restoring Active Directory contacts

One Identity Manager uses various methods to delete contacts. For more information, see Deleting and restoring Active Directory user accounts on page 134.

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

To delete a contact

1. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list.
3. Delete the contact.
4. Confirm the security prompt with **Yes**.

To restore a contact

1. Select the **Active Directory | Contacts** category.
2. Select the contact in the result list.
3. Click **Undo delete** in the result list toolbar.

Configuring deferred deletion

By default, Active Directory contacts are finally deleted from the database after 30 days. During this period you have the option to reactivate the contacts. A restore is not possible once deferred deletion has expired. In the Designer, you can set an alternative delay on the `ADSContact` table.

7

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

  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 groups

  Distribution groups can be used as email-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 authorizations 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 authorizations 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 authorizations available. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.

Related topics

- Entering master data for Active Directory groups on page 149
- Validity of group memberships on page 152

Entering master data for Active Directory groups

To edit group master data

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

Detailed information about this topic

- General master data for Active Directory groupS on page 149
- Extensions data for Active Directory groups on page 151

General master data for Active Directory groupS

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

Table 54: General master 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	The display name is used to display the group in the One Identity Manager tools user interface.
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. By default, you set up groups in One Identity Manager with the object class `GROUP`.

Property	Description
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.
Account manager	Manager responsible for the group. ***To specify an account manager*** 1. Click → next to the field. 2. In the **Table** menu, 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 memberships for these groups.
Email address	Group's email address
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
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 menu.
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.

Property	Description
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 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 by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Service item	Service item data for requesting the group through the IT Shop.

Related topics

- Active Directory group inheritance based on categories on page 169
- For more detailed information about preparing groups for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Extensions data for Active Directory groups

On the **Extensions** tab, you enter the user-defined Active Directory schema extensions for the group.

Table 55: Extensions 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.

Validity of group memberships

There are different assignments to groups possible depending on the construction of the domain structure and the domain trusts. You can find more exact information about permitted group memberships in 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 56: Group memberships permitted within a domain

Target Group		Member in target group								
		Group								
		Distribution			Security			User account	Contact	Computer
		G	U	L	G	U	L			
Distribution	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 57: Group memberships permitted within a hierarchical domain structure

Target Group		Member in target group								
		Group						User account	Contact	Computer
		Distribution			Security					
		G	U	L	G	U	L			
Distribution	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 58: Group memberships permitted within a forest

Target Group		Member in target group								
		Group						User account	Contact	Computer
		Distribution			Security					
		G	U	L	G	U	L			
Distribution	Global									
	Universal									
	Local	x	x		x	x		x		x
Security	Global									
	Universal									
	Local	x	x		x	x		x		x

Table 59: Group memberships permitted between forests

Target Group		Member in target group								
		Group						User account	Contact	Computer
		Distribution			Security					
		G	U	L	G	U	L			
Distribution	Global									
	Universal									
	Local	x	x		x	x		x		x
Security	Global									
	Universal									
	Local	x	x		x	x		x		x

Related topics

- Trusted Active Directory domains on page 93
- Active Directory specific master data for Active Directory domains on page 90

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

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

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

- Assignment of employees and groups is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts and contacts are labeled with the **Groups can be inherited** option.

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

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

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

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

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

Detailed information about this topic

- Assigning Active Directory groups to departments, cost centers and locations on page 155
- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160
- Adding Active Directory groups to system roles on page 161
- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164
- One Identity Manager Identity Management Base Module Administration Guide

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, cost center, or location (role-based login)

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

    - OR -

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

    - OR -

    In the Manager, select the **Organizations | Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign 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 on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160

- Adding Active Directory groups to system roles on page 161
- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164
- One Identity Manager users for managing Active Directory on page 10

Assigning Active Directory groups to business roles

Installed modules: Business Roles Module

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

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

1. In the Manager, select the **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, assign business roles.

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

5. Save the changes.

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

1. In the Manager, select the **Business roles | <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign 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 departments, cost centers and locations on page 155
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160
- Adding Active Directory groups to system roles on page 161
- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164
- One Identity Manager users for managing Active Directory on page 10

Assigning Active Directory user accounts directly to Active Directory groups

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is done by allocating the employee and groups into company structures such as departments, cost centers, locations, or business roles. If the employee has a user account in 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.

To assign a group directly to user accounts

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

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

5. Save the changes.

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

Related topics

- Assigning Active Directory groups directly to an Active Directory user account on page 124
- Assigning Active Directory groups to departments, cost centers and locations on page 155
- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160
- Adding Active Directory groups to system roles on page 161
- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164
- Validity of group memberships on page 152
- General master data of Active Directory user accounts on page 109

Assigning Active Directory contacts directly to an Active Directory group

Groups can be assigned directly or indirectly to a contact. Indirect assignment is done by allocating the employee and groups into company structures such as departments, cost centers, locations, or business roles. If the employee has a 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. 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.

   - OR -

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

Related topics

- Assigning Active Directory groups directly to an Active Directory contact on page 144
- Assigning Active Directory groups to departments, cost centers and locations on page 155

- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory computers directly to an Active Directory group on page 160
- Adding Active Directory groups to system roles on page 161
- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164
- Validity of group memberships on page 152

Assigning Active Directory computers directly to an Active Directory group

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

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

To assign a group directly to computers

1. 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 the computers.

   - OR -

   In the **Remove assignments** pane, remove the computers.
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 master data to change its primary group.

Related topics

- Assigning Active Directory computers directly to Active Directory groups on page 184
- Assigning Active Directory groups to departments, cost centers and locations on page 155
- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159

- Adding Active Directory groups to system roles on page 161
- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164
- Validity of group memberships on page 152
- Master data for an Active Directory computer on page 182

Adding Active Directory groups to system roles

Installed modules:	System Roles Module

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

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

To assign a group to system roles

1. In the Manager, select the **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 assigned system roles.
   >
   > ***To remove an assignment***
   >
   > - Select the system role and double-click ✓.

5. Save the changes.

Related topics

- Assigning Active Directory groups to departments, cost centers and locations on page 155
- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160

- Adding Active Directory groups to the IT Shop on page 162
- Adding Active Directory groups automatically to the IT Shop on page 164

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

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

To add a group to the IT Shop.

1. In the Manager select the **Active Directory | Groups** category (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. In the **Add assignments** pane, assign the group to the IT Shop shelves.
5. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager select the **Active Directory | Groups** category (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. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
5. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **Active Directory | Groups** category (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 detailed information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- General master data for Active Directory groupS on page 149
- Adding Active Directory groups automatically to the IT Shop on page 164
- Assigning Active Directory groups to departments, cost centers and locations on page 155
- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160
- Adding Active Directory groups to system roles on page 161

Adding Active Directory groups automatically to the IT Shop

Table 60: Configuration parameter for automatically add groups in the IT Shop

Configuration parameter	Description
QER | ITShop | GroupAutoPublish	Preprocessor-relevant configuration parameter for automatically adding groups to the IT Shop. This configuration parameter specifies whether all Active Directory and SharePoint target system groups are automatically added to the IT Shop. Changes to this parameter require the database to be recompiled.
QER | ITShop | GroupAutoPublish | ADSGroupExcludeList	This configuration parameter contains a list of all Active Directory groups for which automatic IT Shop assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`

To add groups automatically to the IT Shop

1. In the Designer, set the **QER | ITShop | GroupAutoPublish** configuration parameter.
2. In the Designer, set the **QER | ITShop | GroupAutoPublish | ADSGroupExcludeList** configuration parameter and specify the Active Directory groups that are not to be added automatically to the IT Shop.
3. Compile the database.

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

- Synchronization ensures that the groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor.
- New groups created in One Identity Manager are added to the IT Shop.

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

1. A service item is determined for the group.

   The service item is tested and modified for each group as required. The service item name corresponds to the name of the group. The service item is assigned to one of the default service categories.

   - The service item is modified for groups with service items.
   - Groups without service items are allocated new service items.

2. An application role for product owners is determined and the service item is assigned. Product owners can approve requests for membership in these groups. By default, the group's account manager is established as 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 group 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 group.
   - If the account manager of the group is not yet a member of an application role for product owners, a new application role is created. The name of the application corresponds to the name of the account manager.
     - If the account manager is a user account or a contact, the user account's employee or the contact's employee is added to the application role.
     - If it is a group of account managers, the employees of all this group's user accounts are added to the application role.
   - If the group does not have an account manager, the **Request & Fulfillment | IT Shop | Product owner | Without owner in AD** default application role is used.
3. The group is labeled with the **IT Shop** option and assigned to the **Active Directory Groups** IT Shop shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can request group memberships through the Web Portal.

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

Related topics

- Adding Active Directory groups to the IT Shop on page 162
- Assigning Active Directory groups to departments, cost centers and locations on page 155
- Assigning Active Directory groups to business roles on page 157
- Assigning Active Directory user accounts directly to Active Directory groups on page 158
- Assigning Active Directory contacts directly to an Active Directory group on page 159
- Assigning Active Directory computers directly to an Active Directory group on page 160
- Adding Active Directory groups to system roles on page 161
- Default solutions for requesting Active Directory groups and group memberships on page 173
- One Identity Manager IT Shop Administration Guide

Additional tasks for managing Active Directory groups

After you have entered the master data, you can run the following tasks.

Overview of Active Directory groups

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

To obtain an overview of a group

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

Adding Active Directory groups to Active Directory groups

Use this task to add a group to another group.

To assign groups 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 groups** task.
4. In the **Add assignments** pane, assign the groups that are subordinate to the selected group.

   > 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

- Validity of group memberships on page 152

Effectiveness of group memberships

Table 61: Configuration parameters for conditional inheritance

Configuration parameter	Effect when set
QER | Structures | Inherite | GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. Changes to this parameter require the database to be recompiled.

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

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

NOTE:

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

The effectiveness of the assignments is mapped in the `ADSAccountInADSGroup` and `BaseTreeHasADSGroup` tables by the `XIsInEffect` column.

Example of the effect of group memberships

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

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

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

Table 62: Specifying excluded groups (`ADSGroupExclusion` table)

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

Table 63: Effective assignments

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

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

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

Table 64: Excluded groups and effective assignments

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

Prerequisites

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

To exclude a group

1. In the Manager, select the **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 not 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 31** category positions.

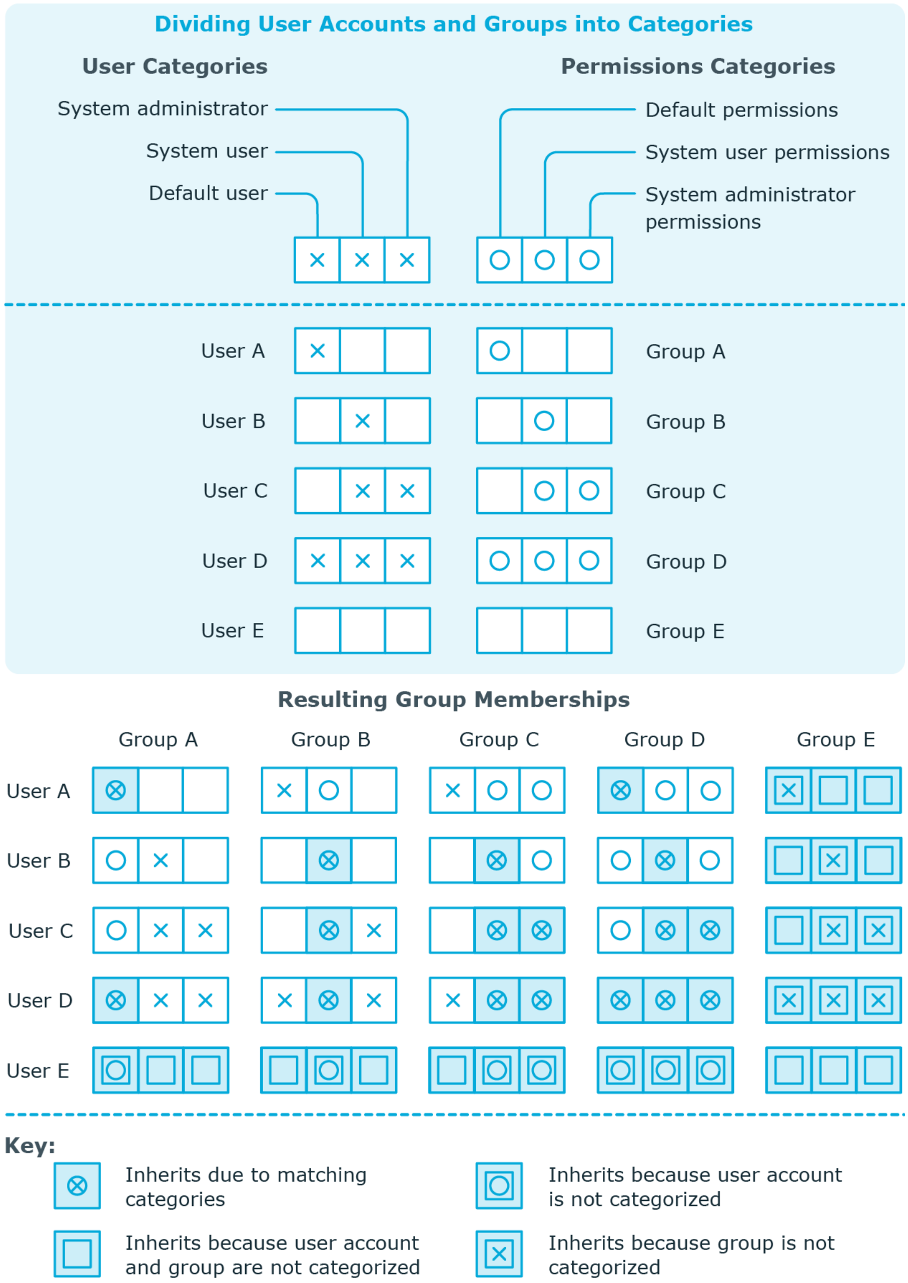
Every user account (contact) can be assigned to one or more categories. Each group can also be assigned to one or more categories. If at least one user account (contact) category position matches an assigned structural profile, the structural profile is inherited by the user account (contact). If the 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 65: 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.


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

To use inheritance through categories

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

Related topics

- Specifying categories for inheriting Active Directory groups on page 92
- General master data of Active Directory user accounts on page 109
- General master data for Active Directory contacts on page 139
- General master data for Active Directory groupS on page 149

Assigning Active Directory account policies directly to an Active Directory group

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. Select **Active Directory | Groups**.
2. Select the group in the result list.
3. Select the **Assign account policies** task.
4. In the **Add assignments** pane, assign the account policies.

   - OR -

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

Related topics

- Active Directory account policies for Active Directory domains on page 94
- Global account policies for an Active Directory domain on page 89
- Assigning Active Directory account policies to an Active Directory user account on page 124

Assigning secretaries to an Active Directory group

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. 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 menu **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.

   - OR -

   In the **Remove assignments** pane, remove secretaries.
6. Save the changes.

Moving an Active Directory group

NOTE: You can only move groups within a domain.

To move a group

1. Select the **Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Change master 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** menu on the **General** tab.
7. 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.

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

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

5. Save the changes.

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

Deleting Active Directory groups

To delete an Active Directory group

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

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

> NOTE: When a group is deleted, an entry is created in One Identity Manager for the Active Directory SID. For more information, see Active Directory security IDs on page 177.

Default solutions for requesting Active Directory groups and group memberships

In One Identity Manager, default 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 detailed information, see the *One Identity Manager Web Portal User Guide*.

Detailed information about this topic

- Adding Active Directory groups on page 174
- Changing Active Directory groups on page 175
- Deleting Active Directory groups on page 175
- Active DirectoryRequesting Groups Memberships on page 176

Adding Active Directory groups

By requesting this default 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

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

If the **QER | ITShop | GroupAutoPublish** 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 66: 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

Detailed information about this topic

- Adding Active Directory groups automatically to the IT Shop on page 164

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

Table 67: 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.
- Employees are assigned to the **Target systems | Active Directory** application role.

Table 68: 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

Table 69: Default objects for requesting group memberships

Shelves:	Identity & Access Lifecycle | Active Directory groups
Approval policies/approval workflows	Approval of Active Directory group membership requests

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.

Related topics

- Adding Active Directory groups automatically to the IT Shop on page 164
- Adding Active Directory groups on page 174

8

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

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

- 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.

9

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. These are only taken into account in the synchronization when the relevant configuration option is set.

Setting up Active Directory containers

To edit container master data

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

   - OR -

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

Detailed information about this topic

- Master data for an Active Directory container on page 178

Master data for an Active Directory container

Enter the following data for a container.

Table 70: Master 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. Click → next to the field. 2. In the **Table** menu, select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.
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.

Property	Description
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 this option is set, delete permissions are removed from the container object.

Related topics

- Target system managers on page 73

Additional tasks for managing Active Directory containers

After you have entered the master data, you can run the following tasks.

Overview of Active Directory containers

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

To obtain an overview of a container

1. Select the **Active Directory | Container** category.
2. Select the container in the result list.
3. Select the **Active Directory container overview** task.

Moving an Active Directory container

> NOTE: You can only move containers within a domain.

To move a container

1. Select the **Active Directory | Container** category.
2. Select the container in the result list.
3. Select the **Change master 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** menu on the **General** tab.
7. Save the changes.

10

Active Directory computers

Computers and servers are loaded into One Identity Manager by synchronization.

To edit computer master data

1. Select the **Active Directory | Computers** category.
2. Select the computer in the result list and run the **Change master data** task.

   - OR -

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

Related topics

- Master data for an Active Directory computer on page 182
- Editing a server on page 75

Master data for an Active Directory computer

Enter the following data for a computer.

Table 71: Computer master data

Property	Description
Device	The computer is connected to this device. Specify a new device using the + button next to the menu. For detailed information about rule checking, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Property	Description
Name	Computer identifier
Domain	Domain in which to create the computer.
Container	Container in which to create the computer. The distinguished name of the computer is determined by a template when the container is selected.
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. Click → next to the field. 2. In the **Table** menu, 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.
Hotfix operating system	Hotfix identifier.

Additional tasks for managing Active Directory computers

After you have entered the master data, you can run the following tasks.

Overview of Active Directory computers

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

To obtain an overview of a computer

1. Select the **Active Directory | Computers** category.
2. Select the computer in the result list.
3. Select the **Active Directory computer overview** task.

Moving an Active Directory computer

NOTE: Computers can only be moved within an domain.

To move a computer

1. Select the **Active Directory | Computers** category.
2. Select the computer in the result list.
3. Select the **Change master 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** menu on the **General** tab.
7. Save the changes.

Assigning Active Directory computers directly to Active Directory groups

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

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

To assign a computer directly to groups

1. Select the **Active Directory | Computers** category.
2. Select the computer in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign groups.

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

5. Save the changes.

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

Related topics

- Assigning Active Directory groups to Active Directory user accounts, Active Directory contacts, and Active Directory computers on page 154
- Validity of group memberships on page 152
- Master data for an Active Directory computer on page 182

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.

Table 72: Diagnostics tasks

Task	Description
Diagnostics - Browse	This opens a Window Explorer window. All shares for the selected computer are shown.
Diagnostics - Windows Diagnostics	This opens the system information (`winmsd.exe` or `msinfo32.exe`) for the computer.
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.

To run diagnostics for a computer

1. Select the **Active Directory | Computers** category.
2. Select the computer and run the required diagnosis task from the task view.

11

Active Directory printers

All shared printers of a domain are read into One Identity Manager during synchronization.

To display a printer

1. Select the **Active Directory | Printers** category.
2. In the result list, select a printer then select the **Change master data** task.

Following information is displayed for a printer.

Table 73: Printer master 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	Defines whether the printer supports a sorter.
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.

12

Active Directory locations

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

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

To display location information

1. Select the **Active Directory | Locations** category.
2. Select the location in the result list.
3. To display a location's server, select the **Location overview** task.
4. To display a location's master data, select the **Change master data** task.

Following information about locations is displayed.

Table 74: Location master data

Property	Description
Name	Location name.
Canonical name	The location'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 location belongs.
Subnets	IP address range at this location.

Related topics

- Information about the Active Directory forest on page 92

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 75: Reports for the target system

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

Report	Description
Active Directory user account and group administration	This report contains a summary of user account and group distribution in all domains. You can find this report in **My One Identity Manager**.
Data quality summary for Active Directory user accounts	This report contains different evaluations of user account data quality in all domains. You can find this report in **My One Identity Manager**.

Related topics

- Overview of all assignments on page 191

Overview of all assignments

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

Examples

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

To display detailed information about assignments

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

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

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

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

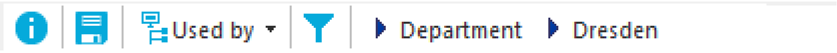


Table 76: Meaning of icons in the report toolbar

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

Appendix A

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 77: Configuration parameter

Configuration parameters	Description
QER | ITShop | GroupAutoPublish	Preprocessor relevant configuration parameter for automatically adding groups to the IT Shop. This configuration parameter specifies whether all Active Directory and SharePoint target system groups are automatically added to the IT Shop. Changes to this parameter require the database to be recompiled.
QER | ITShop | GroupAutoPublish | ADSGroupExcludeList	This configuration parameter contains a list of all groups for which automatic IT Shop assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
TargetSystem | ADS	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system Active Directory. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
TargetSystem | ADS | Accounts	This configuration parameter permits configuration of user account data.
TargetSystem | ADS | Accounts |	This configuration parameter specifies whether a random generated password is issued when a new user account is

Configuration parameters	Description
InitialRandomPassword	added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee's manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter **TargetSystem | ADS | DefaultAddress**.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The **Employee - new user account created** mail template is used.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem | ADS | Accounts | MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | ADS | Accounts | NotRequirePassword	The configuration parameter specifies whether a password is required when new Active Directory user accounts are added in One Identity Manager. If the configuration parameter is not set, you are prompted for a password that complies with the defined password policies when a new Active Directory user account is added. If the configuration parameter is set, a password is not required when a new Active Directory user account is added.
TargetSystem | ADS | Accounts | PrivilegedAccount	This configuration parameter allows configuration of settings for privileged Active Directory user accounts.
TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_Postfix	This configuration parameter contains the postfix for formatting login names for privileged user accounts.

Configuration parameters	Description
TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_ Prefix	This configuration parameter contains the prefix for formatting login names for privileged user accounts.
TargetSystem | ADS | Accounts | ProfileFixedString	This configuration parameter contains a fixed character string that is appended to the user profile's default profile path.
TargetSystem | ADS | Accounts | TransferJPegPhoto	This configuration parameter specifies whether changes to the employee's picture are published in existing user accounts. The picture is not part of default synchronization. It is only published when employee data is changed.
TargetSystem | ADS | Accounts | TransferSIDHistory	This configuration parameter specifies whether the history of an SID is loaded from the target system.
TargetSystem | ADS | Accounts | TSProfileFixedString	This configuration parameter contains a fixed character string, which is appended to the user profile's default profile path on a terminal server.
TargetSystem | ADS | Accounts | UnlockByCentralPassword	This configuration parameter specifies whether the employee’s Active Directory user account is also blocked by synchronizing the central password.
TargetSystem | ADS | Accounts | UserMustChangePassword	This configuration parameter defines if the **Change password at next login** option is enabled when a new user account is created.
TargetSystem | ADS | AuthenticationDomains	This configuration parameter contains a pipe (|) delimited list of domains to be used by the manual Active Directory authentication module to authenticate users. The list is processed in the given order. This list should only contain domains to be synchronized. Example: `MyDomain|MyOtherDomain` For detailed information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
TargetSystem | ADS | AutoCreateDepartment	This configuration parameter specifies whether departments are automatically created when user accounts are modified or synchronized.

Configuration parameters	Description
TargetSystem | ADS | AutoCreateLocality	This configuration parameter specifies whether locations are automatically created when user accounts are modified or synchronized.
TargetSystem | ADS | AutoCreateHardwaretype	This configuration parameter specifies whether corresponding device types are created automatically in the database for imported printer objects.
TargetSystem | ADS | AutoCreateServers	This configuration parameter specifies whether entries for missing home servers and profile servers are created automatically when user accounts are synchronized.
TargetSystem | ADS | AutoCreateServers | PreferredLanguage	This configuration parameter contains the referred language for automatically created servers.
TargetSystem | ADS | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem | ADS | HardwareInGroupFromOrg	The configuration parameter specifies whether computers are added to groups on the basis of group assignment to roles.
TargetSystem | ADS | MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem | ADS | MembershipAssignCheck	When assigning group memberships in the One Identity Manager database, this configuration parameter specifies whether permissibility of the membership is verified at the time of saving. 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.
TargetSystem | ADS | MemberShipRestriction | Container	This configuration parameter contains the number of Active Directory objects allowed per container before warning email is sent.
TargetSystem | ADS | MemberShipRestriction | Group	This configuration parameter contains the number of Active Directory objects allowed per group before warning email is sent.
TargetSystem | ADS |	This configuration parameter contain the default email address

Configuration parameters	Description
MemberShipRestriction | MailNotification	for sending warnings by email.
TargetSystem | ADS | PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | ADS | PersonAutoDisabledAccounts	This configuration parameter specifies whether employees are automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
TargetSystem | ADS | PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem | ADS | PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. 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	This configuration parameter specifies whether employees are updated if their user accounts are changed. This configuration parameter is set to allow ongoing update of employee objects from associated user accounts.
TargetSystem | ADS | ReplicateImmediately	This configuration parameter is used to speed up synchronization of modifications between two domain controllers. When set, the accumulated modifications in Active Directory are immediately replicated between domain controllers.
TargetSystem | ADS | VerifyUpdates	This configuration parameter specifies whether modified properties are checked by updating. If this parameter is set, the objects in the target system are verified after every update.

Appendix B

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 template uses mappings for the following schema types.

Table 78: 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
printQueue	ADSPrinter
serverInSite	ADSMachineInADSSite

Schema type in Active Directory	Table in the One Identity Manager Schema
site	ADSSite
trustedDomain	DomainTrustsDomain
user	ADSAccount

About us

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

Contacting us

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

Technical support resources

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

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

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

Index