One Identity Manager 8.1.1

Administration Guide for Connecting to Active Directory
Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

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

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

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

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

Patents

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

Trademarks

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

Legend

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

One Identity Manager Administration Guide for Connecting to Active Directory
Updated - August 2019
Version - 8.1.1
## Contents

**Managing an Active Directory environment** .......................................................... 9  
Architecture overview ................................................................................................ 9  
One Identity Manager users for managing an Active Directory environment ............ 10

**Setting up synchronization with an Active Directory environment** ..................... 13

User names and permissions for synchronizing with Active Directory ....................... 14  
Communications ports and firewall configuration ................................................. 17  
Setting up the synchronization server ....................................................................... 18  
Creating a synchronization project for initial synchronization of an Active Directory domain ................................................................................................................................................................. 21  
Displaying synchronization results ............................................................................. 28  
Customizing synchronization configuration ............................................................ 28  
  - Configuring synchronization in Active Directory domains ................................ 30  
  - Configuring synchronization of several Active Directory domains ..................... 30  
  - Updating schemas .......................................................................................... 31  
Speeding up synchronization with revision filtering .................................................. 32  
Post-processing outstanding objects ......................................................................... 33  
Configuring the provisioning of memberships ............................................................ 35  
Help for the analysis of synchronization issues .......................................................... 36  
Deactivating synchronization ....................................................................................... 37

**Basic data for managing an Active Directory environment** .................................. 38

Account definitions for Active Directory user accounts ............................................. 40  
  - Creating an account definition ....................................................................... 40  
  - Master data for an account definition ............................................................. 41  
Setting up manage levels ............................................................................................ 43  
  - Master data for a manage level ...................................................................... 44  
Creating a mapping rule for IT operating data ............................................................ 45  
Determining IT operating data .................................................................................. 47  
Modify IT operating data ............................................................................................ 48  
Assigning account definitions to employees .............................................................. 49  
  - Assigning account definitions to departments, cost centers, and locations ....... 50  
  - Assigning account definitions to business roles ............................................. 51
Information about the Active Directory forest ................................................................. 90
Trusted Active Directory domains .................................................................................. 91
Active Directory account policies for Active Directory domains ..................................... 92
Entering Active Directory account policies ..................................................................... 92
  General master data for an Active Directory account policy ......................................... 93
  How to Define a Policy ................................................................................................... 93
Assigning Active Directory account policies to Active Directory user accounts and Active Directory groups ............................................................. 94
Editing a synchronization project ................................................................................... 95
Monitoring the number of memberships in Active Directory groups and Active Directory containers .............................................................................................................. 96

Active Directory user accounts ....................................................................................... 98
Linking user accounts to employees ............................................................................... 98
Supported user account types .......................................................................................... 99
  Default user accounts ................................................................................................... 101
  Administrative user accounts ...................................................................................... 102
    Providing an administrative user account for one employee ..................................... 102
    Providing an administrative user account for multiple employees ......................... 103
  Privileged user accounts .............................................................................................. 104
Entering master data for Active Directory user accounts .............................................. 105
  General master data of an Active Directory user account ........................................... 107
Password data for Active Directory user accounts ......................................................... 111
Profile and home directories ............................................................................................ 113
Active Directory user account login data ...................................................................... 114
Remote access service dial-in permissions ..................................................................... 115
Connection data for terminal servers .............................................................................. 116
Extensions data for an Active Directory user account ..................................................... 118
Further identification data ............................................................................................... 119
Contact data for an Active Directory user account ......................................................... 120
Additional tasks for managing Active Directory user accounts ..................................... 121
  Overview of Active Directory user accounts ................................................................ 121
  Changing the manage level of an Active Directory user account ................................ 121
Unlocking Active Directory user accounts ..................................................................... 122
Assigning Active Directory account policies to an Active Directory user account ....... 122
Assigning Active Directory groups directly to an Active Directory user account ......... 123
Assigning wizards to an Active Directory user account ........................................124
Moving an Active Directory user account ............................................................124
Assigning extended properties to an Active Directory user account .................125
Automatic assignment of employees to Active Directory user accounts ..........125
Editing search criteria for automatic employee assignment ..............................127
Updating employees when Active Directory user accounts are modified ..........130
Automatic creation of departments and locations based on user account information 131
Disabling Active Directory user accounts ..........................................................132
Deleting and restoring Active Directory user accounts ....................................133

**Active Directory contacts** .............................................................................137
Entering master data for Active Directory contacts ............................................137
General master data for Active Directory contacts ..........................................138
Contact data for Active Directory contacts .......................................................140
Further identification data ................................................................................141
Extensions data for an Active Directory contact ..............................................142
Additional tasks for managing Active Directory contacts ................................142
Overview of Active Directory contacts ..............................................................142
Changing the manage level of an Active Directory contact ............................142
Assigning Active Directory groups directly to an Active Directory contact ....143
Assigning a secretary to an Active Directory contact ......................................144
Moving an Active Directory contact ...............................................................144
Assigning extended properties to an Active Directory contact .....................145
Deleting and restoring Active Directory contacts .............................................145

**Active Directory groups** .............................................................................147
Entering master data for Active Directory groups ............................................148
General master data for an Active Directory group .........................................148
Extensions data for Active Directory groups ....................................................150
Validity of group memberships .........................................................................151
Assigning Active Directory groups to Active Directory user accounts, Active
Directory contacts and Active Directory computers .........................................153
Assigning Active Directory groups to departments, cost centers, and locations ..154
Assigning Active Directory groups to business roles ......................................156
Assigning Active Directory user accounts directly to an Active Directory group 157
Assigning Active Directory contacts directly to an Active Directory group ........158
Assigning Active Directory computers directly to an Active Directory group ....159
Adding Active Directory groups to system roles ........................................... 160
Adding Active Directory groups to the IT Shop ........................................... 161
Adding Active Directory groups automatically to the IT Shop ......................... 162
Additional tasks for managing Active Directory groups .................................. 164
Overview of Active Directory groups ......................................................... 165
Adding Active Directory groups to Active Directory groups ......................... 165
Effectiveness of group memberships ......................................................... 166
Active Directory group inheritance based on categories ............................... 168
Assigning Active Directory account policies directly to an Active Directory group ... 170
Assigning a secretary to an Active Directory group ....................................... 171
Moving an Active Directory group ........................................................... 171
Assigning extended properties to an Active Directory group ......................... 172
Deleting Active Directory groups ............................................................. 172

Active Directory security IDs ...................................................................... 173

Active Directory container hierarchies ....................................................... 174
Setting up Active Directory containers ...................................................... 174
  Master data for an Active Directory container ......................................... 174
Additional tasks for managing Active Directory containers ......................... 176
  Overview of Active Directory containers ............................................... 176
  Moving an Active Directory container ................................................. 176

Active Directory computers ...................................................................... 178
Master data for an Active Directory computer ........................................... 178
Additional tasks for managing Active Directory computers ......................... 179
  Overview of Active Directory computers ............................................... 180
  Moving an Active Directory computer ................................................. 180
  Assigning Active Directory computers directly to Active Directory groups .... 180
Performing computer diagnostics .............................................................. 181

Active Directory printers ........................................................................... 182

Active Directory locations ......................................................................... 184

Active Directory object reports ................................................................... 185
Overview of all assignments ....................................................................... 186

Appendix: Configuration parameters for managing Active Directory ............... 188
Managing an Active Directory environment

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

One Identity Manager provides company employees with the necessary user accounts. For this, you can use different mechanisms to connect 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

The following servers are used for managing an Active Directory environment in One Identity Manager:

- **Active Directory domain controller**
  Domain controller with which the synchronization of the Active Directory objects runs. The synchronization server connects to this server in order to access the Active Directory objects.

- **Synchronization server**
  The synchronization server for synchronizing the One Identity Manager database with the Active Directory system. The One Identity Manager Service is installed on this server with the Active Directory connector. 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 an Active Directory environment

The following users are used in Active Directory system administration.

Table 1: Users

<table>
<thead>
<tr>
<th>Users</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target system administrators</td>
<td>Target system administrators must be assigned to the **Target systems</td>
</tr>
<tr>
<td></td>
<td>* Administrate application roles for individual target systems types.</td>
</tr>
<tr>
<td></td>
<td>* Specify the target system manager.</td>
</tr>
<tr>
<td></td>
<td>* Set up other application roles for target system managers if required.</td>
</tr>
<tr>
<td>Users</td>
<td>Task</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
</tbody>
</table>
| Users | • Specify which application roles for target system managers are mutually exclusive.  
|       | • Authorize other employee 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 **Target systems | Active Directory** or a sub-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 for adding to the IT Shop.  
|       | • Can add employees, who have an other identity than the **Primary identity**.  
|       | • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.  
|       | • Edit the synchronization's target system types and outstanding objects.  
|       | • Authorize other employees within their area of responsibility as target system managers and create child application roles if required. |
| One Identity Manager administrators | • Create customized permissions groups for application roles for role-based login to administration tools in Designer as required.  
|       | • Create system users and permissions groups for non-role-based login to administration tools in Designer as required.  
|       | • Enable or disable additional configuration parameters in Designer as required.  
|       | • Create custom processes in Designer as required.  
|       | • Create and configure schedules as required.  
<p>|       | • Create and configure password policies as required. |
| Administrators for the IT Shop | Administrators must be assigned to the <strong>Request &amp; Fulfillment | IT Shop | Administrators</strong> application role. |</p>
<table>
<thead>
<tr>
<th>Users</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users with this application role:</td>
<td></td>
</tr>
<tr>
<td>- Assign groups to IT Shop structures.</td>
<td></td>
</tr>
<tr>
<td>Product owner for the IT Shop</td>
<td>Product owners must be assigned to the **Request &amp; Fulfillment</td>
</tr>
<tr>
<td>- Approve through requests.</td>
<td></td>
</tr>
<tr>
<td>- Edit service items and service categories under their management.</td>
<td></td>
</tr>
<tr>
<td>Administrators for organizations</td>
<td>Administrators must be assigned to the application role **Identity Management</td>
</tr>
<tr>
<td>- Assign groups to departments, cost centers and locations.</td>
<td></td>
</tr>
<tr>
<td>Business roles administrators</td>
<td>Administrators must be assigned to the application role **Identity Management</td>
</tr>
<tr>
<td>- Assign groups to business roles.</td>
<td></td>
</tr>
</tbody>
</table>
Setting up synchronization with an Active Directory environment


To load objects from an Active Directory environment 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.
   - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
   - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with 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
- Deactivating synchronization on page 37
- Customizing synchronization configuration on page 28

One Identity Manager 8.1.1 Administration Guide for Connecting to Active Directory
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

<table>
<thead>
<tr>
<th>Users</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User for accessing Active Directory</td>
<td>For full synchronization of Active Directory objects with the supplied One Identity Manager default configuration, you must provide a user account with the following permissions.</td>
</tr>
<tr>
<td></td>
<td>- Member of the Active Directory Group <strong>Domain administrators</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> In a hierarchical domain structure, the user account of the One Identity Manager Service of a child domain must be a member of the <strong>Enterprise Admins</strong> group.</td>
</tr>
<tr>
<td></td>
<td>We cannot recommend any practical minimum configuration with different permissions in terms of user administration from a member of the group <strong>Domain administrators</strong>.</td>
</tr>
<tr>
<td>One Identity Manager Service user account</td>
<td>The user account for One Identity Manager Service requires rights to carry out operations at file level, for example, assigning user rights and creating and editing directories and files.</td>
</tr>
<tr>
<td></td>
<td>The user account must belong to the <strong>Domain users</strong> group.</td>
</tr>
<tr>
<td></td>
<td>The user account must have the <strong>Login as a service</strong> extended user right.</td>
</tr>
<tr>
<td></td>
<td>The user account requires access rights to the internal web service.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If One Identity Manager Service runs under the network service (<strong>NT Authority\NetworkService</strong>), you can issue access rights for the internal web service with the following command line call:</td>
</tr>
<tr>
<td></td>
<td><code>netsh http add urlacl url=http://&lt;IP address&gt;:&lt;port number&gt;/ user=&quot;NT AUTHORITY\NETWORKSERVICE&quot;</code></td>
</tr>
<tr>
<td></td>
<td>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>In the default installation the One Identity Manager is installed under:</td>
</tr>
</tbody>
</table>
### Users Permissions

- `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems)
- `%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 for executing 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 the One Identity Manager:

- Read All Properties
- Write All Properties
Essentially user account functionality is partially stored as an entry in the permissions list (DACL) of an Active Directory object. It is necessary that the One Identity Manager Service user account can 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 administration tools of the One Identity Manager 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

<table>
<thead>
<tr>
<th>Default port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>Port for communicating with the One Identity Manager database.</td>
</tr>
<tr>
<td>1880</td>
<td>Port for the HTTP protocol of One Identity Manager Service.</td>
</tr>
<tr>
<td>2880</td>
<td>Port for access tests with the Synchronization Editor, such as in the target system browser or for simulating synchronization.</td>
</tr>
<tr>
<td>80</td>
<td>Port for accessing web applications.</td>
</tr>
<tr>
<td>88</td>
<td>Kerberos authentication system. (if Kerberos authentication is implemented). Required for authentication against Active Directory.</td>
</tr>
<tr>
<td>135</td>
<td>Microsoft End Point Mapper (EPMAP) (also, DCE/RPC Locator Service).</td>
</tr>
<tr>
<td>137</td>
<td>NetBIOS Name Service.</td>
</tr>
<tr>
<td>139</td>
<td>NetBIOS Session Service.</td>
</tr>
<tr>
<td>445</td>
<td>Microsoft-DS Active Directory, Windows shares. Required for synchronization (TCP/UDP)</td>
</tr>
<tr>
<td>53</td>
<td>Domain Name System (DNS), mainly through UDP. Required for access to the Active Directory total structure.</td>
</tr>
<tr>
<td>3268</td>
<td>Global catalog. Required for searching in the global catalog. Either port 3268 or 3269 should be open depending on the connection settings.</td>
</tr>
<tr>
<td>3269</td>
<td>Global catalog over SSL. Required for searching in the global catalog. Either port 3268 or 3269 should be open depending on the connection settings.</td>
</tr>
</tbody>
</table>
Setting up the synchronization server

To set up synchronization with an Active Directory environment a server has to be available on which the following software is installed:

- Windows operating system
  Following versions are supported:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- 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 **Select installation modules with existing database**.
    2. Select the machine role **Server | Job server | Active Directory**.

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

  **NOTE:** If several target system environments of the same type are synchronized under the same synchronization server, it is useful to set up a Job server for each target system on performance grounds. This avoids unnecessary swapping of 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:

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

  **NOTE:** The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.
For remote installation of One Identity Manager Service, you require 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 install and configure One Identity Manager Service remotely on a server**

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the **Database connection** page.
3. Specify the server on which you want to install One Identity Manager Service on the **Server properties** page.
   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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>Job server name.</td>
</tr>
<tr>
<td><strong>Queue</strong></td>
<td>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 exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.</td>
</tr>
<tr>
<td><strong>Full server name</strong></td>
<td>Full server name in accordance with DNS syntax. Example: &lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</td>
</tr>
</tbody>
</table>

**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 Designer.

4. Select **Active Directory** on the **Machine roles** page.
5. Select **Active Directory connector** on the **Server functions** page.
6. Check the One Identity Manager Service configuration on the **Service settings** page.

**NOTE:** The initial service configuration is predefined already. 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.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on **Select installation source**.
10. Select the file with the private key on the page **Select private key file**.

   **NOTE:** This page is only displayed when the database is encrypted.
11. Enter the service's installation data on the **Service access** page.

### Table 5: Installation data

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Server on which to install and start the service from.</td>
</tr>
<tr>
<td></td>
<td><strong>To select a server</strong></td>
</tr>
<tr>
<td></td>
<td>- Enter a name for the server.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Select a entry from the list.</td>
</tr>
<tr>
<td>Service account</td>
<td>User account data for the One Identity Manager Service.</td>
</tr>
<tr>
<td></td>
<td><strong>To enter a user account for the One Identity Manager Service</strong></td>
</tr>
<tr>
<td></td>
<td>- Set the option <strong>Local system account</strong>.</td>
</tr>
<tr>
<td></td>
<td>This starts the One Identity Manager Service under the <strong>NT AUTHORITY\SYSTEM</strong> account.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Enter user account, password and password confirmation.</td>
</tr>
<tr>
<td>Installation account</td>
<td>Data for the administrative user account to install the service.</td>
</tr>
<tr>
<td></td>
<td><strong>To enter an administrative user account for installation</strong></td>
</tr>
<tr>
<td></td>
<td>- Enable <strong>Advanced</strong>.</td>
</tr>
<tr>
<td></td>
<td>Enable <strong>Current user</strong>.</td>
</tr>
<tr>
<td></td>
<td>This uses the user account of the current user.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Enter user account, password and password confirmation.</td>
</tr>
</tbody>
</table>

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 Server Installer.

   **NOTE:** The service is entered with the name **One Identity Manager Service** in the server service management.
Creating a synchronization project for initial synchronization of an Active Directory domain

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

1. **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 6: Information Required for Setting up a Synchronization Project

<table>
<thead>
<tr>
<th>Data</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full domain name</td>
<td>Full domain name. Example: Docu.Testlab.dd</td>
</tr>
<tr>
<td>User account and password for domain login</td>
<td>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.</td>
</tr>
<tr>
<td>DNS name of the domain controller.</td>
<td>Full name of the domain controller for connecting to the synchronization server to provide access to Active Directory objects. Example: Server.Doku.Testlab.dd</td>
</tr>
<tr>
<td>Communications port on the domain controller</td>
<td>Communications port on the domain controller. LDAP default communications port is 389.</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 authentication type Secure is used by default. For more information about authentication types, see the MSDN</td>
</tr>
</tbody>
</table>
Synchronization server for Active Directory

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 connector.

The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.

Table 7: Additional properties for the Job server

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server function</td>
<td>Active Directory connector</td>
</tr>
<tr>
<td>Machine role</td>
<td>Server/Jobserver/Active Directory</td>
</tr>
</tbody>
</table>

For more information, see Setting up the synchronization server on page 18.

One Identity Manager database connection data

- 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.

Remote connection server

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

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
### Data

<table>
<thead>
<tr>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• RemoteConnectPlugin is installed</td>
</tr>
<tr>
<td>• Active Directory connector is installed</td>
</tr>
<tr>
<td>• Target system specific components are installed</td>
</tr>
</tbody>
</table>

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 you configure a synchronization project if Synchronization Editor is both:

- executed In default mode, and
- started from the launchpad

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

### To set up an initial synchronization project for a Active Directory domain.

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

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

2. Select **Target system type Active Directory** 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 Synchronization Editor, you do not need to make any settings.
   - If access is not possible from the workstation on which you started 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.
   - Enter the user account and password for logging into the target system.
   - 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 authentication type **Secure** is used by default.
   - In the **Enter or select domain controller** view, you define the domain controller.
     - In the **Domain controller** menu, select an existing domain controller or enter the full name of the domain controller directly.
     - In the **Port** input field, enter the communications port on the domain controller. LDAP default communications port is 389.
     - With the **Use SSL** option, define whether a secure connection should be used.
     - 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 8: Additional settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When restoring objects with the same Distinguished Name or GUID from the recycle bin.</td>
<td>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.</td>
</tr>
<tr>
<td>Allow read and write access to Remote Access Service (RAS) properties.</td>
<td>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.</td>
</tr>
<tr>
<td>Allow read and write access to the terminal service properties.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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, you specify how system access should work. You have the following options:

    **Table 9: Specify target system access**

    | Option                           | Meaning                                                                 |
    |----------------------------------|-------------------------------------------------------------------------|
    | Read-only access to target system. | Specifies whether a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: |
    |                                  |   - Synchronization is in the direction of **One Identity Manager**. |
    |                                  |   - Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**. |
    | Read/write access to target system. Provisioning available. | Specifies whether a provisioning workflow is 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. Select the synchronization server to execute synchronization on the **Synchronization server** page.

    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 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 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 under **Configuration | Variables** in Synchronization Editor.

---

**To configure the content of the synchronization log**

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

**NOTE:** Some content generates a particularly large volume of log data. The synchronization log should only contain data required for troubleshooting and other analyses.

7. Click **OK**.

---

**To synchronize on a regular basis**

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

6. Click **OK**.

**To start initial synchronization manually**

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

---

**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 the account definition and manage level to user accounts in **linked** status.
   a. In Manager, select **Active Directory | User accounts | Linked but not configured | <Domain>**.
   b. **OR**
   c. In Manager, select **Active Directory | Contacts | Linked but not configured | <Domain>**.
   d. Select **Assign account definition to linked accounts**.

---

**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 synchronization configuration](#) on page 28
- [Speeding up synchronization with revision filtering](#) on page 32
- [Appendix: Default project template for Active Directory](#) on page 193
- [Account definitions for Active Directory user accounts](#) on page 40
- [Automatic assignment of employees to Active Directory user accounts](#) on page 125
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 Logs.
3. Click ⬆ in the navigation view toolbar.
   Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking on it.
   An analysis of the synchronization is shown as a report. You can save the report.

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs
- In Designer, enable the DPR | Journal | LifeTime configuration parameter and enter the maximum retention period.

Customizing synchronization configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization of an Active Directory domain. You can use this 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 in order to compare the Active Directory database with the regularly 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 which can be used for several different domains. Store a connection parameter as a variable for logging in to the domain.
- To specify which Active Directory objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

- If another synchronization is started with the same start up configuration, this process is stop and is assigned the **Frozen** execution status. An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
  - Use the schedule to ensure that the start up configurations are executed in sequence.
  - Group start up configurations with the same start up behavior.

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

**Related topics**

- Configuring synchronization of several Active Directory domains on page 30

---

Configuring synchronization of several 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 wizards 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, which 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 loading the synchronization project. Deleted schema data can be added to the synchronization configuration again at a later point.

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

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

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

- A schema in the synchronization project was shrunk by:
  - 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 Configuration | Target system.
   - OR -
Select Configuration | One Identity Manager Connection.

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

**To edit a mapping**

1. Open the synchronization project in the Synchronization Editor.
2. Select the category Mappings.
3. Select a mapping in the navigation view.
   Opens the Mapping Editor. For more detailed information about 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 been 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 USNs of the Active Directory objects are compared with the version 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.

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

Revision filtering can be applied to workflows and start up configuration.
To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

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

For 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 synchronization.
- 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 Manager, select the Active Directory | Target system synchronization: Active Directory category.
   All tables assigned to the target system type Active Directory as synchronization tables 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 in the target system.
  The base object of the assignment has been 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 in the target system.
  During synchronization, the object and all corresponding entries in 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 one of the following icons in the form toolbar to execute the respective method.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Delete Icon]</td>
<td>Delete</td>
<td>The object is immediately deleted in the One Identity Manager database. Deferred deletion is not taken into account. The <strong>Outstanding</strong> label is removed for the object. Indirect memberships cannot be deleted.</td>
</tr>
</tbody>
</table>
| ![Publish Icon] | Publish | The object is added in the target system. The **Outstanding** label is removed for 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 Icon] | 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

- Deactivate in the form toolbar.

You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization

1. In Manager, select Active Directory | Basic configuration data | Target system types.
2. In the result list, select the target system type Active Directory.
3. Select Assign synchronization tables.
4. Assign custom tables whose outstanding objects you want to handle in Add assignments.
5. Save the changes.
6. Select Configure tables for publishing.
7. Select custom tables whose outstanding objects can be published in the target system and set Publishable.
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 option Connection is read only must no be set for the target system connection.

Configuring the provisioning of memberships

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

- Memberships are saved in the target system as an object property in list form (Example: List of user accounts in the 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 a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; previously deleted memberships are added again.

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

To allow separate provisioning of memberships

1. In Manager, select **Active Directory | Basic configuration data | Target system types**.
2. Select **Active Directory** in the result list.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
   - This option can only be enabled for assignment tables that have a base table with XDateSubItem or CCC_XDateSubItem column.
   - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically (for example, ADSAccountInADSGroup, ADSGroupInADSGroup and ADSMachineInADSGroup).
5. Click **Enable merging**.
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 the members list does not get entirely overwritten.

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

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

Help for the analysis of synchronization issues

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

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

**To generate a synchronization analysis report**

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

**Deactivating synchronization**

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

**To prevent regular synchronization**

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 General 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 a Active Directory environment in One Identity Manager, the following basic data is relevant.

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

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

  For more information, see Appendix: Configuration parameters for managing Active Directory on page 188.

- **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 40.

- **Password policies**

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password 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 user 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 58.

- 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 68.

- Email notifications about login data
  When a new user account is created, the login data are send 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 69.

- 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 70.

- 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. ns for target system managers to individual farms. SharePoint The application roles must be added under the default application role.
  For more information, see Target system managers on page 71.

- 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 73.
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 (template processing). Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

For 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 mapping rule for IT operating data
- Determining IT operating data
- Assigning account definitions to employees
- Assigning account definitions to a target system

Creating an account definition

To create a new account definition

1. In Manager, select Active Directory | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list. Select Change master data.
   -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 41
Master data for an account definition

Enter the following data for an account definition:

**Table 11: Master data for an account definition**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account definition</td>
<td>Account definition name.</td>
</tr>
<tr>
<td>User account table</td>
<td>Table in the One Identity Manager schema that maps user accounts.</td>
</tr>
<tr>
<td>Target system</td>
<td>Target system to which the account definition applies.</td>
</tr>
<tr>
<td>Required account definition</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Manage level (initial)</td>
<td>Manage level to use by default when you add new user accounts.</td>
</tr>
<tr>
<td>Risk index</td>
<td>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 configuration parameter QER</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>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 of IT Shop.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>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.</td>
</tr>
<tr>
<td>Automatic assignment</td>
<td>Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>to employees</td>
<td>not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.</td>
</tr>
<tr>
<td>Retain account definition if permanently disabled</td>
<td>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.</td>
</tr>
<tr>
<td>Retain account definition if temporarily disabled</td>
<td>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.</td>
</tr>
<tr>
<td>Retain account definition on deferred deletion</td>
<td>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.</td>
</tr>
<tr>
<td>Retain account definition on security risk</td>
<td>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.</td>
</tr>
<tr>
<td>Resource type</td>
<td>Resource type for grouping account definitions.</td>
</tr>
<tr>
<td>Spare field 01 - spare field 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>
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 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 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 Manager, select **Active Directory | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level**.
4. Assign the manage levels in **Add assignments**.
   - OR -
   Delete the manage levels in **Remove assignments**.
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. Select **Active Directory | Basic configuration data | Account definitions | Manage levels**.
2. Select the manage level in the result list. Select **Change master data**.
   - OR -
   Click in the result list.
3. Edit the manage level's master data.
4. Save the changes.

**Related topics**

- Master data for a manage level on page 44

**Master data for a manage level**

Enter the following data for a manage level.

**Table 12: Master data for manage levels**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage level</td>
<td>Name of the manage level.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>IT operating data overwrites</td>
<td>Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Never</strong>: Data is not updated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Always</strong>: Data is always updated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Only initially</strong>: The data is only determined at the start.</td>
</tr>
<tr>
<td>Retain groups if temporarily disabled</td>
<td>Specifies whether user accounts of temporarily disabled employees retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if temporarily disabled</td>
<td>Specifies whether user accounts of temporarily disabled employees are locked.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retain groups if permanently disabled</td>
<td>Specifies whether user accounts of permanently disabled employees retain group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if permanently disabled</td>
<td>Specifies whether user accounts of permanently disabled employees are locked.</td>
</tr>
<tr>
<td>Retain groups on deferred deletion</td>
<td>Specifies whether user accounts of employees marked for deletion retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if deletion is deferred</td>
<td>Specifies whether user accounts of employees marked for deletion are locked.</td>
</tr>
<tr>
<td>Retain groups on security risk</td>
<td>Specifies whether user accounts of employees posing a security risk retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if security is at risk</td>
<td>Specifies whether user accounts of employees posing a security risk are locked.</td>
</tr>
<tr>
<td>Retain groups if user account disabled</td>
<td>Specifies whether locked user accounts retain their group memberships.</td>
</tr>
</tbody>
</table>

**Creating a mapping 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 automatic creating and modifying of user accounts for an employee in the target system.

- 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 Manager, select Active Directory | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Edit IT operating data mapping and enter the following data.

Table 13: Mapping rule for IT operating data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>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.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies which roles to use in order to find the user account properties. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• Primary department</td>
</tr>
<tr>
<td></td>
<td>• Primary location</td>
</tr>
<tr>
<td></td>
<td>• Primary cost center</td>
</tr>
<tr>
<td></td>
<td>• Primary business roles</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only use the primary business role if the Business Roles Module is installed.</td>
</tr>
<tr>
<td></td>
<td>• Empty</td>
</tr>
<tr>
<td></td>
<td>If you select a role, you must specify a default value and set the option <strong>Always use default value.</strong></td>
</tr>
<tr>
<td>Default value</td>
<td>Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.</td>
</tr>
<tr>
<td>Always use default value</td>
<td>Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.</td>
</tr>
<tr>
<td>Notify when applying the standard</td>
<td>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</td>
</tr>
</tbody>
</table>

4. Save the changes.

Related topics

- Determining IT operating data on page 47
Determining 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 domainA. In addition, certain employees in department A obtain administrative user accounts in the domainA.

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

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

To define IT operating data

1. In Manager, select the role in the Organizations or Business roles category.
2. Select the Edit IT operating data task.
3. Click Add and enter the following data.

**Table 14: IT operating data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects on</td>
<td>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.</td>
</tr>
<tr>
<td>To specify an application scope</td>
<td>a. Click ➔ next to the text box.</td>
</tr>
<tr>
<td></td>
<td>b. Under Table, select the table that maps the target system for selecting the TSBAccountDef table for an account definition.</td>
</tr>
<tr>
<td></td>
<td>c. Select the specific target system or account definition under Effects on.</td>
</tr>
<tr>
<td></td>
<td>d. Click OK.</td>
</tr>
<tr>
<td>Column</td>
<td>User account property for which the value is set.</td>
</tr>
<tr>
<td>Value</td>
<td>Concrete value which is assigned to the user account property.</td>
</tr>
</tbody>
</table>

4. Save the changes.

**Related topics**

- Creating a mapping rule for IT operating data on page 45

**Modify IT operating data**

If IT operating data changes, you must transfer these changes to the existing user accounts. To do this, templates must be rerun on the affected columns. Before you can run the templates, you can check what 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, cost center, business role, or a location was changed.
  - OR -
- The default values in the IT operating data template were modified for an account definition.
NOTE: If the assignment of an employee to a primary department, cost center, business role or to a primary location changes, the templates are automatically executed.

To execute the template

1. In Manager, select Active Directory | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Execute templates in the task view
   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

   Old value: Current value of the object property.
   New value: Value that the object property would have following modification of the IT operating data.
   Selection: Specifies whether the modification shall be adopted for the user account.

4. Mark all the object properties in the selection column that will be given the new value.
5. Click Apply.
   The templates are applied to all selected user accounts and properties.

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

### Prerequisites for indirect assignment of account definitions to employees

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

**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 50
- Assigning account definitions to business roles on page 51
- Assigning account definitions to all employees on page 52
- Assigning account definitions directly to employees on page 52
- Assigning account definitions to system roles on page 53
- Adding account definitions in the IT Shop on page 54
- Assigning account definitions to a target system on page 55

### Assigning account definitions to departments, cost centers, and locations

**To add account definitions to hierarchical roles**

1. In Manager, select *Active Directory | Basic configuration data | Account definitions | Account definitions*.
2. Select an account definition in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.
TIP: In the **Remove assignments** area, you can remove the assignment of organizations.

**To remove an assignment**
- Select the organization and double click 🔍.

5. Save the changes.

**Related topics**
- Assigning account definitions to business roles on page 51
- Assigning account definitions to all employees on page 52
- Assigning account definitions directly to employees on page 52
- Assigning account definitions to system roles on page 53
- Adding account definitions in the IT Shop on page 54

**Assigning account definitions to business roles**

Installed modules: Business Roles Module

**To add account definitions to hierarchical roles**
1. In Manager, select **Active Directory | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

TIP: In the **Remove assignments** area, you can remove the assignment of 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 50
- Assigning account definitions to all employees on page 52
- Assigning account definitions directly to employees on page 52
- Assigning account definitions to system roles on page 53
- Adding account definitions in the IT Shop on page 54
Assigning account definitions to all employees

To assign an account definition to all employees

1. In Manager, select Active Directory | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Change master data.
4. Set Automatic assignment to employees on General.
   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 50
- Assigning account definitions to business roles on page 51
- Assigning account definitions directly to employees on page 52
- Assigning account definitions to system roles on page 53
- Adding account definitions in the IT Shop on page 54

Assigning account definitions directly to employees

To assign an account definition directly to employees

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

    **TIP:** In the **Remove assignments** area, you can remove the assignment of 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 50
- Assigning account definitions to business roles on page 51
- Assigning account definitions to all employees on page 52
- Assigning account definitions to system roles on page 53
- Adding account definitions in the IT Shop on page 54

Assigning account definitions to system roles

Installed modules: System Roles Module

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

**To add account definitions to a system role**

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

    **TIP:** In the **Remove assignments** area, you can remove the assignment of 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 50
- Assigning account definitions to business roles on page 51
Assigning account definitions to all employees on page 52
Assigning account definitions directly to employees on page 52
Adding account definitions in the IT Shop on page 54

Adding account definitions in the IT Shop

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

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

**TIP:** In Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in 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 **Only for use in IT Shop**. Direct assignment to hierarchical roles may not be possible.

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

**To add an account definition to the IT Shop**

1. In Manager select **Active Directory | Basic configuration data | Account definitions | Account definitions** (non-role-based login).
   - OR -
   In Manager, select **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop**.
4. Assign the account definitions to the IT Shop shelves in **Add assignments**.
5. Save the changes.

**To remove an account definition from individual IT Shop shelves**

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

**To remove an account definition from all IT Shop shelves**

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

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

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

**Related topics**

- Master data for an account definition on page 41
- Assigning account definitions to departments, cost centers, and locations on page 50
- Assigning account definitions to business roles on page 51
- Assigning account definitions to all employees on page 52
- Assigning account definitions directly to employees on page 52
- Assigning account definitions to system roles on page 53

**Assigning account definitions to a target system**

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

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

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

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

Detailed information about this topic

- Automatic assignment of employees to Active Directory user accounts on page 125

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 Manager, select Active Directory | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Change master data.
   d. Disable Automatic assignment to employees on the General tab.
   e. Save the changes.
2. Remove direct assignments of the account definition to employees.
   a. In Manager, select Active Directory | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Assign to employees in the task view.
   d. Remove employees from Remove assignments.
   e. Save the changes.
3. Remove the account definition’s assignments to departments, cost centers and locations.
a. In Manager, select **Active Directory | Basic configuration data | Account definitions | Account definitions.**
b. Select an account definition in the result list.
c. Select **Assign organizations.**
d. In **Remove assignments**, remove the relevant departments, cost centers, and locations.
e. Save the changes.

4. Remove the account definition’s assignments to business roles.
   a. In Manager, select **Active Directory | Basic configuration data | Account definitions | Account definitions.**
b. Select an account definition in the result list.
c. Select **Assign business roles.**
   Remove the business roles in **Remove assignments.**
d. Save the changes.

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

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

   **To remove an account definition from all IT Shop shelves**
   a. In Manager select **Active Directory | Basic configuration data | Account definitions | Account definitions** (non-role-based login).
   - OR -
   In Manager, select **Entitlements | Account definitions** (role-based login).
b. Select an account definition in the result list.
c. Select **Remove from all shelves (IT Shop).**
d. Confirm the security prompt with **Yes.**
e. Click **OK.**

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

6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
   a. In Manager, select **Active Directory | Basic configuration data | Account definitions | Account definitions.**
b. Select an account definition in the result list.
c. Select **Change master data.**
d. Remove the account definition in the **Required account definition** menu.

e. Save the changes.

7. Remove the account definition’s assignments to target systems.
   a. In Manager, select the domain in **Active Directory | Domains**.
   b. Select **Change master data**.
   c. Remove the assigned account definitions on the **General** tab.
   d. Save the changes.

8. Delete the account definition.
   a. In Manager, select **Active Directory | Basic configuration data | Account definitions | Account definitions**.
   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 policies apply not only when the user enters a password but also when random passwords are generated.

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

**Detailed information about this topic**

- Predefined password policies on page 58
- Using a password policy on page 60
- Editing password policies on page 62
- Custom scripts for password requirements on page 65
- Excluded list for passwords on page 67
- Checking a password on page 68
- Testing generation of a password on page 68

### 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 defined the settings for the system user passwords (DialogUser.Password and Person.DialogUserPassword) as well as the access code for a one off log in on the Web Portal (Person.Passcode).

ℹ️  **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 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.

ℹ️  **IMPORTANT:** Ensure that the Employee central password policy password policy does not violate the 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.

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

ℹ️  **NOTE:** When you update One Identity Manager version 7.x to One Identity Manager version 8.1.1, 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: The One Identity Manager password policies, global account policy settings for the Active Directory domain and Active Directory account policies are 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 87
- Active Directory account policies for Active Directory domains on page 92

Using a password policy

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: The One Identity Manager password policies, global account policy settings for the Active Directory domain and Active Directory account policies are 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. Password policy 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 standard policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the Active Directory | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.

**Table 15: Assigning a Password Policy**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply to</strong></td>
<td>Application scope of the password policy.</td>
</tr>
<tr>
<td><strong>Password column</strong></td>
<td>The password column's identifier.</td>
</tr>
<tr>
<td><strong>Password policy</strong></td>
<td>The identifier of the password policy to be used.</td>
</tr>
</tbody>
</table>

*To specify an application scope*

a. Click → next to the text box.

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.
   - Select the **TSBBehavior** table to apply the password policy based on the manage level.

c. Select the table that contains the base objects under **Apply to**.
   - 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**.

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 **Assign objects**.
4. Select the assignment you want to change in **Assignments**.
5. Select the new password policy to apply from the **Password Policies** menu.
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 a password policy on page 62
- Policy settings on page 63
- Character classes for passwords on page 64
- Custom scripts for password requirements on page 65

General master data for a password policy

Enter the following master data for a password policy.

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

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

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

### Table 17: Policy settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial password</td>
<td>Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Minimum length of the password. Specify the number of characters a password must have.</td>
</tr>
<tr>
<td>Max. length</td>
<td>Maximum length of the password. Specify the number of characters a password can have.</td>
</tr>
<tr>
<td>Max. errors</td>
<td>Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the One Identity Manager Web Portal User Guide.</td>
</tr>
<tr>
<td>Validity period</td>
<td>Maximum age of the password. Enter the length of time a password can be used before it expires.</td>
</tr>
<tr>
<td>Password history</td>
<td>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.</td>
</tr>
<tr>
<td>Minimum password strength</td>
<td>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.</td>
</tr>
<tr>
<td>Name properties denied</td>
<td>Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name</td>
</tr>
</tbody>
</table>
properties are not permitted in passwords. The values of the columns for which the Contains name properties for password check option is set are taken into account. Adjust this option in the column definition in Designer. For more detailed information, see the One Identity Manager Configuration Guide.

Character classes for passwords

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

Table 18: Character classes for passwords

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. number letters</td>
<td>Specifies the minimum number of alphabetical characters the password must contain.</td>
</tr>
<tr>
<td>Min. number lowercase</td>
<td>Specifies the minimum number of lowercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number uppercase</td>
<td>Specifies the minimum number of uppercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number digits</td>
<td>Specifies the minimum number of digits the password must contain.</td>
</tr>
<tr>
<td>Min. number special characters</td>
<td>Specifies the minimum number of special characters the password must contain.</td>
</tr>
<tr>
<td>Permitted special characters</td>
<td>List of permitted characters.</td>
</tr>
<tr>
<td>Max. identical characters in total</td>
<td>Maximum number of identical characters that can be present in the password in total.</td>
</tr>
<tr>
<td>Max. identical characters in succession</td>
<td>Maximum number of identical character that can be repeated after each other.</td>
</tr>
<tr>
<td>Denied special characters</td>
<td>List of characters, which are not permitted.</td>
</tr>
<tr>
<td>Lowercase not allowed</td>
<td>Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Uppercase not allowed</td>
<td>Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.</td>
</tr>
</tbody>
</table>
| Digits not allowed        | Specifies whether the password can contain digits. This setting is
<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special characters</td>
<td>only applies when passwords are generated.</td>
</tr>
<tr>
<td>not allowed</td>
<td>Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.</td>
</tr>
</tbody>
</table>

**Custom scripts for password requirements**

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

**Detailed information about this topic**

- Script for checking a password on page 65
- Script for generating a password on page 66

**Script for checking a password**

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

**Syntax for Check Scripts**

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

With parameters:
- policy = password policy object
- spwd = password to test

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

**Example for a script for testing a password**

A password cannot start with ? or !. 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)="!

One Identity Manager 8.1.1 Administration Guide for Connecting to Active Directory
Basic data for managing an Active Directory environment
Throw New Exception(#LD("Password can't start with '?' or '!'")#)
End If
End If
If pwd.Length>2
If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
Throw New Exception(#LD("Invalid character sequence in password")#)
End If
End If
End Sub

**To use a custom script for checking a password**

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

**Related topics**

- [Script for generating a password](#) on page 66

**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.PasswordPolicy, spwd As System.Security.SecureString)
With parameters:
policy = password policy object
spwd = generated password

| TIP: To use a base object, take the property **Entity** of the **PasswordPolicy** class. |
Example for a script to generate a password

In random passwords, the script replaces the ? and ! characters, which are not permitted.

```vba
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

To use a custom script for generating a password

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

Related topics

- [Script for checking a password](#) on page 65

Excluded list for passwords

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

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

To add a term to the restricted list

1. Select **Base Data** | **Security settings** | **Restricted passwords** in Designer.
2. Create a new entry with **Object** | **New** an enter the term to excluded to the list.
3. Save the changes.

Checking a password

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

To test whether a password conforms to the password policy
1. In the Manager, select the Active Directory | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
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 generation of a password

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

To generate a password that conforms to the password policy
1. In the Manager, select the Active Directory | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
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.

- Enable the **TargetSystem | ADS | Accounts | InitialRandomPassword** configuration parameter in Designer.
- Apply target system specific password policies and define the character sets that the password must contain.
- Specify which employee will receive the initial password by email.

User 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 *One Identity Manager Identity Management Base Module Administration Guide*.

**Related topics**

- [Password policies for Active Directory user accounts](#) on page 58
- [Email notifications about login data](#) on page 69

**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. which means the recipient’s language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

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 Designer, enable 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, activate the configuration parameter TargetSystem | ADS | Accounts | InitialRandomPassword.
2. In the Designer, activate the configuration parameter TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo and enter the recipient of the notification as a value.
3. In the Designer, activate the configuration parameter TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName. By default, the message sent uses the mail template Employee - new user account created. The message contains the name of the user account.
4. In the Designer, activate the configuration parameter TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword. By default, the message sent uses the mail template Employee - initial password for new user account. The message contains the initial password for the user account.

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

**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 Change master data.
   - 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 assigns employees to be target system managers.
2. These target system managers add employees to the default application role for target system managers.
   Target system managers with the default application role are authorized to edit all 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 19: Default Application Roles for Target System Managers |
|---------------------|---------------------|
| **User**            | **Tasks**           |
| Target system managers | Target system managers must be assigned to [Target systems | Active Directory](#) or a sub-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 for adding to the IT Shop. |
|                     | • Can add employees, who have an other identity than the Primary identity. |
|                     | • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. |
|                     | • Edit the synchronization's target system types and outstanding objects. |

User Tasks
User Tasks

- Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

**To initially specify employees to be target system administrators**

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

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

1. Log yourself into Manager as target system administrator (Target systems | Administrators).
2. Select One Identity Manager Administration | Target systems | Active Directory.
3. Select Assign employees in the task view.
4. Assign the employees you want and save the changes.

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

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

**To specify target system managers for individual domains**

1. Log in to Manager as target system manager.
2. Select the category Active Directory | Domains.
3. Select the domain in the result list.
4. Select Change master data.
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 an Active Directory environment on page 10
- General master data for an Active Directory domain on page 85
- Master data for an Active Directory container on page 174

**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:

- Create an entry for the Job server in Designer under **Base Data | Installation | Job server**. For detailed information, see One Identity Manager Configuration Guide.

- Select an entry for the Job server in **Active Directory | Basic configuration data | Server** in Manager and edit the Job server master data.

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

**NOTE:** One Identity Manager must be installed, configured, and started in order for a server to execute 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 Manager, select the category Active Directory | Basic configuration data | Server.
2. Select the Job server entry in the result list.
3. Select Change master data.
4. Edit the Job server's master data.
5. Select Assign server functions in the task view and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master data for a Job server on page 74
- Specifying server functions on page 77
- Preparing a home server and profile server for creating user directories on page 78

Master data for a Job server

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

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

Table 20: Job Server Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</td>
</tr>
<tr>
<td>Full server name</td>
<td>Full server name in accordance with DNS syntax.</td>
</tr>
<tr>
<td></td>
<td>Example: &lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</td>
</tr>
<tr>
<td>Target system</td>
<td>Computer account target system.</td>
</tr>
<tr>
<td>Language</td>
<td>Language of the server.</td>
</tr>
<tr>
<td>Server is cluster</td>
<td>Specifies whether the server maps a cluster.</td>
</tr>
<tr>
<td>Server belongs to cluster</td>
<td>Cluster to which the server belongs.</td>
</tr>
</tbody>
</table>

NOTE: The properties Server is cluster and Server belongs to cluster are mutually exclusive.
<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Active Directory DC</td>
<td>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.</td>
</tr>
<tr>
<td>IP address (IPv6)</td>
<td>Internet protocol version 6 (IPv6) server address.</td>
</tr>
<tr>
<td>IP address (IPv4)</td>
<td>Internet protocol version 4 (IPv4) server address.</td>
</tr>
<tr>
<td>Max. number of homes</td>
<td>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 (&lt;Homes created&gt;) 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.</td>
</tr>
<tr>
<td>Homes created</td>
<td>Number of homes directories already in existing on the home server.</td>
</tr>
<tr>
<td>Copy process (source server)</td>
<td>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.</td>
</tr>
<tr>
<td>Copy process (target server)</td>
<td>Permitted copying methods that can be used when this server is the destination of a copy action.</td>
</tr>
<tr>
<td>Max. home storage space [MB]</td>
<td>Maximum permitted storage in MB for home directories on the home server. This is taken into account when the home directory is allocated.</td>
</tr>
<tr>
<td>Coding</td>
<td>Character set coding that is used to write files to the server.</td>
</tr>
<tr>
<td>Parent Job</td>
<td>Name of the parent Job server.</td>
</tr>
<tr>
<td><strong>Property</strong></td>
<td><strong>Meaning</strong></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Executing server</td>
<td>Name of the executing server. The name of the server that exists physically and where the processes are handled.</td>
</tr>
<tr>
<td></td>
<td>This input is evaluated when 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.</td>
</tr>
<tr>
<td>Queue</td>
<td>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 exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.</td>
</tr>
<tr>
<td>Server operating system</td>
<td>Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values <strong>Win32</strong>, <strong>Windows</strong>, <strong>Linux</strong> and <strong>Unix</strong> are permitted. If no value is specified, <strong>Win32</strong> is used.</td>
</tr>
<tr>
<td>Service account data</td>
<td>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.</td>
</tr>
<tr>
<td>One Identity Manager Service installed</td>
<td>Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure QBM_PJobQueueLoad 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.</td>
</tr>
</tbody>
</table>
| 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 program "Job Queue Info". For more detailed information, see the **One Identity Manager Process Monitoring and Troubleshooting Guide**. |
| No automatic software update         | Specifies whether to exclude the server from automatic software updating.  
**NOTE:** Servers must be manually updated if this option is set. |
| Software update running              | Specifies whether a software update is currently being executed.                                                                                                                                              |
| Server function                      | Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.                                                                                 |
Related topics

- Specifying server functions on page 77

Specifying server functions

NOTE: All editing options are also available in 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 depending on the server function.

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

Table 21: Permitted server functions

<table>
<thead>
<tr>
<th>Server function</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory connector</td>
<td>Server on which the Active Directory connector is installed. This server executes synchronization with the target system Active Directory.</td>
</tr>
<tr>
<td>CSV connector</td>
<td>Server on which the CSV connector for synchronization is installed.</td>
</tr>
<tr>
<td>Domain controller</td>
<td>The Active Directory domain controller. Servers that are not labeled as domain controller are considered to be member servers.</td>
</tr>
<tr>
<td>Printer server</td>
<td>Server which acts as a print server.</td>
</tr>
<tr>
<td>Generic server</td>
<td>Server for generic synchronization with a custom target system.</td>
</tr>
<tr>
<td>Home server</td>
<td>Server for adding home directories for user accounts.</td>
</tr>
<tr>
<td>Update Server</td>
<td>This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.</td>
</tr>
<tr>
<td>SQL processing server</td>
<td>The server can execute SQL tasks. 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.</td>
</tr>
<tr>
<td>CSV script server</td>
<td>The server can process CSV files using the ScriptComponent process component.</td>
</tr>
<tr>
<td><strong>Server function</strong></td>
<td><strong>Remark</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Native database connector</td>
<td>The server can connect to an ADO.Net database.</td>
</tr>
<tr>
<td>One Identity Manager database connector</td>
<td>Server on which the One Identity Manager connector is installed. This server executes synchronization with the target system One Identity Manager.</td>
</tr>
<tr>
<td>One Identity Manager Service installed</td>
<td>Server on which a One Identity Manager Service is installed.</td>
</tr>
<tr>
<td>Primary domain controller</td>
<td>Primary domain controller.</td>
</tr>
<tr>
<td>Profile server</td>
<td>Server for setting up profile directories for user accounts.</td>
</tr>
<tr>
<td>SAM synchronization Server</td>
<td>Server for running synchronization with an SMB-based target system.</td>
</tr>
<tr>
<td>SMTP host</td>
<td>Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.</td>
</tr>
<tr>
<td>Default report server</td>
<td>Server on which reports are generated.</td>
</tr>
<tr>
<td>Windows PowerShell connector</td>
<td>The server can run Windows PowerShell version 3.0 or later.</td>
</tr>
</tbody>
</table>

**Related topics**

- Master data for a Job server on page 74

**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 Designer, set the configuration parameters `TargetSystem | ADS | AutoCreateServers` and `TargetSystem | ADS | AutoCreateServers | PreferredLanguage`. 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 `Active Directory | Basic configuration data | Servers`.
2. Select the Job server entry in the result list.
3. Select `Change master data`.
4. Edit the Job server's master data.
5. Select `Assign server functions` in the task view and specify the server functions `Home server` and `Profile server`.
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 Designer, set the configuration parameter `QER | Person | User | ConnectHomeDir`.
- To create the user profile in the user’s home directory, in Designer set the configuration parameter `QER | Person | User | PropertyMapping | ProfileFromHome`.
- 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 79
- Supporting multiple profile directories on page 80
- Home and profile directory access permissions on page 82
- Master data for a Job server on page 74
- Specifying server functions on page 77

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 Designer, activate the configuration parameter TargetSystem | ADS | Accounts | ProfileFixedString 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. For this scenario, adjust the configuration parameter TargetSystem | ADS | Accounts | TProfileFixedString in Designer. 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 22: Configuration parameters for setting up user directories

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

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 Designer, set the configuration parameter **QER | Person | User | AccessRights | HomeDir** and its lower-level configuration parameters, and enter the access rights in the configuration parameters.
  
  Granting access permissions to the home directory is done by through One Identity Manager Service.

Table 23: Configuration parameters for home directory access permissions

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

| QER | Person | User | AccessRights | HomeDir | **Everyone** has permission to access a user’s home directory. Default: -r-w-x |

| QER | Person | User | AccessRights | HomeDir | **User** This configuration parameter defines the home directory user rights. Default: +r+w-x |

To grant access permission for the profile directory

- In Designer, set the configuration parameter **QER | Person | User | AccessRights | ProfileDir** and its lower-level configuration parameter, and enter the access rights in the configuration parameters.
  
  Granting access permissions to the profile directory is done by through One Identity Manager Service.
Table 24: Configuration parameters for profile directory access permissions

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

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

- In Designer, set the configuration parameter **QER | Person | User | AccessRights | TerminalHomeDir** and its lower-level configuration parameters, and enter the access rights in the configuration parameters.

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

Table 25: Configuration parameters for access permissions to the home directory on a terminal server

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

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

- In Designer, set the configuration parameter **QER | Person | User | AccessRights | TerminalProfileDir** and its lower-level configuration parameters, and enter the access rights in the configuration parameters.
Granting access permissions to the profile directory is done through One Identity Manager Service.

**Table 26: Configuration parameters for access permissions to the profile directory on a terminal server**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

**Related topics**

- User account names on page 70
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 category **Active Directory | Domains**.
2. Select the domain in the result list.
3. Select **Change master data**.
4. Edit the domain's master data.
5. Save the changes.

**General master data for an Active Directory domain**

Enter the following data on **General**:

**Table 27: Domain master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>NetBIOS domain name. This corresponds to the pre-Windows 2000 domain names. The domain name cannot be changed later.</td>
</tr>
<tr>
<td>Parent domain</td>
<td>Parent domain for mapping a hierarchical domain structure. The full name and the defined name are automatically updated through templates.</td>
</tr>
<tr>
<td>Domain subtype</td>
<td>Active Directory functional level. There are several features available in Active Directory at functional level. Refer to the documentation for the appropriate Windows Server to find out which functional levels are supported by the domain controller's Windows operating system to be implemented. Following functional levels are supported in One Identity Manager:</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2000 (Win2000)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2003 native (Win2003 native)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2003 mixed (Win2003 mixed)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2008 (Win2008)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2008 R2 (Win2008 R2)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2012 (Win2012)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2012 R2 (Win2012 R2)</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2016 (Win2016)</td>
</tr>
<tr>
<td>Display name</td>
<td>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.</td>
</tr>
<tr>
<td>Account definition</td>
<td>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.</td>
</tr>
<tr>
<td>(initial)</td>
<td>User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.</td>
</tr>
<tr>
<td>Contact definition</td>
<td>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). The account definition's default manage level is applied.</td>
</tr>
<tr>
<td>(initial)</td>
<td>Contacts are only linked to the employee (Linked state) if no account definition is given. This is the case on initial synchronization, for example.</td>
</tr>
<tr>
<td>Target system managers</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Synchronized by</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>One Identity Manager</strong> is used when you create a domain with the Synchronization Editor.</td>
</tr>
</tbody>
</table>
### Table 28: Permitted values

<table>
<thead>
<tr>
<th>Value</th>
<th>Synchronization by</th>
<th>Provisioned by</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

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

### Related topics

- Automatic assignment of employees to Active Directory user accounts on page 125
- Target system managers on page 71
- Information about the Active Directory forest on page 90

### 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 settings against the domain. Account policies apply when user accounts are newly added.

Enter the following master data on the Account policies tab.

### Table 29: Account policies for domains

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. password length</td>
<td>Minimum length of the password. Use this option to specify that a password has to be complex.</td>
</tr>
<tr>
<td>Min. password lifetime</td>
<td>Minimum age of the password. Enter the length of time a password has to be used before the user is allowed to change it.</td>
</tr>
<tr>
<td>Max. password lifetime</td>
<td>Maximum age of the password. Enter the length of time a password can be used before it expires.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max. errors</td>
<td>Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.</td>
</tr>
<tr>
<td>Password history</td>
<td>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.</td>
</tr>
<tr>
<td>Block duration [min]</td>
<td>Block duration in minutes. Enter the time period the account should be locked for before it is automatically reset.</td>
</tr>
<tr>
<td>Reset account [min]</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 the One Identity Manager that you can apply to the user account passwords.

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

### Related topics

- Password policies for Active Directory user accounts [on page 58](#)
- Active Directory account policies for Active Directory domains [on page 92](#)
- Password data for Active Directory user accounts [on page 111](#)

## Active Directory specific master data for an Active Directory domain

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

### Table 30: Active Directory data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name (pre Win2000)</td>
<td>Pre-Windows 2000 computer name.</td>
</tr>
<tr>
<td>Full domain</td>
<td>Name of the domain confirming to DNS syntax.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>Name of this domain.name of parent domain.name of default domain Example Docu.Testlab.dd</td>
</tr>
</tbody>
</table>
| Account manager       | Manager responsible for the domain. **To specify an account manager**  
1. Click ➔ next to the text box.  
2. Under Table, select the table which maps the account manager.  
3. Select the manager under **Account 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 151
- Deleting and restoring Active Directory user accounts on page 133
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 for groups in the group table. Each table contains the category positions Position 1 to Position 31.

To define a category

1. Select the category **Active Directory | Domains**.
2. Select the domain in the result list.
3. Select **Change master data**.
4. Select the **Categories** tab.
5. Expand the root in the respective table.
6. Click to enable category.
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 168

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 **Active Directory | Forests**.
2. Select a forest in the result list.
3. To display a domain's forest, select **Forest overview** in the task view.
4. To display a forest's master data, select **Change master data** in the task view.

Related topics
- Trusted Active Directory domains on page 91
- Validity of group memberships on page 151

**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. Select the **Active Directory | Domains** category in Manager.
2. Select the domain in the result list.
3. Select **Change master data**.
4. Enter the parent domain.
5. Save the changes.

Implicit trusts are created automatically.

**To test trusted domains**

1. Select the **Active Directory | Domains** category in Manager.
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 the One Identity Manager that you can apply to the user account passwords.

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

Detailed information about this topic

- Entering Active Directory account policies on page 92
- Assigning Active Directory account policies to Active Directory user accounts and Active Directory groups on page 94

Related topics

- Password policies for Active Directory user accounts on page 58
- Global account policies for an Active Directory domain on page 87

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 Active Directory | Account policies.
2. Select the account policy in the result list and run Change master data in the task view.
   - 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 93
- How to Define a Policy on page 93

General master data for an Active Directory account policy

Enter the following data on General:

Table 31: General master data for an account policy

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Account policy name</td>
</tr>
<tr>
<td>Domain</td>
<td>Active Directory domain for which the account policy is available.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>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.</td>
</tr>
<tr>
<td>Display name</td>
<td>Display name to display in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Simple display</td>
<td>Display name for systems that cannot interpret all the characters of normal display names.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

Related topics

- How to Define a Policy on page 93

How to Define a Policy

Enter the following master data on the Policies tab.

Table 32: Master data for a policy definition

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block duration</td>
<td>Block duration in minutes. Enter the time period the account should be locked for before it is automatically reset.</td>
</tr>
<tr>
<td>Reset account</td>
<td>Duration in minutes of account reset. Enter the time period that can be entered.</td>
</tr>
</tbody>
</table>

One Identity Manager 8.1.1 Administration Guide for Connecting to Active Directory domains 93
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>elapse between two invalid attempts to enter a password before a user account is locked.</td>
</tr>
<tr>
<td>Max. errors</td>
<td>Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.</td>
</tr>
<tr>
<td>Max. password age</td>
<td>Maximum age of the password. Enter the length of time a password can be used before it expires.</td>
</tr>
<tr>
<td>Min. password lifetime</td>
<td>Minimum age of the password. Enter the length of time a password has to be used before the user is allowed to change it.</td>
</tr>
<tr>
<td>Min. password length</td>
<td>Minimum length of the password. Use this option to specify that a password has to be complex.</td>
</tr>
<tr>
<td>Password history</td>
<td>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.</td>
</tr>
<tr>
<td>Ranking</td>
<td>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.</td>
</tr>
<tr>
<td>Complex passwords</td>
<td>Specifies how complicated the password should be. Complex passwords must fulfill certain minimum prerequisites. For more information, see the documentation for implementing Windows Server.</td>
</tr>
<tr>
<td>Save passwords with reversible encryption</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related topics**

- [General master data for an Active Directory account policy](#) on page 93

**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 Windows Server documentation on fine-grained account policies under Active Directory for information about the rules for calculating this.
To specify account policies for a user account

1. Select Active Directory | Account policies.
2. Select the account policy in the result list.
3. Select Assign user accounts in the task view.
4. Assign user accounts in Add assignments.
   
   TIP: In the Remove assignments area, you can remove the assignment of 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 Active Directory | Account policies.
2. Select the account policy in the result list.
3. Select Assign groups in the task view.
4. Assign groups in Add assignments.
   
   TIP: you can remove the assignment of groups in the Remove assignments area.

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

5. Save the changes.

Editing a synchronization project

Synchronization projects in which a domain is already used as a base object can also be opened in 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: Manager is locked for editing throughout. To edit objects in Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

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

- Customizing synchronization configuration on page 28

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

## Table 33: Effective configuration parameters

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
</tbody>
</table>

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 ADSSGroup 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.
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 98
- Supported user account types on page 99
- Entering master data for Active Directory user accounts on page 105

Linking user accounts to employees

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems.

One Identity Manager provides the possibility to manage user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

Because requirements vary between companies, the One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.
Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a 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. 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 105
- Account definitions for Active Directory user accounts on page 40
- Automatic assignment of employees to Active Directory user accounts on page 125
- For 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>
<thead>
<tr>
<th><strong>Table 34: Identities of user accounts</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity</strong></td>
</tr>
<tr>
<td>Primary identity</td>
</tr>
</tbody>
</table>

One Identity Manager 8.1.1 Administration Guide for Connecting to Active Directory

Active Directory user accounts
<table>
<thead>
<tr>
<th>Identity</th>
<th>Description</th>
<th>Value of the IdentityType column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational identity</td>
<td>Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</td>
<td>Organizational</td>
</tr>
<tr>
<td>Personalized admin identity</td>
<td>User account with administrative permissions, used by one employee.</td>
<td>Admin</td>
</tr>
<tr>
<td>Sponsored identity</td>
<td>User account that is used for training purposes, for example.</td>
<td>Sponsored</td>
</tr>
<tr>
<td>Shared identity</td>
<td>User account with administrative permissions, used by several employees.</td>
<td>Shared</td>
</tr>
<tr>
<td>Service identity</td>
<td>Service account.</td>
<td>Service</td>
</tr>
</tbody>
</table>

**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 personal admin identity are used for different user accounts, which can be used by the same actual employee to execute their different tasks within the company.

To provide user accounts with a personal 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 Entitlements 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 Entitlements 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 marked as **Privileged user account** (Column IsPrivilegedAccount).

**Detailed information about this topic**

- Default user accounts on page 101
- Administrative user accounts on page 102
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 via 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 Always use default value.
   - 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 which IT operating data should apply when you set up a user account.
5. Assign the account definition to employees.
   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

Related topics

- Account definitions for Active Directory user accounts on page 40
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, enable the Mark selected user accounts as privileged schedule in Designer.

Related topics

- Providing an administrative user account for one employee on page 102
- Providing an administrative user account for multiple employees on page 103

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 Manager, select Active Directory | User accounts.
   b. Select the user account in the result list.
   c. Select Change master data.

2. Link the user account to the employee who will be using this administrative user account.
   a. In Manager, select Active Directory | User accounts.
   b. Select the user account in the result list.
   c. Select Change master data.
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 ![create button] to create a new person.

**Related topics**

- Providing an administrative user account for multiple employees on page 103
- 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 Manager, select **Active Directory | User accounts**.
   - b. Select the user account in the result list.
   - c. Select **Change master data**.
   - d. On the **General** tab, in the **Identity** selection list, select **Shared identity**.

2. Link the user account to a dummy employee.
   
   - a. In Manager, select **Active Directory | User accounts**.
   - b. Select the user account in the result list.
   - c. Select **Change master data**.
   - d. On the **General** tab, select the dummy employee from the **Employee** selection list.

   |
   | **TIP:** If you are the target system manager, you can choose ![create button] to create a new dummy employee.

3. Assign the employees who will use this administrative user account to the user account.
a. In Manager, select **Active Directory | User accounts**.
b. Select the user account in the result list.
c. Select the task **Assign employees authorized to use**.
d. Assign employees in **Add assignments**.

**TIP:** In the **Remove assignments** area, you can remove the assignment of employees.

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

**Related topics**
- Providing an administrative user account for one employee on page 102
- 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 marked as **Privileged user account** (Column IsPrivilegedAccount).

**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 script TSB_SetIsPrivilegedAccount.

**To create privileged users through account definitions**

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent 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 is 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 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 via 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 enable **Always use default value**.
- 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 enable **Always use default value**.

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

6. Assign the account definition directly to employees who work with privileged user accounts.
   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

   **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, enable the `TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_Prefix` configuration parameter in Designer.
   - To use a postfix for the login name, enable the `TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_Postfix` configuration parameter in Designer.

   These configuration parameters are evaluated in the default installation, if a user account is marked with the property **Privileged user account** (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 40

## 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 Manager, select Active Directory | User accounts.
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 Manager, select Active Directory | User accounts.
2. Select the user account in the result list and run Change master data.
3. Edit the user account’s resource data.
4. Save the changes.

To manually assign or create a user account for an employee
1. Select the Employees | Employees.
2. Select the employee in the result list and run Assign Active Directory user accounts from the task view.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic
- General master data of an Active Directory user account on page 107
- Password data for Active Directory user accounts on page 111
- Profile and home directories on page 113
- Active Directory user account login data
- Remote access service dial-in permissions on page 115
- Connection data for terminal servers on page 116
- Extensions data for an Active Directory user account on page 118
- Further identification data on page 119
- Contact data for an Active Directory user account on page 120
Related topics

- Account definitions for Active Directory user accounts on page 40
- Linking user accounts to employees on page 98
- Supported user account types on page 99

General master data of an Active Directory user account

Table 35: Configuration parameters for setting up user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 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 General:

Table 36: Additional Master Data for a User Account

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>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. For a user account with an identity type <strong>Organizational identity</strong>, <strong>Personalized administrator identity</strong>, <strong>Sponsored identity</strong>, <strong>Shared identity</strong> or <strong>Service identity</strong>, you can create a new employee. 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.</td>
</tr>
<tr>
<td>Account definition</td>
<td>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. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</td>
</tr>
</tbody>
</table>

**NOTE:** The account definition cannot be changed once the user account has been saved.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage level</td>
<td>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.</td>
</tr>
<tr>
<td>First name</td>
<td>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.</td>
</tr>
<tr>
<td>Last name</td>
<td>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.</td>
</tr>
<tr>
<td>Initials</td>
<td>The user’s initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Title</td>
<td>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.</td>
</tr>
<tr>
<td>Name</td>
<td>User account identifier. The identifier is made up of the user’s first and last names.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>User account’s distinguished name. The distinguished name is formatted from the user account’s identifier and the container and cannot be changed.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in which the user account is created.</td>
</tr>
<tr>
<td>Container</td>
<td>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.</td>
</tr>
<tr>
<td>Primary group</td>
<td>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.</td>
</tr>
<tr>
<td>Login name (pre Win2000)</td>
<td>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.</td>
</tr>
<tr>
<td>User login name</td>
<td>User account login name. User login names that are formatted like this correspond to the User Principal Name (UPN) in Active Directory.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>
| Email                 | User account email address. If you assigned an account definition, the
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Email address is made up of the employee’s default email address depending on the manage level of the user account.</td>
</tr>
<tr>
<td>Additional email addresses</td>
<td>Other email addresses for the user account.</td>
</tr>
<tr>
<td>Account expiry date</td>
<td>Account expiry date. Specifying an expiry data for the account has the effect that the logon for this user account is blocked as soon as the given date is exceeded. If you assigned an account definition, the employee’s last day of work is automatically taken as the expiry date depending on the manage level. Any existing account expiry data is overwritten in this case.</td>
</tr>
<tr>
<td>Structural object class</td>
<td>Structural object class representing the object type. By default, you set up user accounts in One Identity Manager with the object class USER. However, the object class INETORGPERSON is also supported, which is used by other LDAP and X.500 directory services for the mapping of user accounts.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Maximum risk index value of all assigned groups. The property is only visible if the QER</td>
</tr>
<tr>
<td>Category</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Identity</td>
<td>User account’s identity type Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Primary identity</strong>: Employee’s default user account.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Organizational identity</strong>: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Personalized administrator identity</strong>: User account with administrative entitlements, used by one employee.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sponsored identity</strong>: User account that is used for training purposes, for example.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Shared identity</strong>: User account with administrative entitlements, used by several employees. Assign all employees show use the user account.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Service identity</strong>: Service account.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privileged user account</td>
<td>Specifies whether this is a privileged user account.</td>
</tr>
<tr>
<td>Groups can be inherited</td>
<td>Specifies whether the user account can inherit groups via the employee. If this option is set, the user account inherits groups via hierarchical roles or IT Shop requests.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Preferred user account</td>
<td>Preferred user account when an employee has several user accounts in Active Directory.</td>
</tr>
<tr>
<td>User account is disabled</td>
<td>Specifies whether the user account is disable. If a user account is not required for a period of time, you can temporarily disable the user account by using the option &lt;User account is deactivated&gt;.</td>
</tr>
<tr>
<td>Account locked</td>
<td>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 Unlock user account.</td>
</tr>
</tbody>
</table>

Related topics

- Account definitions for Active Directory user accounts on page 40
- Active Directory group inheritance based on categories on page 168
- Linking user accounts to employees on page 98
- Supported user account types on page 99
- Disabling Active Directory user accounts on page 132
- Unlocking Active Directory user accounts on page 122
- Automatic assignment of employees to Active Directory user accounts on page 125
Password data for Active Directory user accounts

Table 37: Configuration parameters for setting up password data

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
</tbody>
</table>

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

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

Table 38: User account password data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>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.</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Password last changed</td>
<td>Data of last password change. The date is read in from the Active Directory system and cannot be changed.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>Specifies whether the password expires. This option is usually used for service accounts. It overwrites the maximum lifetime of a password and the option <strong>Change password at next logon</strong>.</td>
</tr>
<tr>
<td>Cannot change password</td>
<td>Specifies whether the password can be changed. This option is normally set for user accounts that are used by several users.</td>
</tr>
<tr>
<td>Change password at next login</td>
<td>Specifies whether the user must change their password the next time they log in.</td>
</tr>
</tbody>
</table>
## Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save passwords with reversible encryption</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>SmartCard required to log on</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Account trusted for delegation purposes</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cannot delegate account</strong></td>
<td>Data required for delegation. Set this option when this user account may not be assigned for delegation purposes from another user account.</td>
</tr>
<tr>
<td><strong>Account uses DES encryption</strong></td>
<td>Data required for encryption. Set this option if you would like to activate the Data Encryption Standard (DES) support.</td>
</tr>
<tr>
<td><strong>Kerberos preauthentication not required</strong></td>
<td>Specifies whether Kerberos pre-authentication is required. Set this option when the user account uses a different implementation of the Kerberos protocol.</td>
</tr>
</tbody>
</table>

### Related topics

- [Password policies for Active Directory user accounts](#) on page 58
- [Initial password for new Active Directory user accounts](#) on page 68
- [Global account policies for an Active Directory domain](#) on page 87
- [Active Directory account policies for Active Directory domains](#) on page 92
- [Assigning Active Directory account policies to an Active Directory user account](#) on page 122
Profile and home directories

Table 39: Configuration parameters for setting up user directories

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

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

**NOTE:** If the configuration parameter QER | Person | User | ConnectHomeDir is enabled, some of the following data for the home directory is formed automatically. If necessary, activate the configuration parameter in the Designer.

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 40: Master data for a user directory

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home server</td>
<td>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.</td>
</tr>
<tr>
<td>Home share</td>
<td>The share that is stored under the user's home directory on the home server. Default is HOMES.</td>
</tr>
<tr>
<td>Home directory path</td>
<td>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.</td>
</tr>
<tr>
<td>Home shared as</td>
<td>Home directory share. This share is formatted using the default home directory path.</td>
</tr>
<tr>
<td>Home drive</td>
<td>The drive to be connected when the user logs in. The default domain home drive is used.</td>
</tr>
<tr>
<td>Home directory</td>
<td>The user's home directory. The given home directory is automatically added and shared by the One Identity Manager Service.</td>
</tr>
<tr>
<td>Size home directory [MB]</td>
<td>Size of the home directory in MB. Find the size of the home directory by running the schedule supplied by default. In Designer, configure and enable the schedule <strong>Load size of home folders for user accounts.</strong></td>
</tr>
</tbody>
</table>
### Property | Description
--- | ---
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.
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 78

## Active Directory user account login data

Enter the following master data on the Log in tab.

### Table 41: Login data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last login</td>
<td>Date of last login. The date is read in from the Active Directory system and cannot be changed manually.</td>
</tr>
<tr>
<td>Login workstation</td>
<td>Workstation on which the user can log in. A user can log in on all workstations by default.</td>
</tr>
<tr>
<td></td>
<td>Select the button next to the input field to activate it and add workstations. Use the button to remove workstations from the list.</td>
</tr>
<tr>
<td>Login times</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 option Enable RAS properties is set.](image)

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 42: Remote access service

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial-up permitted</td>
<td>Specifies whether the user may dial up the network. Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>- Allow access: This permits the user to dial up the network.</td>
</tr>
<tr>
<td></td>
<td>- Deny access: With this users are not allowed to dial up the network.</td>
</tr>
<tr>
<td></td>
<td>- Control access through Remote Access Policy: This data specifies that access to the network is controlled over RAS guidelines. RAS guidelines are usually used to apply the same access permissions to several Active Directory user accounts.</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</td>
</tr>
</tbody>
</table>
Property Description
---
he can be called back on.
Always callback The server tries to call the user back over the given number.
Verifying caller ID A predefined number with which the user should dial into the network.
Static IP address A fixed IP address assigned to the user.
Static routes with IP address, network address and metric Target network IP addresses, network addresses and metrics for dialing in over fixed routes.

Related topics
- Setting up synchronization with an Active Directory environment on page 13

Connection data for terminal servers

Table 43: Configuration parameters for terminal server properties

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

**NOTE:** Terminal server properties are only synchronized and provisioned if **Enable terminal server properties** 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 configuration parameter QER | Person | User | ConnectHomeDir is enabled, some of the following data for the home directory is formed automatically. If necessary, activate the configuration parameter in the Designer.

Enter the following data on the Terminal service tab.

Table 44: Master data for a terminal server

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login permitted on terminal</td>
<td>Specifies whether terminal server login is allowed. Enable this option to allow a user to log on to a terminal server.</td>
</tr>
</tbody>
</table>
## Property | Description
--- | ---
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.
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 activated 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.
## Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interact with session</td>
<td>Specifies whether the person monitoring can input data into the session over the keyboard or the mouse.</td>
</tr>
<tr>
<td>Profile Server</td>
<td>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.</td>
</tr>
<tr>
<td>Profile share</td>
<td>The share that is stored under the user’s profile directory on the profile server. Default is TPROFILES.</td>
</tr>
<tr>
<td>Profile directory path</td>
<td>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.</td>
</tr>
<tr>
<td>Profile path</td>
<td>The full path to the user’s profile directory.</td>
</tr>
<tr>
<td>Home server</td>
<td>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.</td>
</tr>
<tr>
<td>Home share</td>
<td>The share that is stored under the user’s home directory on the home server. Default is THOMES.</td>
</tr>
<tr>
<td>Home directory path</td>
<td>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.</td>
</tr>
<tr>
<td>Shared as</td>
<td>Home directory share. This share is formatted using the default home directory path.</td>
</tr>
<tr>
<td>Home drive</td>
<td>The drive to be connected when the user logs in. The default domain home drive is used.</td>
</tr>
<tr>
<td>Home directory</td>
<td>Home directory. The given home directory is automatically added and shared by the One Identity Manager Service.</td>
</tr>
</tbody>
</table>

### Related topics

- Preparing a home server and profile server for creating user directories on page 78

---

### 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 45: Extensions data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensions data</td>
<td>Custom extension data in binary format.</td>
</tr>
<tr>
<td>Attribute extension 01-</td>
<td>Additional company specific information. Use Designer to customize display</td>
</tr>
<tr>
<td>attribute extension 15</td>
<td>names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

Further identification data

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

Table 46: Master data for identification

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office</td>
<td>Office. If you have assigned an account definition, the input field is</td>
</tr>
<tr>
<td></td>
<td>automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Street</td>
<td>Street or road If you have assigned an account definition, the input field</td>
</tr>
<tr>
<td></td>
<td>is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>Mailbox If you have assigned an account definition, the input field is</td>
</tr>
<tr>
<td></td>
<td>automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code If you have assigned an account definition, the input field is</td>
</tr>
<tr>
<td></td>
<td>automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>City</td>
<td>City. If you have assigned an account definition, the input field is</td>
</tr>
<tr>
<td></td>
<td>automatically filled out with respect to the manage level. Locations can be</td>
</tr>
<tr>
<td></td>
<td>automatically generated and employees assigned based on the town.</td>
</tr>
<tr>
<td>State</td>
<td>State If you have assigned an account definition, the input field is</td>
</tr>
<tr>
<td></td>
<td>automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Country ID</td>
<td>The country ID.</td>
</tr>
<tr>
<td>Company</td>
<td>Employee’s company. If you have assigned an account definition, the input</td>
</tr>
<tr>
<td></td>
<td>field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Department</td>
<td>Employee’s department If you have assigned an account definition, the input</td>
</tr>
<tr>
<td></td>
<td>field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td></td>
<td>Departments can be automatically generated and employees assigned based on</td>
</tr>
<tr>
<td></td>
<td>the department data.</td>
</tr>
<tr>
<td>Job description</td>
<td>Job description. If you have assigned an account definition, the input</td>
</tr>
<tr>
<td></td>
<td>field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Employee’s unique marker, for example their ID.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Employee number</td>
<td>Number for identifying the employee in addition to their ID.</td>
</tr>
<tr>
<td>Account manager</td>
<td>Manager responsible for the user account.</td>
</tr>
</tbody>
</table>

**To specify an account manager**

1. Click next to the text box.
2. Under Table, select the table which maps the account manager.
3. Select the manager under Account manager.
4. Click OK.

**Related topics**

- Automatic creation of departments and locations based on user account information on page 131

**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 47: Contact Data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Telephone number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Phone private</td>
<td>Private telephone number.</td>
</tr>
<tr>
<td>Fax</td>
<td>Fax number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>Mobile number If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Pager</td>
<td>Pager number.</td>
</tr>
<tr>
<td>Web page</td>
<td>Website.</td>
</tr>
<tr>
<td>IP telephone number</td>
<td>IP telephone number.</td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>
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 Active Directory | User accounts.
2. Select the user account in the result list.
3. Select Active Directory user account overview.

Changing the manage level of an Active Directory user account

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

To change the manage level for a user account

1. In Manager, select Active Directory | User accounts.
2. Select the user account in the result list.
3. Select Change master data.
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 105
Unlocking Active Directory user accounts

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

**To unlock a user account**

1. Select *Active Directory | User accounts*.
2. Select the user account in the result list.
3. Select *Change master data*.
4. Select *Unlock user account* from the task view.
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 105

Assigning Active Directory account policies to an Active Directory user account

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 user account**

1. Select *Active Directory | User accounts*.
2. Select the user account in the result list.
3. Select *Assign account policies* in the task view.
4. Assign the account policies in *Add assignments*.
   - OR -
     Remove the account policies in *Remove assignments*.
5. Save the changes.

Related topics

- [Active Directory account policies for Active Directory domains](#) on page 92
- [Global account policies for an Active Directory domain](#) on page 87
Assigning Active Directory account policies directly to an Active Directory group on page 170

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 Manager, select Active Directory | User accounts.
2. Select the user account in the result list.
3. Select Assign groups.
4. Assign groups in Add assignments.

   TIP: you can remove the assignment of groups in the Remove assignments area.

   To remove an assignment
   - Select an assignment.

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 153
- Validity of group memberships on page 151
- General master data of an Active Directory user account on page 107
Assigning wizards 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 Active Directory | User accounts.
2. Select the user account in the result list.
3. Select Assign secretaries in the task view.
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. Assign secretaries in Add assignments.
   - OR -
   Remove secretaries from Remove assignments.
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 Active Directory | User accounts.
2. Select the user account in the result list.
3. Select Change master data.
4. Select Active Directory Change container in the task view.
5. Confirm the security prompt with Yes.
6. Select the new container from Containers on the General tab.
7. Save the changes.
Assigning extended properties to an Active Directory user account

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

To specify extended properties for a user account

1. In Manager, select Active Directory | User accounts.
2. Select the user account in the result list.
3. Select Assign extended properties.
4. Assign extended properties in Add assignments.
   
   **TIP:** In the Remove assignments area, you can remove the assignment of 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 follow on after a new user account has been created manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account’s target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

**NOTE:** It is not recommended to assign employees using automatic employee assignment in the case of administrative user accounts. Use Change master data to assign employees to administrative user account 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, enable the configuration parameter `TargetSystem | ADS | PersonAutoFullSync` and select the required mode.

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

- In the configuration parameter `TargetSystem | ADS | PersonExcludeList`, define the user accounts for which no automatic assignment to employees shall take place. Example:

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

- Use the configuration parameter `TargetSystem | ADS | PersonAutoDisabledAccounts` to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.

- Assign an account definition to the domain. Ensure 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 status.

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 the account definition and manage level to user accounts in linked status.
   a. In Manager, select Active Directory | User accounts | Linked but not configured | <Domain>.
   - OR -
   In Manager, select Active Directory | Contacts | Linked but not configured | <Domain>.
   b. Select Assign account definition to linked accounts.

For 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 40
- Assigning account definitions to a target system on page 55
- Editing search criteria for automatic employee assignment on page 127

Editing search criteria for automatic employee assignment

The criteria for employee assignment 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 assignment to administrative user accounts based on search criteria. Use Change master data to assign employees to administrative user account 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 category **Active Directory | Domains**.
2. Select the domain in the result list.
3. Select Define search criteria for employee assignment in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

**Table 48: Standard search criteria for user accounts and contacts**

<table>
<thead>
<tr>
<th>Apply to</th>
<th>Column for employee</th>
<th>Column for user account/contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory User accounts</td>
<td>Central user account (CentralAccount)</td>
<td>Login name (pre Win2000) (SAMAccountName)</td>
</tr>
<tr>
<td>Active Directory Contacts</td>
<td>Central user account (CentralAccount)</td>
<td>Name (Cn)</td>
</tr>
</tbody>
</table>

5. Save the changes.

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

In Assignments, 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 49: Manual Assignment View**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suggested assignments</td>
<td>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.</td>
</tr>
<tr>
<td>Assigned</td>
<td>This view lists all user accounts to which an employee is assigned.</td>
</tr>
</tbody>
</table>
### View Description

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>user accounts</strong></td>
<td>This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.</td>
</tr>
</tbody>
</table>

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

### To apply search criteria to user accounts

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

### To assign employees directly over a suggestion list

1. Click **Suggested assignments**.
   
   a. Click **Select** for all user accounts to 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 determined using the search criteria are assigned to the selected user accounts.

   - OR -

2. Click **No employee assignment**.
   
   a. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.
   
   b. Click **Select** for all user accounts to which you want to assign the selected employees. Multi-select is possible.
   
   c. Click **Assign selected**.
   
   d. Confirm the security prompt with **Yes**.
      
      The employees displayed in the **Employee** column are assigned to the selected user accounts.

### To remove assignments

1. Click **Assigned user accounts**.
   
   a. Click **Select** for all user accounts for which you want to delete the employee assignment. 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 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 125

### Updating employees when Active Directory user accounts 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 One Identity Manager to employee properties in Active Directory.

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

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 script `VI_PersonUpdate_ADSAccount`. Contact properties are mapped to employee properties using the script `ADS_PersonUpdate_ADSContact`. 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:

```vbscript
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 50: Configuration Parameter for Automatic Employee Assignment**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
</tbody>
</table>
To implement this method

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

Related topics

- Further identification data on page 119
- Automatic assignment of employees to Active Directory user accounts on page 125
- Updating employees when Active Directory user accounts are modified on page 130

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 manage level 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

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

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

For detailed information about disabling 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 40
- Setting up manage levels on page 43
- Deleting and restoring Active Directory user accounts on page 133

Deleting and restoring Active Directory user accounts

Objects in Active Directory such 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 via 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.
The 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 the 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 via 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 the One Identity Manager. The user account is immediately deleted in Active Directory. The user account is locked in One Identity Manager and once the retention time has expired it is finally deleted in the One Identity Manager database. The retention time is entered in the Retention time option in the domain. If a retention time has not been given, the deferred deletion time is applied.

**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 account 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 51: Configuration parameters for deleting user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>

### Configuring deferred deletion

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

Related topics

- Disabling Active Directory user accounts on page 132
- Deleting and restoring Active Directory contacts on page 145
- Active Directory security IDs on page 173
- Creating a synchronization project for initial synchronization of an Active Directory domain on page 21
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 137
- Linking user accounts to employees on page 98
- Supported user account types on page 99

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:

- To set up contacts for the employees of a company, we recommend that you use account definitions. 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 via 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 Active Directory | Contacts.
2. Select the contact in the result list and run Change master data.
   - 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.
2. Select the employee from the result list and run Active Directory Assign contacts from the task view.
3. Assign a contact.
   - OR -
   Select New contact and edit the master data.
4. Save the changes.

Detailed information about this topic

- General master data for Active Directory contacts on page 138
- Contact data for Active Directory contacts on page 140
- Further identification data on page 141
- Extensions data for an Active Directory contact on page 142

General master data for Active Directory contacts

Enter the following data on General:

Table 52: General Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>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.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **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** box. You can select all the account definitions assigned to this employee and through which no contact has been created for this employee. |
<p>| <strong>Manage level</strong>     | 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. |
| <strong>First name</strong>       | 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.                                                                 |
| <strong>Last name</strong>        | 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.                                                               |
| <strong>Initials</strong>         | The contact’s initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.                                                               |
| <strong>Title</strong>            | Contact’s academic title. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.                                                             |
| <strong>Display name</strong>     | The contact’s display name. The display name is made up of the contact’s first and last names.                                                                                                               |
| <strong>Structural object class</strong> | Structural object class representing the object type. By default, set up contacts with “Contact” in One Identity Manager.                                                                                     |
| <strong>Name</strong>             | The contact’s identifier. The identifier is made up of the contact’s first and last names.                                                                                                                |
| <strong>Distinguished name</strong> | Contact’s distinguished name. The distinguished name is formatted from the contact’s identifier and the container and cannot be changed.                                                                  |
| <strong>Domain</strong>           | Domain in which to create the contact.                                                                                                                                                                   |
| <strong>Container</strong>        | 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. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>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.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Maximum risk index value of all assigned groups. The property is only visible if the QER</td>
</tr>
<tr>
<td>Category</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Identity</td>
<td>Contact's type of identity.</td>
</tr>
<tr>
<td>Groups can be inherited</td>
<td>Specifies whether the employee's groups are inherited. If this option is set, contacts inherit groups through hierarchical roles.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related topics**

- Account definitions for Active Directory user accounts on page 40
- Supported user account types on page 99
- Linking user accounts to employees on page 98
- Active Directory group inheritance based on categories on page 168

**Contact data for Active Directory contacts**

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

**Table 53: Contact Data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Telephone number.</td>
</tr>
<tr>
<td>Phone private</td>
<td>Private telephone number.</td>
</tr>
<tr>
<td>Fax</td>
<td>Fax number.</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>Mobile number.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Pager</td>
<td>Pager number.</td>
</tr>
<tr>
<td>Web page</td>
<td>Website.</td>
</tr>
<tr>
<td>IP telephone</td>
<td>IP telephone number.</td>
</tr>
<tr>
<td>number.</td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

**Further identification data**

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

**Table 54: Master data for identification**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office</td>
<td>Office</td>
</tr>
<tr>
<td>Street</td>
<td>Street or road.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>Mailbox</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code</td>
</tr>
<tr>
<td>City</td>
<td>City</td>
</tr>
<tr>
<td>State</td>
<td>State</td>
</tr>
<tr>
<td>Country ID</td>
<td>The country ID</td>
</tr>
<tr>
<td>Company</td>
<td>Employee’s company</td>
</tr>
<tr>
<td>Department</td>
<td>Employee’s department</td>
</tr>
<tr>
<td>Job description</td>
<td>Job description</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Employee's unique marker, for example their ID.</td>
</tr>
<tr>
<td>Account manager</td>
<td>Manager responsible for the contact.</td>
</tr>
</tbody>
</table>

**To specify an account manager**

1. Click next to the text box.
2. Under Table, select the table which maps the account manager.
3. Select the manager under Account manager.
4. Click OK.
Extensions data for an Active Directory contact

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

Table 55: Extensions data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensions data</td>
<td>Custom extension data in binary format.</td>
</tr>
<tr>
<td>Attribute extension 01 - attribute extension 15</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

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 Active Directory | Contacts.
2. Select the contact in the result list.
3. Select Active Directory contact overview.

Changing the manage level of an Active Directory contact

The Unmanaged manage level is used when you create contacts via automatic employee assignment. You can change the contact’s manage level later.
To change the manage level for a contact

1. Select Active Directory | Contacts.
2. Select the contact in the result list.
3. Select Change master data.
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 carried out by allocating the employee and groups in company structures, like 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 Active Directory | Contacts.
2. Select the contact in the result list.
3. Select Assign groups in the task view.
4. Assign groups in Add assignments.

   ! TIP: you can remove the assignment of groups in the Remove assignments area.

   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 153
• Validity of group memberships on page 151
Assigning a 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 **Active Directory | Contacts**.
2. Select the contact in the result list.
3. Select the task **Assign secretaries**.
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. Assign secretaries in **Add assignments**.
   - OR -
   Remove secretaries from **Remove assignments**.
6. Save the changes.

Moving an Active Directory contact

**NOTE:** Contacts can only be moved within an domain.

**To move a contact**

1. Select **Active Directory | Contacts**.
2. Select the contact in the result list.
3. Select **Change master data**.
4. Select **Active Directory Change container** in the task view
5. Confirm the security prompt with **Yes**.
6. Select the new container from **Containers on the General** tab.
7. Save the changes.
Assigning extended properties to an Active Directory contact

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

To assign extended properties for a contact

1. Select Active Directory | Contacts.
2. Select the contact in the result list.
3. Select Assign extended properties in the task view.
4. Assign extended properties in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of 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 133.

**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 Active Directory | Contacts.
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 Active Directory | Contacts.
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 the delete delay has expired. You can configure an alternative delay on the table ADSContact in Designer.
Active Directory groups

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

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 148
- Validity of group memberships on page 151
**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 **Change master data**.
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 an Active Directory group on page 148
- Extensions data for Active Directory groups on page 150

**General master data for an Active Directory group**

Enter the following data on **General**:

Table 56: General Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group The group identifier is used to form the group name for previous <strong>group name (pre Win2000)</strong> versions.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in which to create the group.</td>
</tr>
<tr>
<td>Container</td>
<td>Container in which to create the group.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>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.</td>
</tr>
<tr>
<td>Display name</td>
<td>The display name is used to display the group in the One Identity Manager tools user interface.</td>
</tr>
<tr>
<td>Group name (pre Win2000)</td>
<td>Name of the group for the previous versions. The group name is taken from the group identifier.</td>
</tr>
<tr>
<td>Structural object class</td>
<td>Structural object class representing the object type. By default, you set up groups in the One Identity Manager with the object class GROUP.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Object class</td>
<td>List of classes defining the attributes for this object. The object classes listed are imported from the database during synchronization with the Active Directory environment. However, you can add object classes and auxiliary classes in the input field that are used by other LDAP and X.500 directory services.</td>
</tr>
<tr>
<td>Account manager</td>
<td>Manager responsible for the group.</td>
</tr>
<tr>
<td><strong>To specify an account manager</strong></td>
<td></td>
</tr>
<tr>
<td>1. Click next to the text box.</td>
<td></td>
</tr>
<tr>
<td>2. Under Table, select the table which maps the account manager.</td>
<td></td>
</tr>
<tr>
<td>3. Select the manager under Account manager.</td>
<td></td>
</tr>
<tr>
<td>4. Click OK.</td>
<td></td>
</tr>
<tr>
<td>Group manager can update members list.</td>
<td>Specifies whether the account manager can change memberships for these groups.</td>
</tr>
<tr>
<td>Email address</td>
<td>Group's email address</td>
</tr>
<tr>
<td>Risk index</td>
<td>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 configuration parameter QER</td>
</tr>
<tr>
<td>Category</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Remark</td>
<td>Spare text box for additional explanation. Abbreviations for combinations of group type and group area are added in the comment and should not be changed.</td>
</tr>
<tr>
<td>Security group</td>
<td>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.</td>
</tr>
<tr>
<td>Distribution group</td>
<td>Group type. Distribution groups can be used as email distribution groups. Distribution groups do not have any security.</td>
</tr>
</tbody>
</table>
### 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 no 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 168
- For 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 57: Extensions data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute extension 01 - attribute extension 15</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>
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 58: Group memberships permitted within a domain

<table>
<thead>
<tr>
<th>Target Group</th>
<th>Member in target group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td></td>
</tr>
<tr>
<td>Global</td>
<td></td>
</tr>
<tr>
<td>Universal</td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Global</td>
<td></td>
</tr>
<tr>
<td>Universal</td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td></td>
</tr>
</tbody>
</table>
### Table 59: Group memberships permitted within a hierarchical domain structure

<table>
<thead>
<tr>
<th>Target Group</th>
<th>Member in target group</th>
<th>User account</th>
<th>Contact</th>
<th>Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>G U L</td>
<td>G U L</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td>x x x</td>
<td>x x x</td>
</tr>
<tr>
<td></td>
<td>Universal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Universal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 60: Group memberships permitted within a forest

<table>
<thead>
<tr>
<th>Target Group</th>
<th>Member in target group</th>
<th>User account</th>
<th>Contact</th>
<th>Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>G U L</td>
<td>G U L</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Universal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Universal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x x x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 61: Group memberships permitted between forests

<table>
<thead>
<tr>
<th>Target Group</th>
<th>Member in target group</th>
<th>Group</th>
<th>Distribution</th>
<th>Security</th>
<th>User account</th>
<th>Contact</th>
<th>Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>G  U  L</td>
<td>G  U  L</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Universal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Security</td>
<td>Global</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Universal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Related topics
- Trusted Active Directory domains on page 91
- Active Directory specific master data for an Active Directory domain on page 88

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 indirect assignment of employees to user accounts:

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

Groups can also be requested in 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 154
- Assigning Active Directory groups to business roles on page 156
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
- Assigning Active Directory computers directly to an Active Directory group on page 159
- Adding Active Directory groups to system roles on page 160
- Adding Active Directory groups to the IT Shop on page 161
- Adding Active Directory groups automatically to the IT Shop on page 162
- 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 Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.

**TIP:** In the Remove assignments area, you can remove the assignment of 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. Select Organizations | Departments in Manager.
   - OR -
   Select Organizations | Cost centers in Manager.
   - OR -
   In Manager, select Organizations | Locations.
2. Select the department, cost center or location in the result list.
3. Select the Assign Active Directory groups task.
4. Assign groups in Add assignments.

**TIP:** you can remove the assignment of groups in the Remove assignments area.

**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 156
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
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 Assign business roles in the task view.
4. Assign business roles in Add assignments.
   
   | TIP: In the Remove assignments area, you can remove the assignment of 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 Manager, select Business roles | <role class>.
2. Select the business role in the result list.
3. Select Assign Active Directory groups.
4. Assign groups in Add assignments.
   
   | TIP: you can remove the assignment of groups in the Remove assignments area.
   
   | **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 154
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
- Assigning Active Directory computers directly to an Active Directory group on page 159
- Adding Active Directory groups to system roles on page 160
- Adding Active Directory groups to the IT Shop on page 161
- Adding Active Directory groups automatically to the IT Shop on page 162
- One Identity Manager users for managing an Active Directory environment on page 10

Assigning Active Directory user accounts directly to an Active Directory group

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is carried out by allocating the employee and groups in company structures, like departments, cost centers, locations or business roles. If the employee has a user account in 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 Assign user accounts in the task view.
4. Assign user accounts in Add assignments.
   
   TIP: In the Remove assignments area, you can remove the assignment of 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.
Assigning Active Directory contacts directly to an Active Directory group

Groups can be assigned directly or indirectly to a contact. Indirect assignment is carried out by allocating the employee and groups in company structures, like departments, cost centers, locations or business roles. If the employee has a 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 Active Directory | Groups.
2. Select the group in the result list.
3. Select Assign contacts in the task view.
4. Assign the contacts in Add assignments.
   - OR -
   Remove the contacts in Remove assignments.
5. Save the changes.

Related topics
- Assigning Active Directory groups directly to an Active Directory contact on page 143
- Assigning Active Directory groups to departments, cost centers, and locations on page 154
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 Active Directory | Groups.
2. Select the group in the result list.
3. Select Assign computers in the task view.
4. Assign the computers in Add assignments.
   - OR -
   Remove the computers in Remove assignments.
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 180
- Assigning Active Directory groups to departments, cost centers, and locations on page 154
- Assigning Active Directory groups to business roles on page 156
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
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 **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

**TIP:** In the **Remove assignments** area, you can remove the assignment of 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 154
- Assigning Active Directory groups to business roles on page 156
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
Assigning Active Directory computers directly to an Active Directory group on page 159

Adding Active Directory groups to the IT Shop on page 161

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

Adding Active Directory groups to the IT Shop

When you assign a group to a 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 marked with the IT Shop option.
- the group must be assigned a service item.

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

- If you only want it to be possible for 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 IT Shop.

1. In Manager select the **Active Directory | Groups** category (non-role-based login).
   - OR -
   1. In Manager, select **Entitlements | Active Directory groups** (role-based login).
2. In the result list, select the group.
3. Select **Add to IT Shop**.
4. In **Add assignments**, 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 Manager select the **Active Directory | Groups** category (non-role-based login).
   - OR -
   1. In Manager, select **Entitlements | Active Directory groups** (role-based login).
2. In the result list, select the group.
3. Select **Add to IT Shop**.
4. In **Remove assignments**, 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 Manager select the **Active Directory | Groups** category (non-role-based login).
   - OR -
     In Manager, select **Entitlements | Active Directory groups** (role-based login).
2. In the result list, select the group.
3. Select **Remove from all shelves (IT Shop)**.
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 request from company resources through the IT Shop, see the **One Identity Manager IT Shop Administration Guide**.

Related topics

- General master data for an Active Directory group on page 148
- Adding Active Directory groups automatically to the IT Shop on page 162
- Assigning Active Directory groups to departments, cost centers, and locations on page 154
- Assigning Active Directory groups to business roles on page 156
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
- Assigning Active Directory computers directly to an Active Directory group on page 159
- Adding Active Directory groups to system roles on page 160

Adding Active Directory groups automatically to the IT Shop

Table 62: Configuration parameter for automatically add groups in the IT Shop

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| QER | ITShop | Preprocessor relevant configuration parameter for automatically
### Configuration parameter

<table>
<thead>
<tr>
<th>GroupAutoPublish</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QER</th>
<th>ITShop</th>
<th>GroupAutoPublish</th>
<th>ADSGroupExcludeList</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 (</td>
<td>) delimited list that is handled as a regular search pattern.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example: .<em>Administrator.</em></td>
<td>Exchange.*</td>
<td>.*Admins</td>
<td>.*Operators</td>
</tr>
</tbody>
</table>

### To add groups automatically to IT Shop

1. Enable the **QER | ITShop | GroupAutoPublish** configuration parameter in Designer.
2. Enable the **QER | ITShop | GroupAutoPublish | ADSGroupExcludeList** configuration parameter in Designer and specify the Active Directory groups that are not to be added automatically to 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 step 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 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 owner, 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 owner, 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 161
- Assigning Active Directory groups to departments, cost centers, and locations on page 154
- Assigning Active Directory groups to business roles on page 156
- Assigning Active Directory user accounts directly to an Active Directory group on page 157
- Assigning Active Directory contacts directly to an Active Directory group on page 158
- Assigning Active Directory computers directly to an Active Directory group on page 159
- Adding Active Directory groups to system roles on page 160
- 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 Active Directory | Groups.
2. Select the group in the result list.
3. Select Active Directory group overview in the task view.

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 Assign groups.
4. Assign the groups that are are subordinate to the selected group in Add assignments.

TIP: you can remove the assignment of groups in the Remove assignments area.

To remove an assignment
- Select the group and double click ☑.

5. Save the changes.

Related topics
- Validity of group memberships on page 151
Effectiveness of group memberships

Table 63: Configuration Parameter for Conditional Inheritance

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER Structures Inherite GroupExclusion</td>
<td>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 the parameter require recompiling the database.</td>
</tr>
</tbody>
</table>

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

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

**NOTE:**

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

The effectiveness of the assignments is mapped in the ADSAccountInADSGroup and BaseTreeHasADSGroup via the column XIsInEffect.

Example of the effect of group memberships

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

Clara Harris has a user account in this domain. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B and C.
By using suitable controls, you want to prevent an employee from being able to trigger a request and to pay invoices. That means, groups A, B and C are mutually exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 64: Specifying excluded groups (table ADSGroupExclusionAADGroupExclusion)

<table>
<thead>
<tr>
<th>Effective Group</th>
<th>Excluded Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td></td>
</tr>
<tr>
<td>Group B</td>
<td>Group A</td>
</tr>
<tr>
<td>Group C</td>
<td>Group B</td>
</tr>
</tbody>
</table>

Table 65: Effective Assignments

<table>
<thead>
<tr>
<th>Employee</th>
<th>Member in Role</th>
<th>Effective Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ben King</td>
<td>Marketing</td>
<td>Group A</td>
</tr>
<tr>
<td>Jan Bloggs</td>
<td>Marketing, finance</td>
<td>Group B</td>
</tr>
<tr>
<td>Clara Harris</td>
<td>Marketing, finance, control group</td>
<td>Group C</td>
</tr>
<tr>
<td>Jenny Basset</td>
<td>Marketing, control group</td>
<td>Group A, Group C</td>
</tr>
</tbody>
</table>

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

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

Table 66: Excluded groups and effective assignments

<table>
<thead>
<tr>
<th>Employee</th>
<th>Member in Role</th>
<th>Assigned Group</th>
<th>Excluded Group</th>
<th>Effective Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jenny Basset</td>
<td>Marketing</td>
<td>Group A</td>
<td>Group B</td>
<td>Group C</td>
</tr>
<tr>
<td></td>
<td>Control group</td>
<td>Group C</td>
<td>Group A</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisites

- The configuration parameter **QER | Structures | Inherit | GroupExclusion** is enabled.
- 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 **Exclude groups**.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.
   - OR -
   In **Remove assignments**, 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 category positions **Position 1 to Position 31**.

Every user account (contact) can be assigned to one or more categories. Each group can also be assigned to one or more categories. The structural profile is inherited by the user account (contact) when at least one user account (contact) category item matches an assigned structural profile. 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 67: Category Examples

<table>
<thead>
<tr>
<th>Category Position</th>
<th>Categories for User Accounts</th>
<th>Categories for Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default user</td>
<td>Default permissions</td>
</tr>
<tr>
<td>2</td>
<td>System user</td>
<td>System user permissions</td>
</tr>
<tr>
<td>3</td>
<td>System administrator</td>
<td>System administrator permissions</td>
</tr>
</tbody>
</table>

Figure 2: Example of inheriting through categories.

![Diagram showing user and permission categories and resulting group memberships]

Key:
- Inherit due to matching categories
- Inherit because user account is not categorized
- Inherit 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 90
- General master data of an Active Directory user account on page 107
- General master data for Active Directory contacts on page 138
- General master data for an Active Directory group on page 148

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 Assign account policies in the task view.
4. Assign the account policies in Add assignments.
   - OR -
   Remove the account policies in Remove assignments.
5. Save the changes.

Related topics

- Active Directory account policies for Active Directory domains on page 92
- Global account policies for an Active Directory domain on page 87
- Assigning Active Directory account policies to an Active Directory user account on page 122
Assigning a secretary 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 *Active Directory | Groups.*
2. Select the group in the result list.
3. Select *Assign secretaries* in the task view.
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. Assign secretaries in *Add assignments.*
   - OR -
   Remove secretaries from *Remove assignments.*
6. Save the changes.

Moving an Active Directory group

*NOTE:* You can only move groups within a domain.

**To move a group**

1. Select *Active Directory | Groups.*
2. Select the group in the result list.
3. Select *Change master data.*
4. Select *Active Directory Change container* in the task view
5. Confirm the security prompt with *Yes.*
6. Select the new container from *Containers* on the *General* tab.
7. Save the changes.
Assigning extended properties to an Active Directory group

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

To specify extended properties for a group

1. In the Manager, select the Active Directory | Groups category.
2. Select the group in the result list.
3. Select Assign extended properties.
4. Assign extended properties in Add assignments.

TIP: In the Remove assignments area, you can remove the assignment of 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 category Active Directory | Groups.
2. Select the group in the result list.
3. Delete the group using 🗑.
4. Confirm the security prompt with Yes.

The group is deleted completely from the One Identity Manager database and from 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 173.
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 Active Directory | Active Directory SIDs.

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

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. Select Active Directory | Container.
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 174

Master data for an Active Directory container

Enter the following data for a container.
Table 68: Master Data for a Container

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Container name.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>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.</td>
</tr>
<tr>
<td>Structural object class</td>
<td>Structural object class representing the object type.</td>
</tr>
<tr>
<td>Object class</td>
<td>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.</td>
</tr>
<tr>
<td>Domain</td>
<td>Container domain.</td>
</tr>
<tr>
<td>Parent container</td>
<td>Parent container for mapping a hierarchical container structure. The distinguished name is automatically updated using templates.</td>
</tr>
<tr>
<td>Account manager</td>
<td>Manager responsible for the container.</td>
</tr>
<tr>
<td>To specify an account manager</td>
<td>1. Click ➔ next to the text box.</td>
</tr>
<tr>
<td></td>
<td>2. Under Table, select the table which maps the account manager.</td>
</tr>
<tr>
<td></td>
<td>3. Select the manager under Account manager.</td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
</tr>
<tr>
<td>Target system manager</td>
<td>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.</td>
</tr>
<tr>
<td>Street</td>
<td>Street or road.</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Location.</td>
</tr>
<tr>
<td>State</td>
<td>State.</td>
</tr>
<tr>
<td>Country ID</td>
<td>The country ID.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Extended Function</td>
<td>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.</td>
</tr>
<tr>
<td>Protected from accidental deletion</td>
<td>Specifies whether to protect the container against accidental deletion. If this option is set, delete permissions are removed from the container object.</td>
</tr>
</tbody>
</table>

**Related topics**

- [Target system managers](#) on page 71

---

## 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 Active Directory | Container.
2. Select the container in the result list.
3. Select Active Directory container overview.

### Moving an Active Directory container

**NOTE:** You can only move containers within a domain.
To move a container

1. Select Active Directory | Container.
2. Select the container in the result list.
3. Select Change master data.
4. Select Active Directory Change container in the task view.
5. Confirm the security prompt with Yes.
6. Select the new container from Containers on the General tab.
7. Save the changes.
Active Directory computers

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

To edit computer master data

2. Select the computer in the result list and run Change master data.
   - 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 178
- Editing a server on page 73

Master data for an Active Directory computer

Enter the following data for a computer.

Table 69: Computer master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device   | The computer is connected to this device. Specify a new device using the 🍃 button next to the menu.   
<p>|          | For detailed information about rule checking, see the One Identity Manager Identity Management Base Module Administration Guide. |</p>
<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Computer identifier</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in which to create the computer.</td>
</tr>
<tr>
<td>Container</td>
<td>Container in which to create the computer. The distinguished name of the computer is determined by a template when the container is selected.</td>
</tr>
<tr>
<td>Primary group</td>
<td>Computer's primary group. Then, only groups that are already assigned to the computer can be selected.</td>
</tr>
</tbody>
</table>
| Account manager | Manager responsible for the computer. **To specify an account manager**  
1. Click ➔ next to the text box.  
2. Under **Table**, select the table which maps the account manager.  
3. Select the manager under **Account manager**.  
4. Click **OK**. |
| 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

2. Select the computer in the result list.
3. Select Active Directory computer overview in the task view.

Moving an Active Directory computer

**NOTE:** Computers can only be moved within an domain.

To move a computer

2. Select the computer in the result list.
3. Select Change master data.
4. Select Active Directory Change container in the task view
5. Confirm the security prompt with Yes.
6. Select the new container from Containers 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

2. Select the computer in the result list.
3. Select Assign groups in the task view.
4. Assign groups in **Add assignments**.

   **TIP:** you can remove the assignment of groups in the **Remove assignments** area.

   **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 153
- Validity of group memberships on page 151
- Master data for an Active Directory computer on page 178

**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 70: Diagnostics tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostics - Browse</td>
<td>This opens a Window Explorer window. All shares for the selected computer are shown.</td>
</tr>
<tr>
<td>Diagnostics - Windows</td>
<td>This opens the system information (winmsd.exe or msinfo32.exe) for the computer.</td>
</tr>
<tr>
<td>Diagnostics - Computer</td>
<td>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.</td>
</tr>
</tbody>
</table>

**To run diagnostics for a computer**

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

It is important for the administration of printers, to remember that printers are physically present in the network. All shared printers of a domain are read into One Identity Manager during synchronization.

To display a printer

1. Select **Active Directory | Printers**.
2. Select a printer in the result list and select the **Change master data** task.
   - OR -
   Click 🔄 in the result list.

Following information is displayed for a printer.

**Table 71: Printer master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printer name</td>
<td>Name of the printer.</td>
</tr>
<tr>
<td>Driver</td>
<td>Printer driver identifier.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Computer or server to which the printer is connected.</td>
</tr>
<tr>
<td>computer</td>
<td></td>
</tr>
<tr>
<td>Full server name</td>
<td>Full name of the server to which the printer is connected.</td>
</tr>
<tr>
<td>Server</td>
<td>Server's short name.</td>
</tr>
<tr>
<td>Port</td>
<td>Printer connection.</td>
</tr>
<tr>
<td>UNC name</td>
<td>Universal Naming Convention (UNC) address of the printer.</td>
</tr>
<tr>
<td>Location description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Specifies whether double sided printing is supported.</td>
</tr>
<tr>
<td>Color</td>
<td>Specifies whether color is supported.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supports sorter</td>
<td>Defines whether the printer supports a sorter.</td>
</tr>
<tr>
<td>Pages per minute</td>
<td>Printer speed in page per minute.</td>
</tr>
<tr>
<td>Max. resolution [dpi]</td>
<td>Maximum printer resolution in dpi.</td>
</tr>
<tr>
<td>Max. horizontal resolution</td>
<td>Maximum printer resolution along the X-axis (width).</td>
</tr>
<tr>
<td>Max. vertical resolution</td>
<td>Maximum printer resolution along the Y-axis (height).</td>
</tr>
<tr>
<td>Spare field no. 01 ... Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>
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 **Active Directory | Locations**.
2. Select the location in the result list.
3. To display a location's server, select **Location overview** in the task view.
4. To display a location's master data, select **Change master data** in the task view.

Following information about locations is displayed.

**Table 72: Location master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Location name.</td>
</tr>
<tr>
<td>Canonical name</td>
<td>The location's canonical name</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Location description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Forest</td>
<td>The name of the Forest to which this location belongs.</td>
</tr>
<tr>
<td>subnets</td>
<td>IP address range at this location.</td>
</tr>
</tbody>
</table>

**Related topics**

- Information about the Active Directory forest on page 90
Active Directory object reports

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 73: Reports for the Target System

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of all assignments (domain)</td>
<td>This report finds all roles containing employees with at least one user account in the selected domain.</td>
</tr>
<tr>
<td>Overview of all assignments (container)</td>
<td>This report finds all roles containing employees with at least one user account in the selected container.</td>
</tr>
<tr>
<td>Overview of all assignments (group)</td>
<td>This report finds all roles containing employees with the selected group.</td>
</tr>
<tr>
<td>Show orphaned user accounts</td>
<td>This report shows all user accounts in the domain, which are not assigned to an employee. The report contains group memberships and risk assessment.</td>
</tr>
<tr>
<td>Show employees with multiple user accounts</td>
<td>This report shows all employees with more than one user account in the domain. The report contains a risk assessment.</td>
</tr>
<tr>
<td>Show unused user accounts</td>
<td>This report shows all user accounts in the domain, which have not been used in the last few months. The report contains group memberships and risk assessment.</td>
</tr>
<tr>
<td>Show system entitlement drifts</td>
<td>This report shows all groups in the domain that are the result of manual operations in the target system rather than using the One Identity Manager.</td>
</tr>
<tr>
<td>Show user accounts with an above average number of system entitlements</td>
<td>This report contains all user accounts in the domain with an above average number of group memberships.</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active Directory user account and group</td>
<td>This report contains a summary of user account and group distribution in all domains. You can find this report in My One Identity Manager.</td>
</tr>
<tr>
<td>administration</td>
<td></td>
</tr>
<tr>
<td>Data quality summary for Active Directory</td>
<td>This report contains different evaluations of user account data quality in all domains. You can find this report in My One Identity Manager.</td>
</tr>
<tr>
<td>user accounts</td>
<td></td>
</tr>
</tbody>
</table>

**Related topics**

- [Overview of all assignments](#) on page 186

---

**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 employee 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 report **Overview of all assignments**.
- Click the Span 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 `v` button in a role’s control, you display all employees in the role with the base object.
- Use the small arrow next to `v` to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="i icon" /></td>
<td>Show the legend with the meaning of the report control elements</td>
</tr>
<tr>
<td><img src="image" alt="save icon" /></td>
<td>Saves the current report view as a graphic.</td>
</tr>
<tr>
<td><img src="image" alt="role class icon" /></td>
<td>Selects the role class used to generate the report.</td>
</tr>
<tr>
<td><img src="image" alt="display roles icon" /></td>
<td>Displays all roles or only the affected roles.</td>
</tr>
</tbody>
</table>

**Table 74: Meaning of Icons in the Report Toolbar**
Appendix: Configuration parameters for managing Active Directory

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

Table 75: Configuration parameters

<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>ITShop</td>
</tr>
<tr>
<td>QER</td>
<td>ITShop</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
</tbody>
</table>
### Configuration parameters

<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td>ProfileFixedString</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>Example:</td>
<td>MyDomain</td>
</tr>
<tr>
<td>For detailed information about the One Identity Manager authentication modules, see the One Identity Manager Authorization and Authentication Guide.</td>
<td></td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
</tbody>
</table>
| TargetSystem | ADS | | This configuration parameter specifies the mode for automatic
<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PersonAutoFullSync</td>
<td>Employee assignment for user accounts added to or updated in the database through synchronization.</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
</tbody>
</table>
Appendix: 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 76: Mapping Active Directory schema types to tables in the One Identity Manager schema.

<table>
<thead>
<tr>
<th>Schema type in Active Directory</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>builtInDomain</td>
<td>ADSContainer</td>
</tr>
<tr>
<td>computer</td>
<td>ADSMachine</td>
</tr>
<tr>
<td>contact</td>
<td>ADSContact</td>
</tr>
<tr>
<td>container</td>
<td>ADSContainer</td>
</tr>
<tr>
<td>domainDNS</td>
<td>ADSDomain</td>
</tr>
<tr>
<td>forest (virtual schema type)</td>
<td>ADSForest</td>
</tr>
<tr>
<td>group</td>
<td>ADSGroup</td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td>ADSAccount</td>
</tr>
<tr>
<td>msDS-PasswordSettings</td>
<td>ADSPolicy</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>ADSContainer</td>
</tr>
<tr>
<td>printQueue</td>
<td>ADSPrinter</td>
</tr>
<tr>
<td>serverInSite</td>
<td>ADSMachineInADSSite</td>
</tr>
<tr>
<td>Schema type in Active Directory</td>
<td>Table in the One Identity Manager Schema</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Site</td>
<td>ADSSSite</td>
</tr>
<tr>
<td>trustedDomain</td>
<td>DomainTrustsDomain</td>
</tr>
<tr>
<td>user</td>
<td>ADSAccount</td>
</tr>
</tbody>
</table>
One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

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

Technical support resources

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

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

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product
A
account definition 40
   add to IT Shop 54
   assign automatically 52
   assign to Active Directory domain 55
   assign to all persons 52
   assign to business role 51
   assign to department 50
   assign to employee 49, 52
   assign to location 50
   create 40
   delete 56
   IT operating data 45, 47
   manage level 43
account definitions
   assign to system roles 53
Active Directory account policy 87
   assign to groups 94, 170
   assign to user accounts 94, 122
   set up 92
Active Directory computer
   account manager 178
   assign group 159, 180
   change container 180
   computer name 178
   container 178
   device 178
   diagnostics 181
   DNS host 178
   domain 178
   edit 178
move 180
   primary group 159, 178, 180
Active Directory contact
   account definition 55, 138
   account manager 141
   assign employee 137
   assign employees 138
   assign extended properties 145
   assign group 158
   assign groups 143
   category 138
   change container 144
   contact data 140
   container 138
   delete 145
   department 141
   domain 138
   employee 138
   extensions data 142
   identification 141
   identity 138
   inherintg groups 138
   location 141
   lock 145
   manage 137
   manage level 138, 142
   move 144
   name 138
   primary group 138
   restore 145
   risk index 138
Active Directory container
- account manager 174
- change container 176
- domain 174
- edit 174
- manage 174
- monitor memberships 96
- move 176
- object class 174
- target system manager 71, 174

Active Directory domain
- account definition 85
- account definition (initial) 55
- account manager 88
- account policies 87, 92
- application roles 10
- category 90, 168
- contact definition 85
- contact definition (initial) 55
- domain name 88
- domain type 85
- edit 85
- employee assignment 127
- functional level 85
- NetBIOS name 85
- overall structure 88
- overview of all assignments 186
- recycle bin 85
- reports 185
- set up 85
- synchronization 85
- target system manager 85
- target system managers 10, 71

Active Directory group
- account manager 148
- add to IT Shop 161
- add to IT Shop (automatically) 162
- add to system role 160
- assign account policy 170
- assign computer 153, 159, 180
- assign contact 153, 158
- assign extended properties 172
- assign group 165
- assign to business roles 156
- assign to cost center 154
- assign to department 154
- assign to location 154
- assign user account 123, 153, 157
- category 148, 168
- change container 171
- container 148
- delete 172
- distribution group 147-148
- domain 148
- edit 148
- effective 166
- exclude 166
- global 147-148
- group area 147
- group moving 171
- group type 147
- local domain 147-148
- manage 147
- monitor memberships 96
- object class 148
- permitted memberships 151
architecture overview 9
assign account definition to cost center 50

C
configuration parameter 188

D
direction of synchronization
to Manager 21
to target system 21

E
e-mail notification 69
employee assignment
  automatic 125
  manual 128
  removing 128
  search criterion 127
  table column 127
exclusion definition 166

F
firewall configuration 17

H
home server 78
  home directory 78, 80, 82
HomePost.cmd 79
HomePre.cmd 79
Homeserver
  home directory 79

I
identity 99
installation prerequisites 17
IT operating data
  change 48
IT Shop shelf
  assign account definition 54

J
Job server
  process 18

L
logon information 69

M
membership
  change provisioning 35

N
notification 69

O
object
  delete immediately 33
  outstanding 33
  publish 33
One Identity Manager
  administrator 10
  target system administrator 10
  target system manager 10, 71, 174
user 10
outstanding object 33

P
password
  initial 69
password policy 58
  assign 60
  character classes 64
  check password 68
  default policy 60, 62
  display name 62
  editing 62
  error message 62
  excluded list 67
  failed logins 63
  generate password 68
  generation script 65-66
  initial password 63
  name properties 63
  password age 63
  password cycle 63
  password length 63
  password strength 63
  predefined 58
  test script 65
ports 17
product owner 162
profile server 78
  profile directory 78, 80, 82
project template 193
provisioning
  member list 35

R
revision filter 32

S
schedule
  deactivation 37
schema
  changes 31
  compress 31
  update 31
start synchronization 21
synchronization
  accelerate 32
  base object
    create 30
  configuration 28
  configure 21
  connection parameters 21, 28, 30
  extended schema 30
  multiple domains 30
  permissions 14
  prevent 37
  scope 28
  set up 13
synchronization project
  create 21
target system schema 30
users 14
variable 28
variable set 30
workflow 21, 30
synchronization analysis report 36
synchronization configuration 30
adjust 30
customize 28, 30
synchronization direction

to target system 30
synchronization log 28
synchronization project
create 21
deactivation 37edit 95
project template 193
synchronization server
configure 18
install 18
Job server 18
synchronization workflow
create 21
set up 30

T

target system reconciliation 33
template
  IT operating data, modify 48

U

user account
  administrative user account 102-103
  apply template 48
default user account 101
identity 99
password
  notification 69
privileged user account 99, 104
type 99