One Identity Manager 8.1.1

Administration Guide for Connecting to LDAP
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 NONINFRINGEMENT. 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] An information icon indicates supporting information.

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

**Managing LDAP environments** .................................................. 7  
Architecture overview ............................................................... 7  
One Identity Manager users for managing an LDAP environment ........ 8

**Setting up LDAP directory synchronization** .............................. 11  
Users and permissions for synchronizing with an LDAP directory ........ 12  
  Special cases for synchronizing an Active Directory Lightweight Directory Service .. 13  
Setting up the synchronization server ......................................... 14  
Creating a synchronization project for initial synchronization of a LDAP domain .... 17  
Displaying synchronization results ............................................... 28  
Customizing synchronization configuration ................................... 29  
  Configuring synchronization in LDAP domains .......................... 31  
  Configuring synchronization of several LDAP domains ............... 31  
  Updating schemas .............................................................. 32  
Speeding up synchronization with revision filtering ...................... 33  
Post-processing outstanding objects .......................................... 34  
Configuring the provisioning of memberships ............................. 36  
Help for the analysis of synchronization issues ............................ 37  
Disabling synchronization ....................................................... 38

**Basic configuration data** ....................................................... 39  
Setting up account definitions .................................................. 40  
  Creating an account definition .............................................. 41  
  Master data for an account definition .................................. 41  
Setting up manage levels .......................................................... 43  
  Master data for a manage level ............................................ 45  
Creating a mapping rule for IT operating data ............................. 46  
Determining IT operating data .................................................. 48  
Modify IT operating data .......................................................... 49  
Assigning account definitions to employees .............................. 50  
  Assigning account definitions to departments, cost centers, and locations .... 51  
  Assigning account definitions to business roles ....................... 52  
  Assigning account definitions to all employees ....................... 53
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning account definitions directly to employees</td>
<td>53</td>
</tr>
<tr>
<td>Assigning account definitions to system roles</td>
<td>54</td>
</tr>
<tr>
<td>Adding account definitions in the IT Shop</td>
<td>54</td>
</tr>
<tr>
<td>Assigning account definitions to a target system</td>
<td>56</td>
</tr>
<tr>
<td>Deleting an account definition</td>
<td>57</td>
</tr>
<tr>
<td>Password policies for LDAP user accounts</td>
<td>59</td>
</tr>
<tr>
<td>Predefined password policies</td>
<td>59</td>
</tr>
<tr>
<td>Using a password policy</td>
<td>60</td>
</tr>
<tr>
<td>Editing password policies</td>
<td>63</td>
</tr>
<tr>
<td>General master data for a password policy</td>
<td>63</td>
</tr>
<tr>
<td>Policy settings</td>
<td>64</td>
</tr>
<tr>
<td>Character classes for passwords</td>
<td>65</td>
</tr>
<tr>
<td>Custom scripts for password requirements</td>
<td>66</td>
</tr>
<tr>
<td>Script for checking a password</td>
<td>66</td>
</tr>
<tr>
<td>Script for generating a password</td>
<td>67</td>
</tr>
<tr>
<td>Deny list for passwords</td>
<td>68</td>
</tr>
<tr>
<td>Checking a password</td>
<td>69</td>
</tr>
<tr>
<td>Testing generation of a password</td>
<td>69</td>
</tr>
<tr>
<td>Initial password for new LDAP user accounts</td>
<td>69</td>
</tr>
<tr>
<td>Email notifications about login data</td>
<td>70</td>
</tr>
<tr>
<td>Target system managers</td>
<td>71</td>
</tr>
<tr>
<td><strong>LDAP domains</strong></td>
<td>74</td>
</tr>
<tr>
<td>General master data for a LDAP domain</td>
<td>74</td>
</tr>
<tr>
<td>LDAP specific master data for an LDAP domain</td>
<td>76</td>
</tr>
<tr>
<td>Specifying categories for inheriting LDAP groups</td>
<td>77</td>
</tr>
<tr>
<td>Editing a synchronization project</td>
<td>77</td>
</tr>
<tr>
<td><strong>LDAP user accounts</strong></td>
<td>79</td>
</tr>
<tr>
<td>Linking user accounts to employees</td>
<td>79</td>
</tr>
<tr>
<td>Supported user account types</td>
<td>80</td>
</tr>
<tr>
<td>Default user accounts</td>
<td>82</td>
</tr>
<tr>
<td>Administrative user accounts</td>
<td>82</td>
</tr>
<tr>
<td>Providing administrative user accounts for one employee</td>
<td>83</td>
</tr>
<tr>
<td>Providing administrative user accounts for multiple employees</td>
<td>84</td>
</tr>
<tr>
<td>Privileged user accounts</td>
<td>85</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Entering master data for LDAP user accounts</td>
<td>86</td>
</tr>
<tr>
<td>General master data of a LDAP user account</td>
<td>87</td>
</tr>
<tr>
<td>Contact data for a LDAP user account</td>
<td>91</td>
</tr>
<tr>
<td>Address information for an LDAP user account</td>
<td>92</td>
</tr>
<tr>
<td>Organizational data for an LDAP user account</td>
<td>92</td>
</tr>
<tr>
<td>Miscellaneous data for an LDAP user account</td>
<td>93</td>
</tr>
<tr>
<td>Additional tasks for managing LDAP user accounts</td>
<td>94</td>
</tr>
<tr>
<td>Overview of the LDAP user account</td>
<td>94</td>
</tr>
<tr>
<td>Changing the manage level of a LDAP user account</td>
<td>94</td>
</tr>
<tr>
<td>Assigning LDAP groups directly to an LDAP user account</td>
<td>95</td>
</tr>
<tr>
<td>Assigning extended properties to a LDAP user account</td>
<td>95</td>
</tr>
<tr>
<td>Automatic assignment of persons to LDAP user accounts</td>
<td>96</td>
</tr>
<tr>
<td>Editing search criteria for automatic employee assignment</td>
<td>98</td>
</tr>
<tr>
<td>Disabling LDAP user accounts</td>
<td>100</td>
</tr>
<tr>
<td>Deleting and restoring LDAP user accounts</td>
<td>102</td>
</tr>
<tr>
<td><strong>LDAP groups</strong></td>
<td>103</td>
</tr>
<tr>
<td>LDAP Group master data</td>
<td>103</td>
</tr>
<tr>
<td>Assigning LDAP groups directly to LDAP user accounts and LDAP computers</td>
<td>105</td>
</tr>
<tr>
<td>Assigning LDAP groups to departments, cost centers, and locations</td>
<td>106</td>
</tr>
<tr>
<td>Assigning LDAP groups to business roles</td>
<td>107</td>
</tr>
<tr>
<td>Assigning LDAP user accounts directly to an LDAP group</td>
<td>108</td>
</tr>
<tr>
<td>Assigning LDAP computers directly to an LDAP group</td>
<td>109</td>
</tr>
<tr>
<td>Adding LDAP groups to system roles</td>
<td>110</td>
</tr>
<tr>
<td>Adding LDAP groups to the IT Shop</td>
<td>111</td>
</tr>
<tr>
<td>Additional tasks for managing LDAP groups</td>
<td>112</td>
</tr>
<tr>
<td>Overview of the LDAP group</td>
<td>112</td>
</tr>
<tr>
<td>Effectiveness of group memberships</td>
<td>113</td>
</tr>
<tr>
<td>LDAP group inheritance based on categories</td>
<td>115</td>
</tr>
<tr>
<td>Assigning extended properties to a LDAP group</td>
<td>117</td>
</tr>
<tr>
<td>Deleting LDAP groups</td>
<td>117</td>
</tr>
<tr>
<td><strong>LDAP container hierarchies</strong></td>
<td>118</td>
</tr>
<tr>
<td>General master data for a LDAP container</td>
<td>118</td>
</tr>
<tr>
<td>Contact data for LDAP containers</td>
<td>120</td>
</tr>
<tr>
<td>Address information for LDAP containers</td>
<td>120</td>
</tr>
</tbody>
</table>
Managing LDAP environments

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

The default One Identity Manager installation is concerned with employee administration and their user accounts, user groups, and LDAP directory organizational units. The One Identity Manager data model is designed to manage administration of LDAP directory computers and servers.

The One Identity Manager supplies templates for synchronizing with several server systems. However, the synchronization connection has to be custom configured in any case.

Company employees are provided with the necessary user accounts in the One Identity Manager. Different mechanisms can be used to link employees to their user accounts. These user accounts can also be managed separately from employees and therefore administrative user accounts can be set up. In order to provide the required permissions, LDAP groups are managed in One Identity Manager. In One Identity Manager you can also manage organizational units in a hierarchical structure. Organizational units (branches or departments) are used to logically organize the objects in an LDAP directory such as user accounts and groups and thus make administration easier.

Architecture overview

The following servers in One Identity Manager play a role in managing an LDAP environment:

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

The synchronization server for synchronizing the One Identity Manager database with the LDAP system. The One Identity Manager Service is installed on this server with the LDAP connector. The synchronization server connects to the LDAP server.

The LDAP connector is used for synchronization and provisioning LDAP. The LDAP connector communicates directly with an LDAP server.

**Figure 1: Architecture for synchronization**

One Identity Manager users for managing an LDAP environment

The following users are used for setting up and managing an LDAP environment.

**Table 1: User**

<table>
<thead>
<tr>
<th>User</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></td>
<td>- Specify which application roles for target system managers are mutually exclusive.</td>
</tr>
<tr>
<td></td>
<td>- Authorize other employee to be target system administrators.</td>
</tr>
<tr>
<td></td>
<td>- Do not assume any administrative tasks within the target system.</td>
</tr>
<tr>
<td>User</td>
<td>Task</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Target system managers</td>
<td>Target system managers must be assigned to **Target systems</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>- Assume administrative tasks for the target system.</td>
</tr>
<tr>
<td></td>
<td>- Create, change or delete target system objects, like user</td>
</tr>
<tr>
<td></td>
<td>accounts or groups.</td>
</tr>
<tr>
<td></td>
<td>- Edit password policies for the target system.</td>
</tr>
<tr>
<td></td>
<td>- Prepare groups for adding to the IT Shop.</td>
</tr>
<tr>
<td></td>
<td>- Can add employees, who have an other identity than the <strong>Primary identity</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Configure synchronization in the Synchronization Editor</td>
</tr>
<tr>
<td></td>
<td>and defines the mapping for comparing target systems and One</td>
</tr>
<tr>
<td></td>
<td>Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>- Edit the synchronization's target system types and outstanding</td>
</tr>
<tr>
<td></td>
<td>objects.</td>
</tr>
<tr>
<td></td>
<td>- Authorize other employees within their area of responsibility as</td>
</tr>
<tr>
<td></td>
<td>target system managers and create child application roles if</td>
</tr>
<tr>
<td></td>
<td>required.</td>
</tr>
<tr>
<td>One Identity Manager</td>
<td>Create customized permissions groups for application</td>
</tr>
<tr>
<td>administrators</td>
<td>roles for role-based login to administration tools in</td>
</tr>
<tr>
<td></td>
<td>Designer as required.</td>
</tr>
<tr>
<td></td>
<td>- Create system users and permissions groups for non-role-based</td>
</tr>
<tr>
<td></td>
<td>login to administration tools in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>- Enable or disable additional configuration parameters in</td>
</tr>
<tr>
<td></td>
<td>Designer as required.</td>
</tr>
<tr>
<td></td>
<td>- Create custom processes in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>- Create and configures schedules as required.</td>
</tr>
<tr>
<td></td>
<td>- Create and configure password policies as required.</td>
</tr>
<tr>
<td>Administrators for the IT</td>
<td>Administrators must be assigned to the **Request &amp; Fulfillment</td>
</tr>
<tr>
<td>Shop</td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>- Assign groups to IT Shop structures.</td>
</tr>
<tr>
<td>Administrators for</td>
<td>Administrators must be assigned to the application role **Identity Management</td>
</tr>
<tr>
<td>organizations</td>
<td>Users with this application role:</td>
</tr>
<tr>
<td>User</td>
<td>Task</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Business roles administrators| Administrators must be assigned to the application role **Identity Management | Business roles | Administrators.** Users with this application role:  
|                             | • Assign groups to business roles.                                    |
Setting up LDAP directory synchronization

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

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

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

1. Prepare a user account with sufficient permissions for synchronization.
2. The One Identity Manager parts for managing LDAP systems are available if "TargetSystem\LDAP" is set.
   - 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 an LDAP directory on page 12
- Setting up the synchronization server on page 14
- Creating a synchronization project for initial synchronization of a LDAP domain on page 17
- Disabling synchronization on page 38
- Customizing synchronization configuration on page 29
Users and permissions for synchronizing with an LDAP directory

The following users are involved in synchronizing One Identity Manager with LDAP.

Table 2: Users for synchronization

<table>
<thead>
<tr>
<th>User</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User for accessing the LDAP directory</td>
<td>A reasonable minimal configuration for the synchronization user account cannot be recommended because the permissions depend which on the LDAP directory service is implemented. For more information about which permissions are required, see your LDAP directory service documentation.</td>
</tr>
</tbody>
</table>
| One Identity Manager Service user account        | 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. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user right. The user account requires access rights to the internal web service.  

**NOTE:** If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access rights for the internal web service with the following command line call: 

`netsh http add urlacl url=http://<IP address>:<port number>/user="NT AUTHORITY\NETWORKSERVICE"`

The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.

In the default installation the One Identity Manager is installed under:

- %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)
- %ProgramFiles%\One Identity (on 64-bit operating systems)

| User for accessing the One Identity Manager database | The **Synchronization** default system user is provided for executing synchronization with an application server. |
Special cases for synchronizing an Active Directory Lightweight Directory Service

There are various special cases to take into account when setting up a synchronization project for Active Directory Lightweight Directory Services (AD LDS).

AD LDS supports different authentication methods. For more detailed information about AD LDS authentication, see the Microsoft TechNet Library.

Different settings arise, which need to be considered when setting up the synchronization project, depending on the authentication method you choose.

Authentication with AD LDS security principal

For this authentication method, you use a user account that is in AD LDS.

- The user account must be a member in the "Administrators" group of the AD LDS instance.
- The user account must have a password.
  If it does not have a password, authentication is anonymous. This causes the schema to load incorrectly and the synchronization project set up fails.

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

- Authentication must use SSL encryption.
- "Basic" must be used as authentication method.
- Enter the distinguished LDAP name (DN) with the user account's user name for logging in to AD LDS.
  Syntax example: CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd

Authentication with Windows security principal

Use a user account for authentication that resides on a local computer or in an Active Directory domain.

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

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

- "Negotiate" must be used as authentication method.
- If SSL encoding is not being used, sealing and signing authentication modes must be enabled.
- If SSL encoding is being used, sealing and signing authentication modes should not be enabled.
- Enter the user principal name with the user account's user name for logging in to AD
LDS.

Syntax example: Administrator@Doku.Testlab.dd

**Authentication with AD LDS proxy object**

Use a user account for authentication which exists in AD LDS and serves as binding for a local user account or a user account in an Active Directory domain. The local user account or the Active Directory user account is referenced in AD LDS as security ID (SID).

- The user account (AD LDS proxy object) must be a member in the "Administrators" group of the AD LDS instance.

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

- Authentication must use SSL encryption.
- "Basic" must be used as authentication method.
- Use the AD LDS proxy object user name for the AD LDS login.
- Enter the distinguished LDAP name (DN) with the user name.
  Syntax example: CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd
- The user account password referenced by the AD LDS proxy object is to be used as a login password.

**Setting up the synchronization server**

To set up synchronization with an LDAP environment, a server has to be available that has the following software installed on it:

- Windows operating system
  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, LDAP connector
  - Install One Identity Manager components with the installation wizard.
    1. Select **Select installation modules with existing database**.
    2. Select the **Server | Job server | LDAP directories** machine role.
All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

**NOTE:** If several target system environments of the same type are synchronized under the same synchronization server, it is 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 3: Job server properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</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>Full server name</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.

5. Select LDAP 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 4: 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. To select a server:</td>
</tr>
<tr>
<td></td>
<td>* Enter a name for the server.</td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Service account      | User account data for the One Identity Manager Service.  
**To enter a user account for the One Identity Manager Service**  
- Set the option Local system account.  
  This starts the One Identity Manager Service under the *NT AUTHORITY\SYSTEM* account.  
- OR -  
- Enter user account, password and password confirmation. |
| Installation account | Data for the administrative user account to install the service.  
**To enter an administrative user account for installation**  
- Enable Advanced.  
- Enable Current user.  
  This uses the user account of the current user.  
- OR -  
- Enter user account, password and password confirmation. |

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 a LDAP domain

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

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.

**Table 5: Information Required for Setting up a Synchronization Project**

<table>
<thead>
<tr>
<th>Data</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server's DNS name</td>
<td>Full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects. Example: Server.Doku.Testlab.dd</td>
</tr>
<tr>
<td>Authentication type</td>
<td>You can only connect to a target system if the correct type of authentication is selected. Authentication type &quot;Basic&quot; is taken as default. For more information about authentication types, see the MSDN Library.</td>
</tr>
<tr>
<td>Communications port on the domain controller</td>
<td>LDAP default communications port is 389.</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 an LDAP directory on page 12.</td>
</tr>
<tr>
<td>Synchronization server for LDAP</td>
<td>All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The One Identity Manager Service with the LDAP connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.</td>
</tr>
</tbody>
</table>

**Table 6: Additional properties for the Job server**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server function</td>
<td>LDAP connector</td>
</tr>
<tr>
<td>Machine role</td>
<td>Server/Job Server/LDAP directories</td>
</tr>
</tbody>
</table>

For more information, see Setting up the synchronization server on page 14.
### Data | Explanation
--- | ---
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
- RemoteConnectPlugin is installed
- LDAP connector is installed

The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

**TIP:** The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well.

For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

**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 LDAP 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 LDAP** 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. Specify settings for the wizard using **Expert mode (Configure advanced settings)** on the wizard’s start page.
   - If you use a default project template, disable this option. The default templates automatically find which settings to use.
   
   For customized LDAP environments, enable the option. You can set the following options for this case:
     - Definition of virtual classes for RFC non-compliant object mappings
     - Definition of auxiliary classes of type "Auxiliary"
     - Definition of system attributes for object identification, revision properties and additional operational attributes
     - Definition of additional attributes for supporting dynamic groups

5. On the **Network** page, enter network settings for the LDAP server connection.
   - In the **Host** area, enter the connection settings for the LDAP server.

   **Table 7: Connection settings for the LDAP server**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Full name of the LDAP server for connecting to the synchronization server to provide access to LDAP objects.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Server.Doku.Testlab.dd</td>
</tr>
<tr>
<td>Port</td>
<td>Communication port on the server. LDAP default communications port is 389.</td>
</tr>
</tbody>
</table>
   
   - Click **Test**. The system tries to connect to the server.
• In the **Additional settings** area, enter the additional settings for communication with the LDAP server.

**Table 8: Additional connection settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol version</td>
<td>Version of the LDAP protocol.</td>
</tr>
<tr>
<td>No encryption</td>
<td>Specifies that no encryption is used</td>
</tr>
<tr>
<td>Use SSL/TLS</td>
<td>Specifies whether a connection encrypted with SSL/TLS is used</td>
</tr>
<tr>
<td>Use StartTLS</td>
<td>Specifies whether StartTLS is used</td>
</tr>
</tbody>
</table>

6. Enter authentication data on the **Authentication** page.

• In the **Authentication method** area, select the authentication type for the login to the target system.

• Depending on the selected authentication method, additional information may be required. Enter this information under **Credentials**.

**Table 9: Credentials**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>User account name for logging in to the LDAP.</td>
</tr>
<tr>
<td>Password</td>
<td>User account password.</td>
</tr>
<tr>
<td>Enable sealing</td>
<td>Specifies whether to enable sealing Set this option if the selected authentication method supports sealing.</td>
</tr>
<tr>
<td>Enable signing</td>
<td>Specifies whether to enable signing Set this option if the selected authentication method supports signing.</td>
</tr>
</tbody>
</table>

• In the **Verify LDAP connection** area, you can check the connection data entered. Click **Test**. An attempt is made to log into the server.

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

8. Defined additional virtual classes on the **Virtual classes** page.

   **NOTE:** This step is only displayed if you have set **Configure advanced settings (Expert mode)** for the system connection wizard.

Objects made up of several structural classes can only be created in non-RFC compliant LDAP systems. They consist of one or more different classes, which are not derived from each other, for example, "OrganizationalUnit" and "inetOrgPerson".
To map these objects

- In the Configured virtual classes area, enter the name of the virtual class.
- In the Select structural classes area, select the structural classes that are mapped on the virtual class.

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base DN</td>
<td>Root entry (generally the domain) for synchronization.</td>
</tr>
<tr>
<td>Save the LDAP schema in the local cache</td>
<td>Specifies whether the LDAP schema should be maintained locally in the cache. This accelerates synchronization and provisioning of LDAP objects. The cache is stored on the computer used to create the connection at %Appdata%...\Local\One Identity\One Identity Manager\Cache\GenericLdapConnector&lt;ConnectionInternalKey&gt;&lt;Hash&gt;\Hash.Cache</td>
</tr>
<tr>
<td>Request timeout (seconds)</td>
<td>Timeout for requests in seconds.</td>
</tr>
<tr>
<td>Use paged search</td>
<td>Specifies whether the LDAP objects are to be loaded in paged form. If you set this option, you include the page size.</td>
</tr>
<tr>
<td>Page size</td>
<td>The maximum number of objects to be loaded per page.</td>
</tr>
</tbody>
</table>

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

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

**INFORMATION:** Some servers only support renaming of entries on leaf nodes. In this case, you will get an error message when trying to rename other nodes.

11. Assign additional auxiliary classes to structural classes on the Assign auxiliary classes page.
NOTE: This step is only displayed if you have set **Configure advanced settings (Expert mode)** for the system connection wizard.

Auxiliary classes are classes of type "Auxiliary" and contain attributes for extending structural classes. Auxiliary class attributes are offered as optional attributes for structural classes in the schema.

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

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

NOTE: This step is only displayed if you have set **Configure advanced settings (Expert mode)** for the system connection wizard.

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

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

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

NOTE: This step is only displayed if you have set **Configure advanced settings (Expert mode)** for the system connection wizard.

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

**Table 11: password settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password attribute</td>
<td>An attribute that represents the password of a user account, for example, userPassword.</td>
</tr>
<tr>
<td>Password change method</td>
<td>A method that is used to change passwords.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Default method for changing the passwords. The password is written directly to the password attribute.</td>
</tr>
<tr>
<td>ADLDS</td>
<td>A password change method used for systems that are based on Microsoft Active Directory Lightweight Directory Services (AD LDS).</td>
</tr>
</tbody>
</table>

15. 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.

16. 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.

17. Select a project template on the **Select project template** page to use for setting up the synchronization configuration.

**Table 12: Standard project templates**

<table>
<thead>
<tr>
<th>Project template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenDJ Synchronization</td>
<td>This project template is based on OpenDJ. Use this project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.</td>
</tr>
<tr>
<td>AD LDS Synchronization</td>
<td>This project template is based on Active Directory Lightweight Directory Services (AD LDS).</td>
</tr>
</tbody>
</table>
NOTE: 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.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 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. |

19. 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.

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

20. Enter the general setting for the synchronization project under General.

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

Table 14: General properties of the synchronization project

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Display name for the synchronization project.</td>
</tr>
<tr>
<td>Script language</td>
<td>Language in which the scripts for this synchronization project are written.</td>
</tr>
<tr>
<td></td>
<td>Scripts are implemented at various points in the synchronization configuration. Specify the script language when you set up an empty project.</td>
</tr>
<tr>
<td></td>
<td>! IMPORTANT: You cannot change the script language once the synchronization project has been saved.</td>
</tr>
<tr>
<td></td>
<td>If you use a project template, the template's script language is used.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

21. 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.
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 LDAP | User accounts | Linked but not configured | <Domain>.
   b. Select Assign account definition to linked accounts.

**Detailed information about this topic**

- One Identity Manager Target System Synchronization Reference Guide

**Related topics**

- Setting up the synchronization server on page 14
- Users and permissions for synchronizing with an LDAP directory on page 12
- Displaying synchronization results on page 28
- Customizing synchronization configuration on page 29
- Speeding up synchronization with revision filtering on page 33
- OpenDJ basic template on page 132
- Default project template for Active Directory lightweight directory services on page 133
- Setting up account definitions on page 40
- Automatic assignment of persons to LDAP user accounts on page 96

**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 \(\rightarrow\) 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 \(\rightarrow\) 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 LDAP domain. You can use this synchronization project to load LDAP objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the LDAP environment.

You must customize the synchronization configuration in order to compare the LDAP 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.

To specify which LDAP 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.

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.

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

**Detailed information about this topic**

- Configuring synchronization in LDAP domains on page 31
- Configuring synchronization of several LDAP domains on page 31
- Updating schemas on page 32
Configuring synchronization in LDAP domains

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the master system during synchronization, you also require a workflow with synchronization in the direction of the Target system.

To create a synchronization configuration for synchronizing LDAP domains

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.
   Creates a workflow with Target system as its synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related topics

- Configuring synchronization of several LDAP domains on page 31

Configuring synchronization of several LDAP domains

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 LDAP 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 LDAP domains on page 31

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.

LDAP supports revision filtering. Revision attributes defined when the synchronization project was set up, are used for the revision count. In the default version, the creation date and the date that LDAP objects were last modified is used. Every synchronization saves the last execution date in the One Identity Manager database. (table DPRRevisionStore, column value). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. The next time synchronization is run, only those objects that have been changed since this date are loaded. This avoids unnecessary updating of objects that have not changed since the last synchronization.

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

Post-processing outstanding objects

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

Outstanding objects

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent 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 LDAP | Target system synchronization: LDAP category.
   All tables assigned to the target system type LDAP 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>![Icon]</td>
<td><strong>Delete</strong></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>
| ![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:  
  1. The table containing the object can be published.  
  2. The target system connector has write access to the target system. |
| ![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 ![Icon] 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 LDAP | Basic configuration data | Target system types.
2. In the result list, select the target system type LDAP.
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 LDAP GroupOfNames).
- 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 LDAP | Basic configuration data | Target system types.
2. Select LDAP 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, LDAPAccountInLDAPGroup, LDAPGroupInLDAPGroup and LDAPMachineInLDAPGroup).
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 more 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.
Disabling synchronization

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

To prevent regular synchronization

1. Open the synchronization project in the Synchronization Editor.
2. Select the start up configuration and deactivate the configured schedule.
   
   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited extent. 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.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of a LDAP domain on page 17
To manage an LDAP environment in One Identity Manager, the following data is relevant.

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

  Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. 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 LDAP on page 128.

- **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 Setting up account definitions 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 LDAP user accounts on page 59.

- **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 LDAP user accounts on page 69.

- Email notifications about credentials
  
  When a new user account is created, the login data are sent to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.
  
  For more information, see Email notifications about login data on page 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 34.

- 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.

### Setting up 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.

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 necessary 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 LDAP | 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 16: 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</td>
</tr>
<tr>
<td></td>
<td>definitions. When this account definition is requested or assigned, the</td>
</tr>
<tr>
<td></td>
<td>required account definition is automatically requested or assigned with it.</td>
</tr>
<tr>
<td></td>
<td>Leave empty for LDAP domains.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 to employees</td>
<td>Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.</td>
</tr>
<tr>
<td>IMPORTANT:</td>
<td>Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</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>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retain account definition if temporarily</td>
<td>Specifies the account definition assignment to temporarily disabled employees.</td>
</tr>
<tr>
<td>disabled</td>
<td>Option set: the account definition assignment remains in effect. The user account stays the same.</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>Specifies the account definition assignment on deferred deletion of employees.</td>
</tr>
<tr>
<td>deletion</td>
<td>Option set: the account definition assignment remains in effect. The user account stays the same.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Option set: the account definition assignment remains in effect. The user account stays the same.</td>
</tr>
<tr>
<td></td>
<td>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 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 **LDAP | 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 **LDAP | 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 45

Master data for a manage level

Enter the following data for a manage level.

Table 17: 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>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>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</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 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.

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

**To create a mapping rule for IT operating data**

1. In Manager, select **LDAP | 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 18: 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 <em>One Identity Manager Target System Base Module Administration Guide</em>.</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>NOTE: 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</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>default value</td>
<td></td>
</tr>
<tr>
<td>Notify when</td>
<td>Specifies whether email notification to a defined mailbox is sent when the default value is used. The <strong>Employee - new user account with default properties created</strong> mail template is used. To change the mail template, adjust the **TargetSystem</td>
</tr>
<tr>
<td>applying the</td>
<td></td>
</tr>
<tr>
<td>standard</td>
<td></td>
</tr>
</tbody>
</table>

4. Save the changes.

**Related topics**

- Determining IT operating data on page 48
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 domain A. In addition, certain employees in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. Specify the 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 19: 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. To specify an application scope</td>
</tr>
<tr>
<td></td>
<td>a. Click → next to the text box.</td>
</tr>
<tr>
<td></td>
<td>b. Under <strong>Table</strong>, select the table that maps the target system for select the <code>TSBAccountDef</code> table for an account definition.</td>
</tr>
<tr>
<td></td>
<td>c. Select the specific target system or account definition under <strong>Effects on</strong>.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>User account property for which the value is set.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In the menu, you can select the columns that use the <code>TSB_ITDataFromOrg</code> script in their template. For detailed information, see the One Identity Manager Target System Base Module Administration Guide.</td>
</tr>
</tbody>
</table>

| Value | Concrete value which is assigned to the user account property. |

4. Save the changes.

**Related topics**

- Creating a mapping rule for IT operating data on page 46

**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 LDAP | Basic configuration data | 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 51
- Assigning account definitions to business roles on page 52
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 53
- Assigning account definitions to a target system on page 56

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In Manager, select LDAP | 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 52
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 53

Assigning account definitions to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles
1. In Manager, select LDAP | 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 51
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 53
Assigning account definitions to all employees

To assign an account definition to all employees

1. In Manager, select LDAP | 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 51
- Assigning account definitions to business roles on page 52
- Assigning account definitions directly to employees on page 53

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In Manager, select LDAP | 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 51
- Assigning account definitions to business roles on page 52
- Assigning account definitions to all employees on page 53

**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 **LDAP | 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.

**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 **LDAP | 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 **LDAP | 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 **LDAP | 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 **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 51
- Assigning account definitions to business roles on page 52
- Assigning account definitions directly to employees on page 53
- Assigning account definitions to system roles on page 54

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 LDAP | Domains.
2. Select Change master data.
3. Select the account definition for user accounts from Account definition (initial).
4. Save the changes.

Detailed information about this topic
- Automatic assignment of persons to LDAP user accounts on page 96
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 LDAP | 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 LDAP | 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 LDAP | 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 LDAP | 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 LDAP | Basic configuration data | Account definitions | Account definitions (non-role-based login).
   - OR -
   b. In Manager, select Entitlements | Account definitions (role-based login).
   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 LDAP | 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 LDAP | 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 LDAP | 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 LDAP user accounts

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

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

Detailed information about this topic

- Predefined password policies on page 59
- Using a password policy on page 60
- Editing password policies on page 63
- Custom scripts for password requirements on page 66
- Deny list for passwords on page 68
- Checking a password on page 69
- Testing generation of a password on page 69

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).

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.

**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.

**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.

**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 LDAP password policy is predefined for LDAP. You can apply this password policy to LDAP user accounts passwords (LDAPAccount.UserPassword) of an LDAP domain or an LDAP container.

If the domains' or containers' password requirements differ, it is recommended that you set up your own password policies for each domain or container.

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

Using a password policy

The LDAP password policy is predefined for LDAP. You can apply this password policy to LDAP user accounts passwords (LDAPAccount.UserPassword) of an LDAP domain or an LDAP container.

If the domains' or containers' password requirements differ, it is recommended that you set up your own password policies for each domain or container.

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

The password policy that is to be used for a user account is determined in the following sequence:
1. Password policy of the account definition of the user account
2. Password policy of the manage level of the user account
3. Password policy for the LDAP container of the user account
4. Password policy for the LDAP domain of the user account
5. 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 LDAP | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Assign objects.
4. Click **Add** in the **Assignments** section and enter the following data.

**Table 20: Assigning a Password Policy**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply to</td>
<td>Application scope of the password policy.</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**.

<table>
<thead>
<tr>
<th>Password column</th>
<th>The password column's identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password policy</td>
<td>The identifier of the password policy to be used.</td>
</tr>
</tbody>
</table>

5. Save the changes.

*To change a password policy's assignment*

1. In the Manager, select the **LDAP | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select **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 LDAP | Basic configuration data | Password policies category.
2. Select the password policy in the result list and select Change master data.
   - OR -
   Click 📝 in the result list.
3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

- General master data for a password policy on page 63
- Policy settings on page 64
- Character classes for passwords on page 65
- Custom scripts for password requirements on page 66

General master data for a password policy

Enter the following master data for a password policy.

Table 21: 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 22: 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 <em>One Identity Manager Web Portal User Guide</em>.</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>
<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>
<tr>
<td>Digits not allowed</td>
<td>Specifies whether the password can contain digits. This setting is</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Special characters not allowed</td>
<td>Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td></td>
<td>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 66
- [Script for generating a password](#) on page 67

**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**

```vbnet
Public Sub CCC_CustomPwdValidate( 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.

```vbnet
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 LDAP**

Basic configuration data 66
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 LDAP | 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 67

Script for generating a password

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

Syntax for generating script

Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
  With parameters:
  policy = password policy object
  spwd = generated password
  TIP: To use a base object, take the 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.

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 LDAP | 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 66

Deny 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 **LDAP | 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 **LDAP | 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 LDAP user accounts**

You have the following possible options for issuing an initial password for a new LDAP 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** | **LDAP** | **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 LDAP user accounts on page 59
- Email notifications about login data on page 70

### 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 | LDAP | Accounts | InitialRandomPassword.
2. In the Designer, activate the configuration parameter TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo and enter the recipient of the notification as a value.
3. In the Designer, activate the configuration parameter TargetSystem | LDAP | 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 | LDAP | 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.

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 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.
Target system managers must be assigned to **Target systems | LDAP** 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.

**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 | LDAP**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

---

**Table 24: Default Application Roles for Target System Managers**

<table>
<thead>
<tr>
<th>User</th>
<th>Tasks</th>
</tr>
</thead>
</table>
| Target system managers     | Target system managers must be assigned to **Target systems | LDAP** 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.
**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 LDAP | 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 LDAP | 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 | LDAP parent application role.
   b. Click OK to add the new application role.
6. Save the changes.
7. Assign employees to this application role who are permitted to edit the domain in One Identity Manager.

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

**Related topics**

- One Identity Manager users for managing an LDAP environment on page 8
- General master data for a LDAP domain on page 74
- LDAP container hierarchies on page 118
LDAP domains

**INFORMATION:** The Synchronization Editor sets up the domains in the One Identity Manager database if a default project template is used.

**To edit master data for an LDAP domain**

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

**Detailed information about this topic**

- General master data for a LDAP domain on page 74
- LDAP specific master data for an LDAP domain on page 76
- Specifying categories for inheriting LDAP groups on page 77

**General master data for a LDAP domain**

Enter the following data on **General**:

**Table 25: Domain master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>NetBIOS domain name.</td>
</tr>
<tr>
<td>Full domain name</td>
<td>Name of the domain confirming to DNS syntax.</td>
</tr>
<tr>
<td></td>
<td>Name of this domain.name of parent domain.name of default domain</td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>Docu.Testlab.dd</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDAP system type</td>
<td>Type of the LDAP system.</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>Object class</td>
<td>List of classes defining the attributes for this object. The default object class is <strong>DOMAIN</strong>. 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>Distinguished name</td>
<td>Distinguished name of the domain. The distinguished name is determined using a template from the full domain name and cannot be edited.</td>
</tr>
<tr>
<td>Canonical name</td>
<td>Canonical name of the domain.</td>
</tr>
<tr>
<td>Account definition (initial)</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 (<strong>Linked configured</strong>). The account definition's default manage level is applied. User accounts are only linked to the employee (<strong>Linked</strong>) 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. Select the One Identity Manager application role whose members are responsible for administration of this domain. Use the <strong>button</strong> 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. <strong>One Identity Manager</strong> is used when you create a domain with the Synchronization Editor.</td>
</tr>
</tbody>
</table>

**Table 26: Permitted values**

<table>
<thead>
<tr>
<th></th>
<th>Synchronization by</th>
<th>Provisioned by</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Identity Manager</td>
<td>LDAP connector</td>
<td>LDAP connector</td>
</tr>
<tr>
<td>No synchronization</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>
**Property** | **Description**
---|---
| **NOTE:** If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system. |

**Description** | Spare text box for additional explanation.
**Structural object class** | Structural object class representing the object type.

**Related topics**
- Automatic assignment of persons to LDAP user accounts on page 96
- Target system managers on page 71

**LDAP specific master data for an LDAP domain**

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

**Table 27: LDAP data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full domain name</strong></td>
<td>Name of the domain confirming to DNS syntax. Name of this domain.name of parent domain.name of default domain Example Docu.Testlab.dd</td>
</tr>
<tr>
<td><strong>Distinguished name</strong></td>
<td>Distinguished name of the domain. The distinguished name is determined using a template from the full domain name and cannot be edited.</td>
</tr>
<tr>
<td><strong>Structural object class</strong></td>
<td>Structural object class representing the object type.</td>
</tr>
<tr>
<td><strong>Object class</strong></td>
<td>List of classes defining the attributes for this object. The default object class is &quot;DOMAIN&quot;. 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><strong>Search mask</strong></td>
<td>Search mask for another LDAP object.</td>
</tr>
</tbody>
</table>
Specifying categories for inheriting LDAP groups

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

To define a category

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

Detailed information about this topic

- LDAP group inheritance based on categories on page 115

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 LDAP | 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 29
LDAP user accounts

You manage user accounts in One Identity Manager with LDAP. A user can log in to a domain with a user account and receive group memberships and access rights to network resources.

Detailed information about this topic

- Linking user accounts to employees on page 79
- Supported user account types on page 80
- Entering master data for LDAP user accounts on page 86

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 employee 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 LDAP domain, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.
When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.

- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. 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 LDAP user accounts on page 86
- Setting up account definitions on page 40
- Automatic assignment of persons to LDAP user accounts on page 96
- For more detailed information about employee handling and administration, see the One Identity Manager Target System Base Module Administration Guide.

**Supported user account types**

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

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

<table>
<thead>
<tr>
<th>Identity</th>
<th>Description</th>
<th>Value of the IdentityType column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary identity</td>
<td>Employee’s default user account.</td>
<td>Primary</td>
</tr>
<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>Identity</td>
<td>Description</td>
<td>Value of the IdentityType column</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------</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 82
- Administrative user accounts on page 82
- Providing administrative user accounts for one employee on page 83
- Providing administrative user accounts for multiple employees on page 84
- Privileged user accounts on page 85
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

- Setting up account definitions 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 administrative user accounts for one employee on page 83
- Providing administrative user accounts for multiple employees on page 84

## Providing administrative user accounts for one employee

**Prerequisites**

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

**To prepare an administrative user account for a person**

1. Label the user account as a personalized admin identity.
   
   a. In Manager, select **LDAP | 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 **Personalized administrator identity**.

2. Link the user account to the employee who will be using this administrative user account.
   
   a. In Manager, select **LDAP | 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 ↗ to create a new person.
Related topics

- Providing administrative user accounts for multiple employees on page 84
- For detailed information about mapping employee identities, see the One Identity Manager Identity Management Base Module Administration Guide.

Providing administrative user accounts 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 LDAP | User accounts.
   b. Select the user account in the result list.
   c. Select Change master data.

2. Link the user account to a dummy employee.
   a. In Manager, select LDAP | 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 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 LDAP | 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 administrative user accounts for one employee** on page 83
- 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 | LDAP | Accounts | PrivilegedAccount | UserID_Prefix** configuration parameter in Designer.

- To use a postfix for the login name, enable the **TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_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**

- Setting up account definitions on page 40

### Entering master data for LDAP user accounts

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

**NOTE:** It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.
NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location or a primary cost center.

To create a user account
1. In Manager, select LDAP | 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 LDAP | 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 LDAP user accounts from the task view.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic
- General master data of a LDAP user account on page 87
- Contact data for a LDAP user account on page 91
- Address information for an LDAP user account on page 92
- Organizational data for an LDAP user account on page 92
- Miscellaneous data for an LDAP user account on page 93

Related topics
- Supported user account types on page 80
- Setting up account definitions on page 40

General master data of a LDAP user account

Enter the following data on General:
Table 29: 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 of 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. NOTE: The account definition cannot be changed once the user account has been saved.</td>
</tr>
<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>Domain</td>
<td>Domain in which the user account is created.</td>
</tr>
<tr>
<td>Structural object class</td>
<td>Structural object class representing the object type. By default, user accounts in One Identity Manager are added with the object class &quot;INETORGPERSON&quot;.</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>Object class</td>
<td>List of classes defining the attributes for this object. By default, the user accounts in One Identity Manager are created with the &quot;INETORGPERSON&quot; object class. 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>Name</td>
<td>User account identifier. The identifier is made up of the user’s first and last names.</td>
</tr>
</tbody>
</table>
| Display                   | User account display name. The display name is made up of the first and
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>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>Object SID (AD)</td>
<td>The object’s security ID (SID) in Active Directory.</td>
</tr>
<tr>
<td>First name</td>
<td>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>Last name of user account. 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>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>Job description</td>
<td>Job description. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Login name</td>
<td>Login name. If you assigned an account definition, the login name is made up of the employee’s central user account depending on the manage level.</td>
</tr>
</tbody>
</table>
| Password            | Password for the user account. The employee’s central password can be mapped to the user account password. For detailed information about an employee’s central password, see One Identity Manager Identity Management Base Module Administration Guide. If you use an initial password for the user accounts, it is automatically entered when a user account is created.  

NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements. |
| Password confirmation| Reconfirm password.                                                                                                                                                                                                                                                                                                                                |
| Risk index (calculated) | Maximum risk index value of all assigned groups. The property is only visible if the QER | CalculateRiskIndex configuration parameter is enabled. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.                                                                                                      |
| Account expiry date | Account expiry date. Specifying an expiry data for the account has the effect that the logon for this user account is blocked as soon as the given date is exceeded. If you assigned an account definition, the employee’s last day of work it is automatically taken as the expiry date depending on the manage level. Any existing account expiry date is overwritten in this case. |

One Identity Manager 8.1.1 Administration Guide for Connecting to LDAP
LDAP user accounts
89
### Property | Description
--- | ---
Category | Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Description | Spare text box for additional explanation.
Identity | User account’s identity type Permitted values are:
  - **Primary identity**: Employee’s default user account.
  - **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.
  - **Personalized administrator identity**: User account with administrative entitlements, used by one employee.
  - **Sponsored identity**: User account that is used for training purposes, for example.
  - **Shared identity**: User account with administrative entitlements, used by several employees. Assign all employees show use the user account.
  - **Service identity**: Service account.
Privileged user account | Specifies whether this is a privileged user account.
Groups can be inherited | Specifies whether the user account can inherit groups via the employee. If this option is set, the user account inherits groups via hierarchical roles or IT Shop requests.
  - If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.
  - If an employee has requested group membership in the IT Shop and the request is granted approval, the employee’s user account only inherits the group if the option is set.
User account is disabled | Specifies whether the user account is disable. If a user account is not required for a period of time, you can temporarily disable the user account by using the option <User account is deactivated>.

### Related topics
- Setting up account definitions on page 40
- Password policies for LDAP user accounts on page 59
- Initial password for new LDAP user accounts on page 69
Contact data for a LDAP user account

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

Table 30: Contact Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picture</td>
<td>Picture to display in a telephone book, for example.</td>
</tr>
<tr>
<td></td>
<td>• Load the image using the button.</td>
</tr>
<tr>
<td></td>
<td>• You can delete the picture using .</td>
</tr>
<tr>
<td>Email address</td>
<td>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>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>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>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>Phone private</td>
<td>Private telephone number.</td>
</tr>
<tr>
<td>Phone, private (2)</td>
<td>Extra telephone number.</td>
</tr>
<tr>
<td>Internationale ISDN no.</td>
<td>Internationale ISDN number.</td>
</tr>
<tr>
<td>Additional email addresses</td>
<td>Additional email addresses.</td>
</tr>
<tr>
<td>X.121 address</td>
<td>Addressing as X.121 address.</td>
</tr>
<tr>
<td>X.400 address</td>
<td>Address in X.400 format.</td>
</tr>
</tbody>
</table>
Address information for an LDAP user account

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

Table 31: Address data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room</td>
<td>Room. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Registered address</td>
<td>Postal address.</td>
</tr>
<tr>
<td>Address</td>
<td>Postal address.</td>
</tr>
<tr>
<td>Address (private)</td>
<td>Postal address (private).</td>
</tr>
<tr>
<td>Mailbox</td>
<td>PO box. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Street</td>
<td>Street. If you have assigned an account definition, the input field is 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 automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>State</td>
<td>State, county or province. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
</tbody>
</table>

Organizational data for an LDAP user account

Enter the following organizational master data on the Organizational tab.

Table 32: Organizational Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business unit</td>
<td>Business unit to which the employee is assigned.</td>
</tr>
<tr>
<td>Department</td>
<td>Employee's department. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Location</td>
<td>Employee's location. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location ID</td>
<td>Location identifier (country and city) for telegram services.</td>
</tr>
<tr>
<td>Employment</td>
<td>Job details.</td>
</tr>
<tr>
<td>Employee number</td>
<td>Number for identifying the employee in addition to their ID.</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>Organizational position</td>
<td>Details of position in the company, for example, directory or department manager.</td>
</tr>
<tr>
<td>Office</td>
<td>Office. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Preferred language</td>
<td>Preferred language. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Account manager</td>
<td>Manager responsible for the user account.</td>
</tr>
<tr>
<td>Secretary</td>
<td>Secretary’s user account.</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 field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Car license plate</td>
<td>Vehicle's license plate.</td>
</tr>
</tbody>
</table>

### Miscellaneous data for an LDAP user account

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

**Table 33: Miscellaneous Master Data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>See also</td>
<td>Link to another LDAP object.</td>
</tr>
<tr>
<td>Default PC</td>
<td>User’s workstation.</td>
</tr>
<tr>
<td>User ID</td>
<td>User's Identification number.</td>
</tr>
</tbody>
</table>
Additional tasks for managing LDAP user accounts

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

Overview of the LDAP user account

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

To obtain an overview of a user account

1. Select the LDAP | User accounts category.
2. Select the user account in the result list.
3. Select LDAP user account overview.

Changing the manage level of a LDAP 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 LDAP | 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 LDAP user accounts on page 86
Assigning LDAP groups directly to an LDAP 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 LDAP, the groups in the role are inherited by this user account.

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

**NOTE:** User accounts cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

**To assign groups directly to user accounts**

1. In Manager, select **LDAP | 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 the group and double click ✅.

5. Save the changes.

**Related topics**

- Assigning LDAP groups directly to LDAP user accounts and LDAP computers on page 105

Assigning extended properties to a LDAP 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 **LDAP | 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 persons to LDAP user accounts

### Table 34: Configuration parameters for automatic employee assignment

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\LDAP\PersonAutoFullsync</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\PersonAutoDefault</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\PersonAutoDisabledAccounts</td>
<td>This configuration parameter specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.</td>
</tr>
</tbody>
</table>

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 employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\LDAP\PersonAutoFullsync" in the Designer and select the required mode.
- If employees can be assigned by user accounts outside synchronization, set the parameter "TargetSystem\LDAP\PersonAutoDefault" in the Designer and select the required mode.
- Use the configuration parameter "TargetSystem\LDAP\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** 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 **LDAP \ User accounts \ Linked but not configured \ <Domain>**.
   b. Select **Assign account definition to linked accounts**.
For more detailed information about assigning employees automatically, see the One Identity Manager Target System Base Module Administration Guide.

**Related topics**

- Creating an account definition on page 41
- Assigning account definitions to a target system on page 56
- Editing search criteria for automatic employee assignment on page 98

**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 LDAPDomain table.

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

**NOTE:** When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

It is not recommended to make 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 **LDAP | 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 35: Standard search criteria for user accounts**

<table>
<thead>
<tr>
<th>Apply to</th>
<th>Column for employee</th>
<th>Column for user account</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP User accounts</td>
<td>Central user account (CentralAccount)</td>
<td>Login name (UserID)</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 36: 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 user accounts</td>
<td>This view lists all user accounts to which an employee is assigned.</td>
</tr>
<tr>
<td>Without employee assignment</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 more detailed information about defining search criteria, see the One Identity Manager Target System Base Module Administration Guide.

**Related topics**

* Automatic assignment of persons to LDAP user accounts on page 96

**Disabling LDAP user accounts**

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

**Scenario:**

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

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the 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 LDAPAccount.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 LDAP | 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 LDAP | 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.

Related topics

- Setting up account definitions on page 40
- Setting up manage levels on page 43
- Deleting and restoring LDAP user accounts on page 102
- For more detailed information about deactivating and deleting employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.
Deleting and restoring LDAP user accounts

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

To delete a user account
1. Select the LDAP | User accounts category.
2. Select the user account in the result list.
3. Delete the user account.
4. Confirm the security prompt with Yes.

To restore a user account
1. Select the LDAP | User accounts category.
2. Select the user account in the result list.
3. Click Undo delete in the result list toolbar.

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

Related topics
- Disabling LDAP user accounts on page 100
LDAP groups

You can collect user accounts, contacts, computers, and groups into groups that can be used to regulate access to resources in the LDAP directory. In One Identity Manager, you can set up new groups or to edit already existing groups.

To add users to groups, you assign the groups directly to users. This can be assignments of groups to departments, cost centers, location, business roles, or to the IT Shop.

To edit group master data

1. In the Manager, select the LDAP | Groups category.
2. Select the group in the result list and run 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

- LDAP Group master data on page 103
- Assigning LDAP groups directly to LDAP user accounts and LDAP computers on page 105

LDAP Group master data

Enter the following master data:

Table 37: General Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>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>Administrator</td>
<td>The group administrator.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item data for requesting the group through the IT Shop.</td>
</tr>
<tr>
<td>Business unit</td>
<td>Business unit to which the group is assigned.</td>
</tr>
<tr>
<td>See also</td>
<td>Link to another LDAP object.</td>
</tr>
<tr>
<td>Structural object class</td>
<td>Structural object class representing the object type. By default, containers in One Identity Manager are added with &quot;GROUPOFNAMES&quot;.</td>
</tr>
<tr>
<td>Object class</td>
<td>List of classes defining the attributes for this object. By default, the groups in the One Identity Manager are created with the &quot;GROUPOFNAMES&quot; object class. 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>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. To do this, groups and user accounts 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>Condition</td>
<td>LDAP filter for finding memberships in a dynamic groups.</td>
</tr>
<tr>
<td>Dynamic group</td>
<td>Specifies whether this is a dynamic group.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>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.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>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.</td>
</tr>
</tbody>
</table>
Related topics

- LDAP group inheritance based on categories on page 115
- For more detailed information about preparing groups for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning LDAP groups directly to LDAP user accounts and LDAP computers

You can assign 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, the user account is added to the group. Prerequisites for indirect assignment to the user accounts of employees:

- Assignment of employees and groups is permitted for role classes (department, cost center, location or business role).
- User accounts are marked 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.
- "TargetSystem\LDAP\HardwareInGroupFromOrg" 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.

Furthermore, groups can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that groups can be assigned through IT Shop requests. All groups are assigned to this shop can be requested by the customers. Requested groups are assigned to the employees after approval is granted.
Assigning LDAP groups to departments, cost centers, and locations

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

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

1. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select **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 LDAP 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 LDAP groups to business roles on page 107
- Assigning LDAP user accounts directly to an LDAP group on page 108
- Assigning LDAP computers directly to an LDAP group on page 109
- Adding LDAP groups to system roles on page 110
- Adding LDAP groups to the IT Shop on page 111
- One Identity Manager users for managing an LDAP environment on page 8

**Assigning LDAP groups to business roles**

**Installed modules:** Business Roles Module

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

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

1. In the Manager, select the **LDAP | Groups** category.
2. Select the group in the result list.
3. Select **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 LDAP 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 LDAP groups to departments, cost centers, and locations on page 106
- Assigning LDAP user accounts directly to an LDAP group on page 108
- Assigning LDAP computers directly to an LDAP group on page 109
- Adding LDAP groups to system roles on page 110
- Adding LDAP groups to the IT Shop on page 111
- One Identity Manager users for managing an LDAP environment on page 8

Assigning LDAP user accounts directly to an LDAP 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 LDAP, the groups in the role are inherited by this user account.

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

**Note:** User accounts cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

To assign a group directly to user accounts

1. In the Manager, select the LDAP | Groups category.
2. Select the group in the result list.
3. Select 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.

**Related topics**
- Assigning LDAP groups directly to an LDAP user account on page 95
- Assigning LDAP groups to departments, cost centers, and locations on page 106
- Assigning LDAP groups to business roles on page 107
- Assigning LDAP computers directly to an LDAP group on page 109
- Adding LDAP groups to system roles on page 110
- Adding LDAP groups to the IT Shop on page 111

### Assigning LDAP computers directly to an LDAP 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.

**NOTE:** Computers cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

**To assign a group directly to computers**

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **Assign computers** in the task view.
4. Assign the computers in the **Add assignments** area.
   - OR -
   Remove the computers in the **Remove assignments** area.
5. Save the changes.
Related topics

- Assigning LDAP computers directly to LDAP groups on page 123
- Assigning LDAP groups to departments, cost centers, and locations on page 106
- Assigning LDAP groups to business roles on page 107
- Assigning LDAP user accounts directly to an LDAP group on page 108
- Adding LDAP groups to system roles on page 110
- Adding LDAP groups to the IT Shop on page 111

Adding LDAP groups to system roles

Installed modules: System Roles Module

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

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

**To assign a group to system roles**

1. In the Manager, select the LDAP | Groups category.
2. Select the group in the result list.
3. Select 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 LDAP groups to departments, cost centers, and locations on page 106
- Assigning LDAP groups to business roles on page 107
- Assigning LDAP user accounts directly to an LDAP group on page 108
- Assigning LDAP computers directly to an LDAP group on page 109
- Adding LDAP groups to the IT Shop on page 111
Adding LDAP 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 **LDAP | Groups** category (non-role-based login).
   - OR -
     In Manager, select **Entitlements | LDAP 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 **LDAP | Groups** category (non-role-based login).
   - OR -
     In Manager, select **Entitlements | LDAP 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 **LDAP | Groups** category (non-role-based login).
   - OR -
In Manager, select **Entitlements | LDAP 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**

- LDAP Group master data on page 103
- Assigning LDAP groups to departments, cost centers, and locations on page 106
- Assigning LDAP groups to business roles on page 107
- Assigning LDAP user accounts directly to an LDAP group on page 108
- Assigning LDAP computers directly to an LDAP group on page 109
- Adding LDAP groups to system roles on page 110

**Additional tasks for managing LDAP groups**

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

**Overview of the LDAP group**

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

**To obtain an overview of a group**

1. Select the category **LDAP | Groups**.
2. Select the group in the result list.
3. Select **LDAP group overview**.
Effectiveness of group memberships

Table 38: Configuration Parameter for Conditional Inheritance

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</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.</td>
</tr>
<tr>
<td>Structures</td>
<td></td>
</tr>
<tr>
<td>Inherite</td>
<td></td>
</tr>
<tr>
<td>GroupExclusion</td>
<td>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 LDAPAccountInLDAPGroup and BaseTreeHasLDAPGroup 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 39: Specifying excluded groups (table LDAPGroupExclusionAADGroupExclusion)

<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 40: 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 41: 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 | Inherite | GroupExclusion is enabled.
- Mutually exclusive groups belong to the same domain

To exclude a group

1. In the Manager, select the LDAP | Groups category.
2. Select a group in the result list.
3. Select 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.

LDAP group inheritance based on categories

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

Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the user account is not put into categories.

NOTE: Inheritance through categories is only taken into account when groups are assigned indirectly through hierarchical roles. Categories are not taken into account when groups are directly assigned to user accounts.

Table 42: 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 entitlements</td>
</tr>
<tr>
<td>2</td>
<td>System users</td>
<td>System user entitlements</td>
</tr>
<tr>
<td>3</td>
<td>System administrator</td>
<td>System administrator entitlements</td>
</tr>
</tbody>
</table>
**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.
Assigning extended properties to a LDAP 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 LDAP | 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

1. Select the extended property and double click 

5. Save the changes.

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

Deleting LDAP groups

To delete a group

1. Select the category LDAP | 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 LDAP.
LDAP container hierarchies

LDAP containers are represented by a hierarchical tree structure. Containers are often used to display organizational units such as branch offices or departments, to organize LDAP directory objects such as users, groups, and computers logically, and therefore to ease the burden of object administration. LDAP directory containers are loaded by synchronization with the One Identity Manager database.

To edit container master data

1. Select LDAP | 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

- General master data for a LDAP container on page 118
- Contact data for LDAP containers on page 120
- Address information for LDAP containers on page 120

General master data for a LDAP container

Enter the following data on General:
Table 43: Master Data for a Container

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Container’s display name.</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>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 from the container name, the object class, the parent container, and the domain and cannot be modified.</td>
</tr>
<tr>
<td>Business unit</td>
<td>Business unit to which the container is assigned.</td>
</tr>
<tr>
<td>Link (named URI format)</td>
<td>Specifies links in Uniform Resource Identifier (URI) Format; made up of a name and a URL.</td>
</tr>
<tr>
<td>Search mask</td>
<td>Search mask for another LDAP object.</td>
</tr>
<tr>
<td>See also</td>
<td>Link to another LDAP object.</td>
</tr>
<tr>
<td>State</td>
<td>State.</td>
</tr>
<tr>
<td>Structural object class</td>
<td>Structural object class representing the object type. By default, containers in One Identity Manager are added with “ORGANIZATIONALUNIT”.</td>
</tr>
<tr>
<td>Object class</td>
<td>List of classes defining the attributes for this object. By default, the containers in One Identity Manager are created in the “ORGANIZATIONALUNIT” object class. 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>Description</td>
<td>Spare text box for additional explanation.</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>
</tbody>
</table>

Related topics

- Target system managers on page 71
Contact data for LDAP containers

Enter data for making contact on the Contact data tab.

Table 44: Contact Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax</td>
<td>Fax number.</td>
</tr>
<tr>
<td>Internationale ISDN no.</td>
<td>Internationale ISDN number.</td>
</tr>
<tr>
<td>Phone</td>
<td>Telephone number.</td>
</tr>
<tr>
<td>Teletex ID</td>
<td>Teletex terminal identification.</td>
</tr>
<tr>
<td>Telex</td>
<td>Telex number.</td>
</tr>
<tr>
<td>Password</td>
<td>Password.</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
</tbody>
</table>

Address information for LDAP containers

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

Table 45: Address data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building name</td>
<td>Name of the building.</td>
</tr>
<tr>
<td>Location ID</td>
<td>Location identifier (country and city) for telegram services.</td>
</tr>
<tr>
<td>Office</td>
<td>Office.</td>
</tr>
<tr>
<td>Address</td>
<td>Postal address.</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>Mailbox</td>
<td>PO box. 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>Preferred delivery</td>
<td>Preferred method of delivery.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registered address</td>
<td>Postal address.</td>
</tr>
<tr>
<td>Street</td>
<td>Street. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>X.121 address</td>
<td>Addressing as X.121 address.</td>
</tr>
</tbody>
</table>
LDAP computers

The One Identity Manager data model is designed to manage administration of LDAP directory computers and servers. To synchronize this data with LDAP, customize the synchronization project accordingly.

To edit computer master data
1. Select the LDAP | Computers category.
2. Select the computer in the result list and run the Change master data task.
   - OR -
   Click in the result list.
3. Edit the computer's master data.
4. Save the changes.

Detailed information about this topic
- Master data for an LDAP computer on page 122

Related topics
- One Identity Manager Target System Synchronization Reference Guide

Master data for an LDAP computer

Enter the following data for a computer.

Table 46: Computer master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>The computer is connected to this device. Specify a new device using the button next to the menu.</td>
</tr>
</tbody>
</table>
## Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</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>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. 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>
</tbody>
</table>

### Related topics

- One Identity Manager Identity Management Base Module Administration Guide

## Assigning LDAP computers directly to LDAP groups

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

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

**NOTE:** Computers cannot be manually added to dynamic groups. Memberships in a dynamic group are determined through the condition of the dynamic group.

### To assign a computer directly to groups

1. Select the **LDAP | Computers** category.
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.
Related topics

- Assigning LDAP groups directly to LDAP user accounts and LDAP computers on page 105
LDAP 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 LDAP.

<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>
</tbody>
</table>

NOTE: Other sections may be available depending on the modules that are installed.
**Report** | **Description**
--- | ---
LDAP user account and group administration | This report contains a summary of user account and group distribution in all domains. You can find this report in My One Identity Manager.
Data quality summary for LDAP user accounts | This report contains different evaluations of user account data quality in all domains. You can find this report in My One Identity Manager.

**Related topics**
- [Overview of all assignments](#) on page 126

**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 **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 \(\text{\textcopyright}\) icon in the report’s toolbar.

- Double-click a control to show all child roles belonging to the selected role.
- By clicking the \(\text{\textbullet}\) button in a role’s control, you display all employees in the role with the base object.
- Use the small arrow next to \(\text{\textbullet}\) 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 48: Meaning of Icons in the Report Toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{\textcopyright})</td>
<td>Show the legend with the meaning of the report control elements</td>
</tr>
<tr>
<td>(\text{\textbullet})</td>
<td>Saves the current report view as a graphic.</td>
</tr>
<tr>
<td>(\text{\textbullet})</td>
<td>Selects the role class used to generate the report.</td>
</tr>
<tr>
<td>(\text{\textbullet})</td>
<td>Displays all roles or only the affected roles.</td>
</tr>
</tbody>
</table>
Appendix: Configuration parameters for managing LDAP

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

Table 49: Configuration parameter for LDAP directory synchronization

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\LDAP</td>
<td>Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system LDAP. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts</td>
<td>This configuration parameter permits configuration of user account data.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\InitialRandomPassword</td>
<td>This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo</td>
<td>This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee’s manager or XUserInserted). If no recipient can be found, the password is sent to the</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName</td>
<td>This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The <strong>Employee - new user account created</strong> mail template is used.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword</td>
<td>This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The <strong>Employee - initial password for new user account</strong> mail template is used.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\MailTemplateDefaultValues</td>
<td>This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The <strong>Employee - new user account with default properties created</strong> mail template is used.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\PrivilegedAccount</td>
<td>This configuration parameter allows configuration of settings for privileged LDAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\PrivilegedAccount\UserID_Postfix</td>
<td>This configuration parameter contains the postfix for formatting login names for privileged user accounts.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Accounts\PrivilegedAccount\UserID_Prefix</td>
<td>This configuration parameter contains the prefix for formatting login names for privileged user accounts.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Authentication</td>
<td>The configuration parameter allows configuration of the LDAP authentication module. For detailed information about the One Identity Manager authentication modules, see the <em>One Identity Manager Authorization and Authentication Guide</em>.</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Authentication\Authentication</td>
<td>The configuration parameter specified the authentication mechanism. Permitted values are &quot;Secure&quot;, &quot;Encryption&quot;, &quot;SecureSocketsLayer&quot;, &quot;ReadOnlyServer&quot;, &quot;Anonymous&quot;, &quot;FastBind&quot;, &quot;Signing&quot;, &quot;Sealing&quot;, &quot;Delegation&quot;, and &quot;ServerBind&quot;. The value can be combined with commas (,). For more information about authentication types, see the MSDN Library. Default is ServerBind.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Authentication\Port</td>
<td>LDAP server's port. Default is port 389.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Authentication\RootDN</td>
<td>The configuration parameter contains the root domain's distinguished name. Syntax: dc=MyDomain</td>
</tr>
<tr>
<td>TargetSystem\LDAP\Authentication\Server</td>
<td>The configuration parameter contains the name of the LDAP server.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\DefaultAddress</td>
<td>The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\HardwareInGroupFromOrg</td>
<td>The configuration parameter specifies whether computers are added to groups on the basis of group assignment to roles.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\MaxFullsyncDuration</td>
<td>This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\PersonAutoDefault</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user.</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TargetSystem\LDAP\PersonAutoDisabledAccounts</td>
<td>accounts added to the database outside synchronization.</td>
</tr>
<tr>
<td>TargetSystem\LDAP\PersonAutoFullSync</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.</td>
</tr>
</tbody>
</table>
Appendix: Default project template for LDAP

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

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

Detailed information about this topic

- OpenDJ basic template on page 132
- Default project template for Active Directory lightweight directory services on page 133

OpenDJ basic template

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

Table 50: Mapping schema types to tables in the One Identity Manager schema.

<table>
<thead>
<tr>
<th>Schema type in LDAP</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>LDPDomain</td>
</tr>
<tr>
<td>organization</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>locality</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>Schema type in LDAP</td>
<td>Table in the One Identity Manager Schema</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Container</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>groupOfNames</td>
<td>LDAPGroup</td>
</tr>
<tr>
<td>groupOfUniqueNames</td>
<td>LDAPGroup</td>
</tr>
<tr>
<td>groupOfURLs</td>
<td>LDAPGroup</td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td>LDAPAccount</td>
</tr>
</tbody>
</table>

**Default project template for Active Directory lightweight directory services**

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

**Table 51: Mapping schema types to tables in the One Identity Manager schema.**

<table>
<thead>
<tr>
<th>Schema type in AD LDS</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>country</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>domainDNS</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>foreignSecurityPrincipal</td>
<td>LDAPAccount</td>
</tr>
<tr>
<td>group</td>
<td>LDAPGroup</td>
</tr>
<tr>
<td>groupOfNames</td>
<td>LDAPGroup</td>
</tr>
<tr>
<td>inetOrgPerson</td>
<td>LDAPAccount</td>
</tr>
<tr>
<td>organization</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>LDAPContainer</td>
</tr>
<tr>
<td>user</td>
<td>LDAPAccount</td>
</tr>
<tr>
<td>userProxy</td>
<td>LDAPAccount</td>
</tr>
<tr>
<td>userProxyFull</td>
<td>LDAPAccount</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 53
  assign domain to LDAP 56
  assign to all persons 53
  assign to business role 52
  assign to department 51
  assign to employee 50, 53
  assign to location 51
  create 41
  delete 57
  IT operating data 46, 48
  manage level 43
account definitions
  assign to system roles 54
Active Directory domain
  reports 125
architecture overview 7
assign account definition to cost
  center 51

C
configuration parameter 128

D
default user account 82
direction of synchronization
  to the 17
  to the target system 17

E
e-mail notification 70
employee assignment
  automatic 96
  manual 99
  removing 99
search criterion 98
  table column 98
exclusion definition 113

G
group
  effective 113
  exclude 113

I
identity 80
IT operating data
  change 49
IT Shop shelf
  assign account definition 54

J
Job server
  process 14
LDAP computer
  computer name 122
  container 122
  device 122
  domain 122
  edit 122
  object class 122
LDAP container
  address 120
  business unit 118
  contact 120
  domain 118
  edit 118
  manage 118
  object class 118
  target system manager 71, 118
LDAP domain
  account definition 74
  account definition (initial) 56
  application roles 8
  category 77, 115
  domain name 76
  edit 74
  employee assignment 98
  object class 76
  overview of all assignments 126
  setup 74
  synchronization 74
  system type 74
  target system manager 8, 71, 74
LDAP group
  add to 111
  add to system role 110

administrator 103
assign computers 105, 109, 123
assign extended property 117
assign group 109, 123
assign to business roles 107
assign to cost center 106
assign to department 106
assign to location 106
assign user account 95, 105, 108
business unit 103
category 103, 115
container 103
delete 117
domain 103
object class 103
risk index 103
service item 103
setup 103
LDAP user account
  account definition 56, 87
  account manager 92
  address 92
  assign employee 79, 86-87, 96
  assign extended property 95
  assign group 95, 108
  business unit 92
  category 87, 115
  company 92
  container 87
  default PC 93
delete 102
department 92
disable 87, 100
domain 87
e-mail address 91
employee 87
employee number 92
identity 87
image 91
inherit applications 87
inherit groups 87
location 92
lock 100, 102
login name 87
manage 79
manage level 87, 94
object class 87
password
  initial 69
privileged user account 87
restore 102
risk index 87
setup 86
telephone call 91
title 92
user ID 93
wizard 92
logon information 70

M
membership
  change provisioning 36

N
notification 70

O
object
  delete immediately 34

outstanding 34
publishing 34
One Identity Manager
  administrator 8
  target system administrator 8
  target system manager 8, 71, 118
  user 8
outstanding object 34

P
password
  initial 70
password policy 59
  assign 60
  character classes 65
  check password 69
  check script 66
  default policy 60, 63
  deny list 68
  display name 63
  editing 63
  error message 63
  failed logins 64
  generate password 69
  generate script 66-67
  initial password 64
  name properties 64
  password age 64
  password cycle 64
  password length 64
  password strength 64
  predefined 59
project template
  Active Directory Lightweight Directory Services 133
OpenDJ 132
provisioning
        member list 36

R
revision filter 33

S
schedule
        deactivation 38
schema
        changes 32
        compress 32
        update 32
synchronization
        accelerate 33
        base object
        create 31
        configuration 29
        configure 17
        connection parameter 29
        connection parameters 17, 31
        extended schema 31
        permissions 12
        prevent 38
        run 17
        scope 29
        set up 11
        several domains 31
synchronization project
        create 17
        target system schema 31
        users 12
        variable 29
variable set 31
workflow 17, 31
synchronization analysis report 37
synchronization configuration
        adapt 29, 31
        customize 31
synchronization direction
        to target system 31
synchronization log 28
synchronization project
        create 17
        deactivation 38
        editing 77
        project template 132
synchronization server
        configuring 14
        install 14
        Job server 14
synchronization workflow
        create 17
        set up 31

T
target system reconciliation 34
template
        IT operating data, modify 49

U
user account
        administrative user account 82-84
        apply template 49
        default user account 82
        identity 80
password
  notification 70
privileged user account 80, 85
type 80, 82, 85