



## One Identity Manager 9.2

# Administration Guide for Connecting Unix-Based Target Systems

**Copyright 2023 One Identity LLC.**

**ALL RIGHTS RESERVED.**

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

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

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

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

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

**Patents**

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

**Trademarks**

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal/trademark-information.aspx](http://www.OneIdentity.com/legal/trademark-information.aspx). All other trademarks are the property of their respective owners.

**Legend**

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

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

One Identity Manager Administration Guide for Connecting Unix-Based Target Systems  
Updated - 29 September 2023, 05:21

For the most recent documents and product information, see [Online product documentation](#).

# Contents

<b>Managing Unix-based systems</b> .....	<b>8</b>
Architecture overview .....	8
One Identity Manager users for managing Unix-based target systems .....	9
Configuration parameters for managing Unix-based target systems .....	11
<b>Synchronizing Unix-based target systems</b> .....	<b>12</b>
Setting up initial synchronization with a Unix host .....	12
Users and permissions for synchronizing with a Unix-based target system .....	13
Configuring Unix the host .....	15
Setting up a synchronization server for Unix-based target systems .....	15
System requirements for the Unix synchronization server .....	15
Installing One Identity Manager Service with a Unix or AIX connector .....	16
Creating a synchronization project for initial synchronization of a Unix host .....	19
Information required for setting up a synchronization project .....	19
Creating an initial synchronization project for a Unix host .....	22
Configuring the synchronization log .....	25
Customizing the synchronization configuration .....	26
Configuring Unix host synchronization .....	27
Configuring synchronization of several Unix hosts .....	28
Changing system connection settings of Unix hosts .....	29
Editing connection parameters in the variable set .....	29
Editing target system connection properties .....	30
Updating schemas .....	31
Configuring the provisioning of memberships .....	32
Configuring single object synchronization .....	33
Accelerating provisioning and single object synchronization .....	34
Running synchronization .....	36
Starting synchronization .....	36
Deactivating synchronization .....	37
Displaying synchronization results .....	38
Synchronizing single objects .....	39
Tasks following synchronization .....	39

Post-processing outstanding objects .....	40
Adding custom tables to the target system synchronization .....	42
Managing Unix user accounts through account definitions .....	42
Troubleshooting .....	43
Ignoring data error in synchronization .....	44
Pausing handling of target system specific processes (Offline mode) .....	44
<b>Managing Unix user accounts and identities .....</b>	<b>47</b>
Account definitions for Unix user accounts .....	48
Creating account definitions .....	49
Editing account definitions .....	49
Main data for an account definition .....	50
Editing manage levels .....	52
Creating manage levels .....	53
Assigning manage levels to account definitions .....	54
Main data for manage levels .....	54
Creating mapping rules for IT operating data .....	55
Entering IT operating data .....	57
Modify IT operating data .....	58
Assigning account definitions to identities .....	59
Assigning account definitions to departments, cost centers, and locations .....	60
Assigning account definitions to business roles .....	61
Assigning account definitions to all identities .....	61
Assigning account definitions directly to identities .....	62
Assigning account definitions to system roles .....	63
Adding account definitions to the IT Shop .....	64
Assigning account definitions to Unix hosts .....	66
Deleting account definitions .....	66
Assigning identities automatically to Unix user accounts .....	69
Editing search criteria for automatic identity assignment .....	71
Finding identities and directly assigning them to user accounts .....	72
Changing manage levels for Unix user accounts .....	73
Supported user account types .....	74
Default user accounts .....	75
Administrative user accounts .....	76
Providing administrative user accounts for one identity .....	76

Providing administrative user accounts for several people .....	77
Privileged user accounts .....	78
Specifying deferred deletion for Unix user accounts .....	80
<b>Managing memberships in Unix groups .....</b>	<b>81</b>
Assigning Unix groups to Unix user accounts .....	81
Prerequisites for indirect assignment of Unix groups to Unix user accounts .....	82
Assigning Unix groups to departments, cost centers and locations .....	83
Assigning Unix groups to business roles .....	85
Adding Unix groups to system roles .....	86
Adding Unix groups to the IT Shop .....	86
Removing Unix groups from an IT Shop shelf .....	87
Removing Unix groups from all IT Shop shelves .....	88
Assigning Unix user accounts directly to Unix groups .....	88
Assigning Unix groups directly to Unix user accounts .....	89
Effectiveness of membership in Unix user groups .....	89
Unix group inheritance based on categories .....	92
Overview of all assignments .....	94
<b>Login credentials for Unix user accounts .....</b>	<b>96</b>
Password policies for Unix user accounts .....	96
Predefined password policies .....	97
Using password policies .....	98
Creating password policies .....	99
Editing password policies .....	100
General main data for password policies .....	100
Character classes for passwords .....	101
Policy settings .....	102
Custom scripts for password requirements .....	104
Checking passwords with a script .....	104
Generating passwords with a script .....	105
Password exclusion list .....	107
Checking a password .....	107
Testing password generation .....	107
Initial password for new Unix user accounts .....	108
Email notifications about login data .....	108

<b>Mapping Unix objects in One Identity Manager</b> .....	<b>110</b>
Unix hosts .....	110
General main data of Unix hosts .....	111
Defining categories for the inheritance of entitlements .....	112
Editing the synchronization project for a Unix host .....	113
Displaying the Unix hosts overview .....	113
Displaying Unix login shells .....	114
Unix user accounts .....	114
Creating and editing Unix user accounts .....	115
General main data of Unix user accounts .....	116
User account main data for AIX systems .....	120
Limits for user accounts .....	120
Password data for user accounts .....	121
Security-related main data for user accounts .....	122
Main data for user accounts on an encrypted file system .....	124
Assigning extended properties to Unix user accounts .....	125
Disabling AIX system user accounts .....	126
Deleting and restoring Unix user accounts .....	127
Displaying the Unix user account overview .....	128
Unix groups .....	128
Creating and editing Unix groups .....	128
General main data for Unix groups .....	129
Adding Unix groups to Unix groups .....	130
Assigning extended properties to Unix groups .....	131
Deleting Unix groups .....	131
Displaying the Unix group overview .....	131
Reports about Unix objects .....	132
<b>Handling of Unix objects in the Web Portal</b> .....	<b>134</b>
<b>Basic data for Unix-based target systems</b> .....	<b>136</b>
Target system managers for Unix-based systems .....	137
Job server for Unix-specific process handling .....	139
General main data for a Job server .....	140
Server functions of a Job server .....	143
<b>Appendix: Configuration parameters for managing Unix-based target</b> .....	<b>145</b>

<b>systems</b> .....	
<b>Appendix: Default project template for Unix-based target systems</b> .....	<b>148</b>
<b>Appendix: Unix connector settings</b> .....	<b>149</b>
<b>About us</b> .....	<b>151</b>
Contacting us .....	151
Technical support resources .....	151
<b>Index</b> .....	<b>152</b>

## Managing Unix-based systems

One Identity Manager offers simplified user account administration for Unix. One Identity Manager concentrates on setting up and editing user accounts and providing the required permissions. To equip users with the required permissions, groups are mapped in One Identity Manager. This makes it possible to use Identity and Access Governance processes such as attesting, Identity Audit, user account management and system entitlements, IT Shop, or report subscriptions for Unix based target systems.

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

Additional information about the Unix core directory is loaded into the One Identity Manager database by data synchronization. There are only limited options for customizing this information in One Identity Manager due to the complex dependencies and far-reaching effects of any changes.

One Identity Manager supports most Unix and Linux derivatives. For more information, see the specifications for [One Identity Safeguard Authentication Services](#).

**NOTE:** The Unix Based Target Systems Module must be installed as a prerequisite for managing Unix-based target systems in One Identity Manager. For more information about installing, see the *One Identity Manager Installation Guide*.

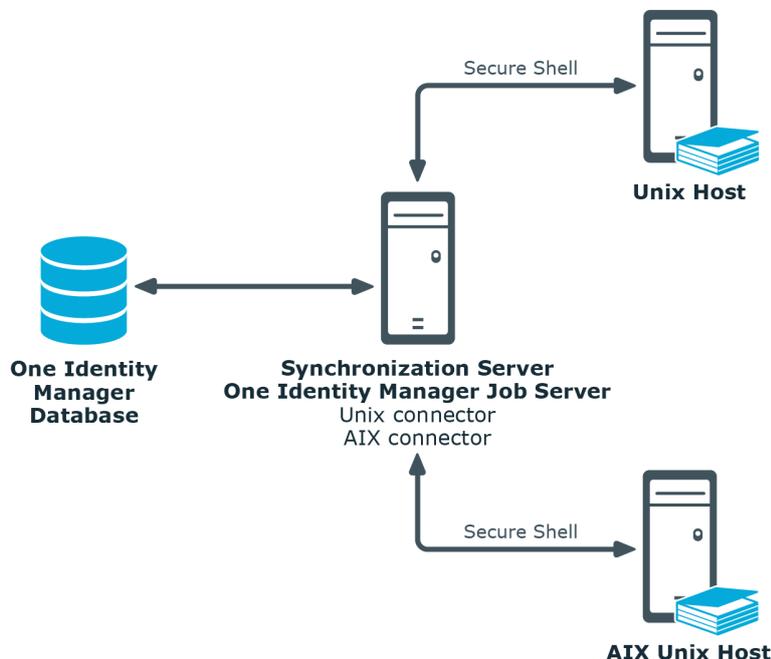
## Architecture overview

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

- Unix host  
Unix host where the directory is kept. This host is a selected live host with a good network connection to the synchronization server. The synchronization server connects to this host in order to access the Unix objects.
- Synchronization server  
The synchronization server for synchronizing the One Identity Manager database with the Unix-based target system. The One Identity Manager Service with the **Unix** machine role is installed on the synchronization server. The **Unix** machine role

contains the Unix connector and the AIX connector. The Unix connector is used for synchronization and provisioning Unix-based objects. The AIX connector is implemented for synchronizing and provisioning IBM AIX systems objects. The connectors communicate directly with the Unix host.

**Figure 1: Architecture for synchronization**



## One Identity Manager users for managing Unix-based target systems

The following users are used for setting up and managing Unix-based target systems.

**Table 1: Users**

Users	Tasks
Target system administrators	<p>Target system administrators must be assigned to the <b>Target systems   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Administer application roles for individual target system types.</li> <li>• Specify the target system manager.</li> <li>• Set up other application roles for target system managers if required.</li> </ul>

Users	Tasks
Target system managers	<ul style="list-style-type: none"> <li>• Specify which application roles for target system managers are mutually exclusive.</li> <li>• Authorize other identities to be target system administrators.</li> <li>• Do not assume any administrative tasks within the target system.</li> </ul> <p>Target system managers must be assigned to the <b>Target systems   Unix</b> application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assume administrative tasks for the target system.</li> <li>• Create, change, or delete target system objects.</li> <li>• Edit password policies for the target system.</li> <li>• Prepare groups to add to the IT Shop.</li> <li>• Can add identities that do not have the <b>Primary identity</b> identity type.</li> <li>• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.</li> <li>• Edit the synchronization's target system types and outstanding objects.</li> <li>• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.</li> </ul>
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> <li>• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.</li> <li>• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.</li> <li>• Enable or disable additional configuration parameters in the Designer as required.</li> <li>• Create custom processes in the Designer as required.</li> <li>• Create and configure schedules as required.</li> </ul>

Users	Tasks
	<ul style="list-style-type: none"> <li>• Create and configure password policies as required.</li> </ul>
Administrators for the IT Shop	<p>Administrators must be assigned to the <b>Request &amp; Fulfillment   IT Shop   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assign groups to IT Shop structures.</li> </ul>
Product owner for the IT Shop	<p>Product owners must be assigned to the <b>Request &amp; Fulfillment   IT Shop   Product owners</b> application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Approve through requests.</li> <li>• Edit service items and service categories under their management.</li> </ul>
Administrators for organizations	<p>Administrators must be assigned to the <b>Identity Management   Organizations   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assign groups to departments, cost centers, and locations.</li> </ul>
Business roles administrators	<p>Administrators must be assigned to the <b>Identity Management   Business roles   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assign groups to business roles.</li> </ul>

## Configuration parameters for managing Unix-based target systems

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

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

For more information, see [Configuration parameters for managing Unix-based target systems](#) on page 145.

## Synchronizing Unix-based target systems

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and the Unix host.

This section explains how to:

- Set up synchronization to import initial data from Unix host to the One Identity Manager database.
- Adjust a synchronization configuration, for example, to synchronize different Unix hosts with the same synchronization project.
- Start and deactivate the synchronization.
- Evaluate the synchronization results.

**TIP:** Before you set up synchronization with a Unix host, familiarize yourself with the Synchronization Editor. For more information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

### Detailed information about this topic

- [Setting up initial synchronization with a Unix host](#) on page 12
- [Customizing the synchronization configuration](#) on page 26
- [Running synchronization](#) on page 36
- [Tasks following synchronization](#) on page 39
- [Troubleshooting](#) on page 43

## Setting up initial synchronization with a Unix host

One Identity Manager supports most Unix and Linux derivatives. For more information, see the specifications for [One Identity Authentication Services](#).

## To load Unix-based objects into the One Identity Manager database for the first time

1. Prepare a user account with sufficient permissions for synchronizing in the Unix-based target system.
2. One Identity Manager components for managing Unix-based target systems are available if the **TargetSystem | Unix** configuration parameter is set.
  - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.  
**NOTE:** If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
  - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

### Related topics

- [Users and permissions for synchronizing with a Unix-based target system](#) on page 13
- [Configuring Unix the host](#) on page 15
- [Setting up a synchronization server for Unix-based target systems](#) on page 15
- [Creating a synchronization project for initial synchronization of a Unix host](#) on page 19
- [Configuration parameters for managing Unix-based target systems](#) on page 145
- [Default project template for Unix-based target systems](#) on page 148

## Users and permissions for synchronizing with a Unix-based target system

The following users play a role in synchronizing One Identity Manager with a Unix-based target system.

**Table 2: Users for synchronization**

User	Permissions
User for accessing the Unix	You must provide a user account with the following

User	Permissions
host	<p>permissions for full synchronization of a Unix-based target system with the supplied One Identity Manager default configuration.</p> <ul style="list-style-type: none"> <li>• Permissions for establishing a Secure Shell (SSH) connection to the host.</li> <li>• Administration permissions for running write operation in the Unix objects.</li> </ul> <p>The rest of the configuration depends on which method is adopted for accessing the Unix host. For more information, see <a href="#">Information required for setting up a synchronization project</a> on page 19.</p>
One Identity Manager Service user account	<p>The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files).</p> <p>The user account must belong to the <b>Domain users</b> group.</p> <p>The user account must have the <b>Login as a service</b> extended user permissions.</p> <p>The user account requires permissions for the internal web service.</p> <p><b>NOTE:</b> If the One Identity Manager Service runs under the network service (<b>NT Authority\NetworkService</b>), you can grant permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://&lt;IP address&gt;:&lt;port number&gt;/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none"> <li>• %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)</li> <li>• %ProgramFiles%\One Identity (on 64-bit operating systems)</li> </ul>
User for accessing the One Identity Manager database	<p>The <b>Synchronization</b> default system user is provided to run synchronization using an application server.</p>

# Configuring Unix the host

The SSH service (sshd daemon) running on the Unix host must be configured so that the **sftp** subsystem is enabled.

## Setting up a synchronization server for Unix-based target systems

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

The One Identity Manager Service with the **Unix** machine role must be installed on the synchronization server. The **Unix** machine role contains the Unix connector and the AIX connector. The Unix connector is used for synchronization and provisioning Unix-based objects. The AIX connector is implemented for synchronizing and provisioning IBM AIX systems objects.

### Detailed information about this topic

- [System requirements for the Unix synchronization server](#) on page 15
- [Installing One Identity Manager Service with a Unix or AIX connector](#) on page 16

## System requirements for the Unix synchronization server

To set up synchronization with a Unix-based target system, a server must be available with the following software installed on it:

- Windows operating system  
The following versions are supported:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework version 4.8 or later

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

# Installing One Identity Manager Service with a Unix or AIX connector

The One Identity Manager Service with the **Unix** machine role is installed on the synchronization server. The **Unix** machine role contains the Unix connector and the AIX connector. The Unix connector is used for synchronization and provisioning Unix-based objects. The AIX connector is implemented for synchronizing and provisioning IBM AIX systems objects.

The synchronization server must be declared as a Job server in One Identity Manager.

**Table 3: Properties of the Job server**

Property	Value
Server function	Unix connector or AIX connector
Machine role	Server   Job Server   Unix

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

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

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

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

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

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

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

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

*One Identity Manager Installation Guide.*

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

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

1. Start the Server Installer program.

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

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

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

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

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

- OR -

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

- b. Enter the following data for the Job server.

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

Syntax:

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

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

4. On the **Machine roles** page, select **Unix**.
5. On the **Server functions** page, select at least one of the following functions:
  - **Unix connector**
  - **AIX connector**
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

**NOTE:** The initial service configuration is predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more information about configuring the service, see the *One Identity Manager Configuration Guide*.

For a direct connection to the database:

- a. In the module list, select **Process collection > sqlprovider**.
- b. Click the **Connection parameter** entry, then click the **Edit** button.
- c. Enter the connection data for the One Identity Manager database.
- d. Click **OK**.

For a connection to the application server:

- a. In the module list, select the **Process collection** entry and click the **Insert** button.
  - b. Select **AppServerJobProvider** and click **OK**.
  - c. In the module list, select **Process collection > AppServerJobProvider**.
  - d. Click the **Connection parameter** entry, then click the **Edit** button.
  - e. Enter the address (URL) for the application server and click **OK**.
  - f. Click the **Authentication data** entry and click the **Edit** button.
  - g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
  - h. Click **OK**.
7. To configure the installation, click **Next**.
  8. Confirm the security prompt with **Yes**.
  9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
  10. On the **Service access** page, enter the service's installation data.
    - **Computer:** Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.  
To run the installation locally, select **Local installation** from the menu.
    - **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

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

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

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

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

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

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

## Creating a synchronization project for initial synchronization of a Unix host

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and the Unix-based target system. 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.

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

### Detailed information about this topic

- [Information required for setting up a synchronization project](#) on page 19
- [Creating an initial synchronization project for a Unix host](#) on page 22
- [Default project template for Unix-based target systems](#) on page 148
- [Unix connector settings](#) on page 149

## Information required for setting up a synchronization project

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

**Table 4: Information required to set up a synchronization project**

Data	Explanation
Server name or IP address of the host	Full name or IP address of the host for connecting to the synchronization server to provide access to Unix objects.
Host communications port	Communications port for establishing a Secure Shell (SSH) connection to the host. The default port is TCP port 22.

Data	Explanation
Authentication	<p>The login data required depends on which authentication method you select.</p> <ul style="list-style-type: none"> <li>• Authentication method <b>Password</b>: User account and password to log in to the host. This user account is used to access the host by SSH. The user account requires permissions for establishing an SSH connection.</li> <li>• Authentication method <b>Private key</b>: File with the private key and the passphrase.</li> </ul>
Method, user name and password for escalating permissions	<p>Running commands requires an administrative context. Make a user account available with sufficient permissions. This user account is used to perform write operations on the Unix objects.</p> <p>Available methods are:</p> <ul style="list-style-type: none"> <li>• <b>Default</b>: The user who logs in to the host already has administrative permissions.</li> <li>• <b>Sudo</b>: The user logged in on the host can run administrative tasks with another user's permissions, such as <b>root</b>. The configuration for this is done in the sudoer file on the host.</li> </ul> <p>Example of a configuration with minimum permissions for an example user <b>OneIM</b>:</p> <pre>OneIM ALL=(root) NOPASSWD: /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel, /usr/bin/passwd, /usr/sbin/groupadd, /bin/mv /tmp/*, /bin/mv /etc/group.tmp /etc/group*, /bin/chmod 644 /etc/group.tmp, /bin/chown * /etc/group.tmp</pre> <ul style="list-style-type: none"> <li>• <b>su</b>: This method uses the su command to change the context. Another user with administrative permissions is required.</li> </ul>
Synchronization server of the Unix-based target system	<p>All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>The One Identity Manager Service must be installed on the synchronization server with the Unix connector.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• Server function: <b>Unix connector or AIX connector</b></li> </ul>

Data	Explanation
One Identity Manager database connection data	<ul style="list-style-type: none"> <li>Machine role: <b>Server   Job Server   Unix</b></li> </ul> <ul style="list-style-type: none"> <li>Database server</li> <li>Database name</li> <li>SQL Server login and password</li> <li>Specifies whether integrated Windows authentication is used</li> </ul> <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p>
Remote connection server	<p>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> <li>One Identity Manager Service is started</li> <li><b>RemoteConnectPlugin</b> is installed</li> <li>Unix connector or AIX connector is installed</li> </ul> <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p><b>TIP:</b> The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time by installing the <b>RemoteConnectPlugin</b> as well.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>

## Related topics

- [Users and permissions for synchronizing with a Unix-based target system](#) on page 13
- [Setting up a synchronization server for Unix-based target systems](#) on page 15

# Creating an initial synchronization project for a Unix host

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

- Run in default mode
- Started from the Launchpad

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

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

## ***To set up an initial synchronization project for a Unix-based target system***

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

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

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

This starts the Synchronization Editor's project wizard.

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

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

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

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

5. On the **General connection settings** page, enter the connection data for the Unix host.

- a. In the **Server or IP** field, enter the server name or the IP address of the host.
- b. In the **Port** field, enter the communications port for establishing the SSH connection. The default communications port is the TCP port **22**.
- c. Select the authentication method. Depending on the method you choose, enter the other information for authentication.
  - For the **Password** authentication method, enter the user account and password for SSH login to the host.

- For the **Private key** authentication method, you need the private key and the passphrase.
- d. Click **Test** to test the connection. The system tries to establish a connection to the host.
  6. In the **Verify connection** pane, click **Test** to test the connection to the host.
  7. On **Change to administrative context** page, select the method to use for obtaining administrative permissions.
    - If the user already possesses administrative permissions, select the **Default** method.
    - If the current user logged in on the host can run administrative tasks as an administrative user, select the **Sudo** method. In the **User name** field, enter an alternative user, such as **root**.
    - If administrative tasks should be run using a different user, select the **su** method. In the **User** and **Password** fields, enter the login data of the other user. The default user is **root**.
  8. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.
- NOTE:**
- If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again.
  - This page is not shown if a synchronization project already exists.
9. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
  10. On the **Restrict target system access** page, specify how system access should work. You have the following options:

**Table 5: Specify target system access**

Option	Meaning
	<p>Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none"> <li>• Synchronization is in the direction of <b>One Identity Manager</b>.</li> <li>• Processing methods in the synchronization steps are only defined for synchronization in the direction of <b>One Identity Manager</b>.</li> </ul>

Option	Meaning
Read/write access to target system. Provisioning available.	<p>Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none"> <li>• Synchronization is in the direction of the <b>Target system</b>.</li> <li>• Processing methods are only defined in the synchronization steps for synchronization in the direction of the <b>Target system</b>.</li> <li>• Synchronization steps are only created for such schema classes whose schema types have write access.</li> </ul>

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

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

- a. Click  to add a new Job server.
- b. Enter a name for the Job server and the full server name conforming to DNS syntax.

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

- To select a Job server, click .

This automatically assigns the server function matching this Job server.

- c. Click **OK**.

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

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

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

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

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

**NOTE:**

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

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

- If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically option**. In this case, save the synchronization project manually before closing the Synchronization Editor.
- The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

## Related topics

- [Information required for setting up a synchronization project](#) on page 19
- [Users and permissions for synchronizing with a Unix-based target system](#) on page 13
- [Setting up a synchronization server for Unix-based target systems](#) on page 15
- [Configuring the synchronization log](#) on page 25
- [Customizing the synchronization configuration](#) on page 26
- [Tasks following synchronization](#) on page 39
- [Default project template for Unix-based target systems](#) on page 148
- [Unix connector settings](#) on page 149

# Configuring the synchronization log

All the information, tips, warnings, and errors that occur during synchronization are recorded in the synchronization log. You can configure the type of information to record separately for each system connection and synchronization workflow.

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

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

- OR -

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

2. In the **General** section, click **Setup**.
3. In the **Synchronization log** section, set **Create synchronization log**.
4. Enable the data to be logged.

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

| analyzes.

5. Click **OK**.

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

1. In the Synchronization Editor, select the **Workflows** category.
2. Select a workflow in the navigation view.
3. In the **General** section, click **Edit**.
4. Select the **Synchronization log** tab.
5. Enable the data to be logged.

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

6. Click **OK**.

Synchronization logs are stored for a fixed length of time.

### ***To modify the retention period for synchronization logs***

- In the Designer, enable the **DPR | Journal | LifeTime** configuration parameter and enter the maximum retention period.

### **Related topics**

- [Displaying synchronization results](#) on page 38

## **Customizing the synchronization configuration**

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a Unix host, you can use the synchronization project to load Unix objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Unix-based target system.

You must customize the synchronization configuration in order to compare the database with the Unix-based target system regularly and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema

classes, or processing method, for example.

- Use variables to set up a synchronization project for synchronizing different hosts. Store a connection parameter as a variable for logging onto the hosts.
- To specify which Unix objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

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

### Detailed information about this topic

- [Configuring Unix host synchronization](#) on page 27
- [Configuring synchronization of several Unix hosts](#) on page 28
- [Changing system connection settings of Unix hosts](#) on page 29
- [Updating schemas](#) on page 31
- [Configuring the provisioning of memberships](#) on page 32
- [Configuring single object synchronization](#) on page 33
- [Accelerating provisioning and single object synchronization](#) on page 34

## Configuring Unix host synchronization

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

### **To create a synchronization configuration for synchronizing a Unix host**

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.  
This creates a workflow with **Target system** as its direction of synchronization.
4. Create a new start up configuration. Use the new workflow to do this.

5. Save the changes.
6. Run a consistency check.

### Detailed information about this topic

- [Configuring synchronization of several Unix hosts](#) on page 28

## Configuring synchronization of several Unix hosts

In some circumstances, you can use a synchronization project to synchronize different Unix hosts.

### Prerequisites

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

### *To customize a synchronization project for synchronizing another host*

1. Prepare a user account with sufficient permissions for synchronizing in the other host.
2. In the Synchronization Editor, open the synchronization project.
3. Create a new base object for the other host.
  - Use the wizard to attach a base object.
  - In the wizard, select the Unix connector or the AIX connector.
  - Declare the connection parameters. The connection parameters are saved in a special variable set.

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

4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

### Related topics

- [Configuring Unix host synchronization](#) on page 27

# Changing system connection settings of Unix hosts

When you set up synchronization for the first time, the system connection properties are set to default values that you can modify. There are two ways to do this:

- a. Specify a specialized variable set and change the values of the affected variables.  
The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).
- b. Edit the target system connection with the system connection wizard and change the effected values.  
The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

## Detailed information about this topic

- [Editing connection parameters in the variable set](#) on page 29
- [Editing target system connection properties](#) on page 30
- [Unix connector settings](#) on page 149

## Editing connection parameters in the variable set

The connection parameters were saved as variables in the default variable set when synchronization was set up. You can change the values in these variables to suit your requirements and assign the variable set to a start up configuration and a base object. This means that you always have the option to use default values from the default variable set.

**NOTE:** To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project is used for synchronizing different Unix hosts.

### *To customize connection parameters in a specialized variable set*

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.  
Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.  
All specialized variable sets are shown in the lower part of the document view.

6. Select a specialized variable set or click on  in the variable set view's toolbar.
  - To rename the variable set, select the variable set and click the variable set view in the toolbar . Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration > Base objects** category.
13. Select the base object and click .
- OR -  
To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

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

## Related topics

- [Editing target system connection properties](#) on page 30

# Editing target system connection properties

You can also use the system connection wizard to change the connection parameters. If variables are defined for the settings, the changes are transferred to the active variable set.

**NOTE:** In the following circumstances, the default values cannot be restored:

- The connection parameters are not defined as variables.
- The default variable set is selected as an active variable set.

In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

### ***To edit connection parameters using the system connection wizard***

1. In the Synchronization Editor, open the synchronization project.
2. In the toolbar, select the active variable set to be used for the connection to the target system.

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

3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.  
This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

## Related topics

- [Editing connection parameters in the variable set](#) on page 29

# Updating schemas

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

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

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

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

### **To update a system connection schema**

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.

- OR -

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

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

This reloads the schema data.

### **To edit a mapping**

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

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

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

## Configuring the provisioning of memberships

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

- Memberships are saved as an object property in list form in the target system.
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and previously deleted memberships are added again.

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

### **To allow separate provisioning of memberships**

1. In the Manager, select the **Unix > Basic configuration data > Target system types** category.
2. In the result list, select the **Unix** target system type.
3. Select the **Configure tables for publishing** task.

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

**NOTE:**

- This option can only be enabled for assignment tables that have a base table with a XDateSubItem column.
- Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.

6. Save the changes.

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

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

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

### **To restore the original condition**

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

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

Example of a condition on the UNXAccountInUNXGroup assignment table:

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

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

## Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already

present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

## Prerequisites

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

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

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

1. In the Manager, select the **Unix > Basic configuration data > Target system types** category.
2. In the result list, select the **Unix** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.  
Enter the path to the base object in the ObjectWalker notation of the VI.DB.  
Example: `FK(UID_UNXHost).XObjectKey`
8. Save the changes.

## Related topics

- [Synchronizing single objects](#) on page 39
- [Post-processing outstanding objects](#) on page 40

# Accelerating provisioning and single object synchronization

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

these processes.

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

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

### **To configure load balancing**

1. Configure the server and declare it as a Job server in One Identity Manager.
  - Job servers that share processing must have the **No process assignment** option enabled.
  - Assign the **Unix connector** server function to the Job server.

All Job servers must access the same Unix host as the synchronization server for the respective base object.

2. In the Synchronization Editor, assign a custom server function to the base object.  
This server function is used to identify all the Job servers being used for load balancing.

If there is no custom server function for the base object, create a new one.

For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.  
Only select those Job servers that have the same configuration as the base object's synchronization server.

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

### **To use the synchronization server without load balancing.**

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

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

### **Detailed information about this topic**

- [Job server for Unix-specific process handling](#) on page 139

# Running synchronization

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

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

## Detailed information about this topic

- [Starting synchronization](#) on page 36
- [Deactivating synchronization](#) on page 37
- [Displaying synchronization results](#) on page 38
- [Synchronizing single objects](#) on page 39
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 44

## Starting synchronization

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

### **To synchronize on a regular basis**

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

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

### **To start initial synchronization manually**

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

3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
  - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
  - Use the schedule to ensure that the start up configurations are run in sequence.
  - Group start up configurations with the same start up behavior.

## Deactivating synchronization

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

### **To prevent regular synchronization**

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

Now you can only start synchronization manually.

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

## Detailed information about this topic

- [Creating a synchronization project for initial synchronization of a Unix host](#) on page 19
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 44

# Displaying synchronization results

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

### *To display a synchronization log*

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ► in the navigation view toolbar.  
Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking it.  
An analysis of the synchronization is shown as a report. You can save the report.

### *To display a provisioning log*

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ⚡ in the navigation view toolbar.  
Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking it.  
An analysis of the provisioning is shown as a report. You can save the report.

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

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

## Related topics

- [Configuring the synchronization log](#) on page 25
- [Troubleshooting](#) on page 43

# Synchronizing single objects

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

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

## To synchronize a single object

1. In the Manager, select the **Unix** category.
2. Select the object type in the navigation view.
3. In the result list, select the object that you want to synchronize.
4. Select the **Synchronize this object** task.

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

## Features of synchronizing memberships

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

### Example:

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

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

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

## Detailed information about this topic

- [Configuring single object synchronization](#) on page 33

# Tasks following synchronization

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

- [Post-processing outstanding objects](#) on page 40
- [Adding custom tables to the target system synchronization](#) on page 42
- [Managing Unix user accounts through account definitions](#) on page 42

## Post-processing outstanding objects

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

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

### ***To post-process outstanding objects***

1. In the Manager, select the **Unix > Target system synchronization: Unix** category.

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

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

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

- The synchronization log has already been deleted.  
- OR -
- An assignment from a member list has been deleted from the target system.  
The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.
- An object that contains a member list has been deleted from the target system.

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

**TIP:**

**To display object properties of an outstanding object**

1. Select the object on the target system synchronization form.
2. Open the context menu and click **Show object**.
3. Select the objects you want to rework. Multi-select is possible.
4. Click on one of the following icons in the form toolbar to run the respective method.

**Table 6: Methods for handling outstanding objects**

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account.  Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The <b>Outstanding</b> label is removed from the object.  This runs a target system specific process that triggers the provisioning process for the object.  Prerequisites: <ul style="list-style-type: none"><li>• The table containing the object can be published.</li><li>• The target system connector has write access to the target system.</li></ul>
	Reset	The <b>Outstanding</b> label is removed for the object.

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

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

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

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

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

**To disable bulk processing**

- Disable the  icon in the form's toolbar.

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

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

## Adding custom tables to the target system synchronization

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

### *To add custom tables to target system synchronization*

1. In the Manager, select the **Unix > Basic configuration data > Target system types** category.
2. In the result list, select the **Unix** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

### Related topics

- [Post-processing outstanding objects](#) on page 40

## Managing Unix user accounts through account definitions

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

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

### *To manage user accounts through account definitions*

1. Create an account definition.
2. Assign an account definition to the host.

3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
  - a. In the Manager, select the **Unix > User accounts > Linked but not configured > <host>** category.
  - b. Select the **Assign account definition to linked accounts** task.
  - c. In the **Account definition** menu, select the account definition.
  - d. Select the user accounts that contain the account definition.
  - e. Save the changes.

## Related topics

- [Account definitions for Unix user accounts](#) on page 48

# Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- **Simulating synchronization**

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

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

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

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

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

## Related topics

- [Displaying synchronization results](#) on page 38

# Ignoring data error in synchronization

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

## *To ignoring data errors during synchronization in One Identity Manager*

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

This starts the system connection wizard.

4. On the **Additional options** page, enable **Try to ignore data errors**.

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

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

5. Save the changes.

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

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

## Pausing handling of target system specific processes (Offline mode)

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

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

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

## Prerequisites

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

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

### **To allow offline mode for a base object**

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Base objects** category.
3. Select a base object in the document view and click .
4. Enable **Offline mode available**.
5. Click **OK**.
6. Save the changes.

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

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

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

### **To flag a target system as offline**

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select **Manage > System monitoring > Flag target systems as offline**.
3. Click **Run**.

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

4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

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

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

## Related topics

- [Deactivating synchronization](#) on page 37

## Managing Unix user accounts and identities

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

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

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

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

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

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

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

## Related topics

- [Account definitions for Unix user accounts on page 48](#)
- [Assigning identities automatically to Unix user accounts on page 69](#)
- [Specifying deferred deletion for Unix user accounts on page 80](#)
- [Creating and editing Unix user accounts on page 115](#)

# Account definitions for Unix user accounts

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

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

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

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

For more detailed information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Collecting IT operating data
- Assigning account definitions to identities and target systems

## Detailed information about this topic

- [Creating account definitions](#) on page 49
- [Editing account definitions](#) on page 49
- [Main data for an account definition](#) on page 50
- [Editing manage levels](#) on page 52
- [Creating manage levels](#) on page 53
- [Main data for manage levels](#) on page 54
- [Creating mapping rules for IT operating data](#) on page 55
- [Entering IT operating data](#) on page 57
- [Modify IT operating data](#) on page 58
- [Assigning account definitions to identities](#) on page 59
- [Assigning account definitions to Unix hosts](#) on page 66
- [Deleting account definitions](#) on page 66

# Creating account definitions

Create one or more account definitions for the target system.

### *To create a new account definition*

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

## Detailed information about this topic

- [Main data for an account definition](#) on page 50

# Editing account definitions

You can edit the main data of account definitions.

### *To edit an account definition*

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

2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Enter the account definition's main data.
5. Save the changes.

### Related topics

- [Main data for an account definition](#) on page 50
- [Creating account definitions](#) on page 49
- [Assigning manage levels to account definitions](#) on page 54

## Main data for an account definition

Enter the following data for an account definition:

**Table 7: Main data for an account definition**

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically.  Leave empty for Unix hosts.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assigning the account definition to identities. Set a value in the range <b>0</b> to <b>1</b> . This input field is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set.  For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.

Property	Description
IT Shop	Specifies whether the account definition can be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The resource can also be assigned directly to identities and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to identities	<p>Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the <b>Enable automatic assignment to identities</b>. The account definition is assigned to every identity that is not marked as external. Once a new internal identity is created, they automatically obtain this account definition.</p> <p>To automatically remove the account definition assignment from all identities, use the <b>Disable automatic assignment to identities</b>. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.</p>
Retain account definition if permanently disabled	<p>Specifies the account definition assignment to permanently deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition if temporarily disabled	<p>Specifies the account definition assignment to temporarily deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on deferred deletion	<p>Specifies the account definition assignment on deferred deletion of identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>

Property	Description
Retain account definition on security risk	<p>Specifies the account definition assignment to identities posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> <li>• If you add an identity with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.</li> <li>• If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.</li> </ul>

## Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged:** User accounts with the **Unmanaged** manage level are linked to the identity but they do not inherit any further properties. When a new user account is added with this manage level and an identity is assigned, some of the identity's properties are transferred initially. If the identity properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed:** User accounts with the **Full managed** manage level inherit defined properties of the assigned identity. When a new user account is created with this manage level and an identity is assigned, the identity's properties are transferred in an initial state. If the identity properties are changed at a later date, the changes are passed onto the user account.

**NOTE:** The **Full managed** and **Unmanaged** manage levels are analyzed in templates. You can customize the supplied templates in the Designer.

You can define other manage levels depending on your requirements. You need to amend the templates to include manage level approaches.

Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

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

### **To edit a manage level**

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list.
3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

### **Related topics**

- [Main data for manage levels](#) on page 54
- [Creating manage levels](#) on page 53
- [Assigning manage levels to account definitions](#) on page 54

## **Creating manage levels**

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

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

### **To create a manage level**

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Manage levels** category.
2. Click  in the result list.

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

### Related topics

- [Main data for manage levels](#) on page 54
- [Editing account definitions](#) on page 49
- [Assigning manage levels to account definitions](#) on page 54

## Assigning manage levels to account definitions

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

### To assign manage levels to an account definition

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage level.

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

#### To remove an assignment

- Select the manage level and double-click .
5. Save the changes.

## Main data for manage levels

Enter the following data for a manage level.

**Table 8: Main data for manage levels**

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are:

Property	Description
	<ul style="list-style-type: none"> <li>• <b>Never:</b> Data is not updated. (Default)</li> <li>• <b>Always:</b> Data is always updated.</li> <li>• <b>Only initially:</b> Data is only determined at the start.</li> </ul>
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated identities are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated identities retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated identities are locked.
Retain groups on deferred deletion	Specifies whether user accounts of identities marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of identities marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of identities posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of identities posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

## Creating mapping rules for IT operating data

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

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

- Login shell
- Groups can be inherited
- Identity
- Privileged user account.

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

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
  - **Column:** User account property for which the value is set. In the menu, you can select the columns that use the TSB\_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
  - **Source:** Specifies which roles to use in order to find the user account properties. You have the following options:
    - Primary department
    - Primary location
    - Primary cost center
    - Primary business roles

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

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

  - **Default value:** Default value of the property for an identity's user account if the value is not determined dynamically from the IT operating data.
  - **Always use default value:** Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
  - **Notify when applying the default:** Specifies whether an email is sent to a specific mailbox when the default value is used. The **Identity - new user account with default properties created** mail template is used.

To change the mail template, in the Designer, adjust the **TargetSystem | Unix | Accounts | MailTemplateDefaultValues** configuration parameter.
5. Save the changes.

### Related topics

- [Entering IT operating data](#) on page 57

# Entering IT operating data

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity is assigned a primary business role, primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

## Example:

Normally, each identity in department A obtains a default user account in the host A. In addition, certain identities in department A obtain administrative user accounts in the host A.

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

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

## To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.
3. Click **Add** and enter the following data.
  - **Effects on:** Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

### To specify an application scope

- a. Click **→** next to the field.
  - b. Under **Table**, select the table that maps the target system for select the **TSBAccountDef** table or an account definition.
  - c. Select the specific target system or account definition under **Effects on**.
  - d. Click **OK**.
- **Column:** Select the user account property for which the value is set.

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

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

## Related topics

- [Creating mapping rules for IT operating data](#) on page 55

# Modify IT operating data

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

## Prerequisites

- The IT operating data of a department, a cost center, a business role, or a location have been changed.  
- OR -
- The default values in the IT operating data template were modified for an account definition.

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

## To run the template

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Run templates** task.

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

- **Old value:** Value of the object property before changing the IT operating data.
- **New value:** Value of the object property after changing the IT operating data.
- **Selection:** Specifies whether the new value is copied to the user account.

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

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

## Assigning account definitions to identities

Account definitions are assigned to company identities.

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

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

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

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

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

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

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

#### *To configure assignments to roles of a role class*

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

- OR -

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

2. Select the **Configure role assignments** task and configure the permitted assignments.
  - To generally allow an assignment, enable the **Assignments allowed** column.
  - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

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

### Detailed information about this topic

- [Assigning account definitions to departments, cost centers, and locations](#) on page 60
- [Assigning account definitions to business roles](#) on page 61
- [Assigning account definitions to all identities](#) on page 61
- [Assigning account definitions directly to identities](#) on page 62
- [Assigning account definitions to system roles](#) on page 63
- [Adding account definitions to the IT Shop](#) on page 64

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

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

### *To add account definitions to hierarchical roles*

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
  - On the **Departments** tab, assign departments.
  - On the **Locations** tab, assign locations.
  - On the **Cost centers** tab, assign cost centers.

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

### *To remove an assignment*

- Select the organization and double-click .
5. Save the changes.

## Related topics

- [Assigning account definitions to business roles](#) on page 61
- [Assigning account definitions to all identities](#) on page 61
- [Assigning account definitions directly to identities](#) on page 62
- [Assigning account definitions to system roles](#) on page 63
- [Adding account definitions to the IT Shop](#) on page 64

## Assigning account definitions to business roles

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

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

### *To add account definitions to hierarchical roles*

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

#### **To remove an assignment**

- Select the business role and double-click .
5. Save the changes.

## Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 60
- [Assigning account definitions to all identities](#) on page 61
- [Assigning account definitions directly to identities](#) on page 62
- [Assigning account definitions to system roles](#) on page 63
- [Adding account definitions to the IT Shop](#) on page 64

## Assigning account definitions to all identities

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

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

### ***To assign an account definition to all identities***

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to identities** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

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

### **Related topics**

- [Assigning account definitions to departments, cost centers, and locations](#) on page 60
- [Assigning account definitions to business roles](#) on page 61
- [Assigning account definitions directly to identities](#) on page 62
- [Assigning account definitions to system roles](#) on page 63
- [Adding account definitions to the IT Shop](#) on page 64

## **Assigning account definitions directly to identities**

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

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

### ***To assign an account definition directly to identities***

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign to identities** task.
4. In the **Add assignments** pane, add identities.

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

### **To remove an assignment**

- Select the identity and double-click .

5. Save the changes.

### **Related topics**

- [Assigning account definitions to departments, cost centers, and locations](#) on page 60
- [Assigning account definitions to business roles](#) on page 61
- [Assigning account definitions to all identities](#) on page 61
- [Assigning account definitions to system roles](#) on page 63
- [Adding account definitions to the IT Shop](#) on page 64

## **Assigning account definitions to system roles**

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

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

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

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

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

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

### **To remove an assignment**

- Select the system role and double-click .

5. Save the changes.

### **Related topics**

- [Assigning account definitions to departments, cost centers, and locations](#) on page 60
- [Assigning account definitions to business roles](#) on page 61
- [Assigning account definitions to all identities](#) on page 61
- [Assigning account definitions directly to identities](#) on page 62
- [Adding account definitions to the IT Shop](#) on page 64

## Adding account definitions to the IT Shop

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

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

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

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

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

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

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.

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

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

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

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

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

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

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

1. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

## Related topics

- [Main data for an account definition](#) on page 50
- [Assigning account definitions to departments, cost centers, and locations](#) on page 60

- [Assigning account definitions to business roles](#) on page 61
- [Assigning account definitions to all identities](#) on page 61
- [Assigning account definitions directly to identities](#) on page 62
- [Assigning account definitions to system roles](#) on page 63

## Assigning account definitions to Unix hosts

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

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

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

### *To assign the account definition to a target system*

1. In the Manager, select the host in the **Unix > Hosts** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

### Detailed information about this topic

- [Assigning identities automatically to Unix user accounts](#) on page 69

## Deleting account definitions

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

### *To delete an account definition*

1. Remove automatic assignments of the account definition from all identities.
  - a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Select the **Change main data** task.

- d. Select the **Disable automatic assignment to identities** task.
  - e. Confirm the security prompt with **Yes**.
  - f. Save the changes.
2. Remove direct assignments of the account definition to identities.
  - a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Select the **Assign to identities** task.
  - d. In the **Remove assignments** pane, remove identities.
  - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
  - a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Select the **Assign organizations** task.
  - d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.
  - e. Save the changes.
4. Remove the account definition's assignments to business roles.
  - a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Select the **Assign business roles** task.
  - d. In the **Remove assignments** pane, remove the business roles.
  - e. Save the changes.
5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

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

- a. In the Manager, select the **Entitlements > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.

- e. Click **OK**.

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

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

- a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

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

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
  - a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Select the **Change main data** task.
  - d. From the **Required account definition** menu, remove the account definition.
  - e. Save the changes.
7. Remove the account definition's assignments to target systems.
  - a. In the Manager, select the host in the **Unix > Hosts** category.
  - b. Select the **Change main data** task.
  - c. On the **General** tab, remove the assigned account definitions.
  - d. Save the changes.
8. Delete the account definition.
  - a. In the Manager, select the **Unix > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Click  to delete an account definition.

# Assigning identities automatically to Unix user accounts

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

Define criteria for finding identities to apply to automatic identity assignment. If a user account is linked to an identity through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

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

Run the following tasks to assign identities automatically.

- If you want identities to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | Unix | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want identities to be assigned outside synchronization, in the Designer, set the **TargetSystem | Unix | PersonAutoDefault** configuration parameter and select the required mode.
- In the **TargetSystem | Unix | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to identities shall take place.

Example:

ROOT

**TIP:** You can edit the value of the configuration parameter in the **Exclude list for automatic identity assignment** dialog.

## ***To edit the exclude list for automatic identity assignment***

1. In the Designer, edit the **PersonExcludeList** configuration parameter.
2. Click ... next to the **Value** field.

This opens the **Exclude list for Unix user accounts** dialog.

3. To add a new entry, click  **Add**.  
To edit an entry, select it and click  **Edit**.
4. Enter the name of the user account that does not allow identities to be assigned automatically.  
Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.
5. To delete an entry, select it and click  **Delete**.
6. Click **OK**.

- Use the **TargetSystem | Unix | PersonAutoDisabledAccounts** configuration parameter to specify whether identities can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the host. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for identities assigned to the host.

#### NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

#### NOTE:

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

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

For more information, see [Managing Unix user accounts through account definitions](#) on page 42.

## Related topics

- [Creating account definitions](#) on page 49
- [Assigning account definitions to Unix hosts](#) on page 66
- [Changing manage levels for Unix user accounts](#) on page 73
- [Editing search criteria for automatic identity assignment](#) on page 71

# Editing search criteria for automatic identity assignment

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

The criteria for identity assignments are defined for the host. You specify which user account properties must match the identity's properties such that the identity can be assigned to the user account. You can limit search criteria further by using format definitions.

The search criterion is written in XML notation to the **Search criteria for automatic identity assignment** column (AccountToPersonMatchingRule) in the UNXHost table.

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

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

## To specify criteria for identity assignment

1. In the Manager, select the **Unix > Hosts** category.
2. Select the host in the result list.
3. Select the **Define search criteria for identity assignment** task.
4. Specify which user account properties must match with which identity so that the identity is linked to the user account.

**Table 9: Search criteria for user accounts**

<b>Apply to</b>	<b>Identity column</b>	<b>Column for user account</b>
Unix user accounts	Central user account (CentralAccount)	User name (AccountName)

5. Save the changes.

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

## Related topics

- [Finding identities and directly assigning them to user accounts](#) on page 72
- [Assigning identities automatically to Unix user accounts](#) on page 69

# Finding identities and directly assigning them to user accounts

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

- **Suggested assignments:** This view lists all user accounts to which One Identity Manager can assign an identity. All identities are shown that were found using the search criteria and can be assigned.
- **Assigned user accounts:** This view lists all user accounts to which an identity is assigned.
- **No identity assignment:** This view lists all user accounts to which no identity is assigned and for which no identity was found using the search criteria.

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

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

## To apply search criteria to user accounts

1. In the Manager, select the category **Unix > Hosts**.
2. Select the host in the result list.
3. Select the **Define search criteria for identity assignment** task.
4. At the bottom of the form, click **Reload**.

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

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

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

## To assign identities directly to user accounts

- Click **Suggested assignments**.
  1. Click the **Selection** box of all user accounts to which you want to assign the suggested identities. Multi-select is possible.
  2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
  3. Click **Assign selected**.

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

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

- OR -

- Click **No identity assignment**.
  1. Click **Select identity** for the user account to which you want to assign an identity. Select an identity from the menu.
  2. Click the **Selection** box of all user accounts to which you want to assign the selected identities. Multi-select is possible.
  3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
  4. Click **Assign selected**.
  5. Confirm the security prompt with **Yes**.

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

### **To remove assignments**

- Click **Assigned user accounts**.
  1. Click the **Selection** box of all the user accounts with the identity assignment you want to delete. Multi-select is possible.
  2. Click **Remove selected**.
  3. Confirm the security prompt with **Yes**.

The assigned identities are removed from the selected user accounts.

## **Changing manage levels for Unix user accounts**

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

### **To change the manage level for a user account**

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

## Related topics

- [Creating and editing Unix user accounts](#) on page 115

# Supported user account types

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

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

- Identity type

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

**Table 10: Identity types of user accounts**

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

- Privileged user account

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

## Detailed information about this topic

- [Default user accounts](#) on page 75
- [Administrative user accounts](#) on page 76
- [Providing administrative user accounts for one identity](#) on page 76
- [Providing administrative user accounts for several people](#) on page 77
- [Privileged user accounts](#) on page 78

# Default user accounts

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

### *To create default user accounts through account definitions*

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level.
3. Create a formatting rule for IT operating data.

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

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

- In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable the **Always use default value** option.
  - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.  
Specify in the departments, cost centers, locations, or business roles that IT operating data should apply when you set up a user account.
  5. Assign the account definition to identities.

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

## Related topics

- [Account definitions for Unix user accounts](#) on page 48

# Administrative user accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as **Administrator**.

Administrative user accounts are imported into One Identity Manager during synchronization.

**NOTE:** Some administrative user accounts can be automatically identified as privileged user accounts. To do this, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

## Related topics

- [Providing administrative user accounts for one identity](#) on page 76
- [Providing administrative user accounts for several people](#) on page 77

# Providing administrative user accounts for one identity

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

## Prerequisites

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

### ***To prepare an administrative user account for an identity***

1. Label the user account as a personalized administrator identity.
  - a. In the Manager, select the **Unix > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Change main data** task.
  - d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.

2. Link the user account to the identity that will be using this administrative user account.
  - a. In the Manager, select the **Unix > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Change main data** task.
  - d. On the **General** tab, in the **Identity** selection list, select the identity that will be using this administrative user account.

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

## Related topics

- [Providing administrative user accounts for several people](#) on page 77
- For more information about mapping identity types, see the *One Identity Manager Identity Management Base Module Administration Guide*.

# Providing administrative user accounts for several people

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

## Prerequisite

- The user account must be labeled as a shared identity.
- There must be an identity with the type **Shared identity** available. The shared identity must have a manager.
- The identities who are permitted to use the user account must be labeled as a primary identity.

### ***To prepare an administrative user account for multiple identities***

1. Label the user account as a shared identity.
  - a. In the Manager, select the **Unix > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Change main data** task.
  - d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to an identity.
  - a. In the Manager, select the **Unix > User accounts** category.
  - b. Select the user account in the result list.

- c. Select the **Change main data** task.
- d. On the **General** tab, in the **Identity** menu, select an identity the type **Shared identity**.

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

3. Assign the identities who will use this administrative user account to the user account.
  - a. In the Manager, select the **Unix > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Assign identities authorized to use** task.
  - d. In the **Add assignments** pane, add identities.

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

#### **To remove an assignment**

- Select the identity and double-click .

## Related topics

- [Providing administrative user accounts for one identity](#) on page 76
- For more information about mapping identity types, see the *One Identity Manager Identity Management Base Module Administration Guide*.

# Privileged user accounts

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

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

## **To create privileged users through account definitions**

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.

3. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships in the manage level.
4. Create a formatting rule for the IT operating data.

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

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

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

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

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

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

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

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

- To use a prefix for the login name, in the Designer, set the **TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName\_Prefix** configuration parameter.
- To use a postfix for the login name, in the Designer, set the **TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName\_Postfix** configuration parameter.

These configuration parameters are evaluated in the default installation, if a user account is marked with the **Privileged user account** property (`IsPrivilegedAccount` column). The user account login names are renamed according to the formatting rules. This also occurs if the user accounts are labeled as privileged using the **Mark selected user accounts as privileged** schedule. If necessary, modify the schedule in the Designer.

## Related topics

- [Account definitions for Unix user accounts](#) on page 48

# Specifying deferred deletion for Unix user accounts

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

You have the following options for configuring deferred deletion.

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

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

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

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

## Example:

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

```
If Not $IsPrivilegedAccount:Bool$ Then
    Value = 10
End If
```

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

## Managing memberships in Unix groups

Unix user accounts can be grouped into Unix groups that can be used to regulate access to resources.

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

### Detailed information about this topic

- [Assigning Unix groups to Unix user accounts](#) on page 81
- [Effectiveness of membership in Unix user groups](#) on page 89
- [Unix group inheritance based on categories](#) on page 92
- [Overview of all assignments](#) on page 94

## Assigning Unix groups to Unix user accounts

Unix groups can be assigned directly or indirectly to Unix user accounts.

In the case of indirect assignment, identities and Unix groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. The Unix groups assigned to an identity are calculated from the position in the hierarchy and the direction of inheritance. If you add an identity to roles and that identity owns an Unix user account, the Unix user account is added to the Unix group.

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

You can use system roles to group Unix groups together and assign them to identities as a package. You can create system roles that contain only Unix groups. You can also group any number of company resources into a system role.

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

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	<i>One Identity Manager Identity Management Base Module Administration Guide</i> <i>One Identity Manager Business Roles Administration Guide</i>
Assigning company resources through IT Shop requests	<i>One Identity Manager IT Shop Administration Guide</i>
System roles	<i>One Identity Manager System Roles Administration Guide</i>

### Detailed information about this topic

- [Prerequisites for indirect assignment of Unix groups to Unix user accounts](#) on page 82
- [Assigning Unix groups to departments, cost centers and locations](#) on page 83
- [Assigning Unix groups to business roles](#) on page 85
- [Adding Unix groups to system roles](#) on page 86
- [Adding Unix groups to the IT Shop](#) on page 86
- [Assigning Unix user accounts directly to Unix groups](#) on page 88
- [Assigning Unix groups directly to Unix user accounts](#) on page 89

## Prerequisites for indirect assignment of Unix groups to Unix user accounts

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

1. Assignment of identities and Unix groups is permitted for role classes (departments, cost centers, locations, or business roles).

For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

### **To configure assignments to roles of a role class**

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
    - OR -
    - In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
  2. Select the **Configure role assignments** task and configure the permitted assignments.
    - To generally allow an assignment, enable the **Assignments allowed** column.
    - To allow direct assignment, enable the **Direct assignments permitted** column.
  3. Save the changes.
2. Settings for assigning Unix groups to Unix user accounts.
    - The Unix user account is linked to an identity.
    - The Unix user account is labeled with the **Groups can be inherited** option.

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

### **Related topics**

- [Creating and editing Unix user accounts](#) on page 115
- [General main data of Unix user accounts](#) on page 116

## **Assigning Unix groups to departments, cost centers and locations**

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

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

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.

4. In the **Add assignments** pane, assign the organizations:

- On the **Departments** tab, assign departments.
- On the **Locations** tab, assign locations.
- On the **Cost centers** tab, assign cost centers.

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

**To remove an assignment**

- Select the organization and double-click .

5. Save the changes.

**To assign groups to a department, a cost center, or a location (non role-based login or role-based login)**

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

- OR -

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

- OR -

In the Manager, select the **Organizations > Locations** category.

2. Select the department, cost center, or location in the result list.

3. Select the **Assign Unix groups** task.

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

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

**To remove an assignment**

- Select the group and double-click .

5. Save the changes.

## Related topics

- [Prerequisites for indirect assignment of Unix groups to Unix user accounts](#) on page 82
- [Assigning Unix groups to business roles](#) on page 85
- [Adding Unix groups to system roles](#) on page 86
- [Adding Unix groups to the IT Shop](#) on page 86
- [Assigning Unix user accounts directly to Unix groups](#) on page 88
- [Assigning Unix groups directly to Unix user accounts](#) on page 89
- [One Identity Manager users for managing Unix-based target systems](#) on page 9

# Assigning Unix groups to business roles

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

Assign the group to business roles so that the group is assigned to user accounts through these business roles.

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

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

### **To remove an assignment**

- Select the business role and double-click .
5. Save the changes.

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

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign Unix groups** task.
4. In the **Add assignments** pane, assign the groups.

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

### **To remove an assignment**

- Select the group and double-click .
5. Save the changes.

## **Related topics**

- [Prerequisites for indirect assignment of Unix groups to Unix user accounts](#) on page 82
- [Assigning Unix groups to departments, cost centers and locations](#) on page 83
- [Adding Unix groups to system roles](#) on page 86
- [Adding Unix groups to the IT Shop](#) on page 86
- [Assigning Unix user accounts directly to Unix groups](#) on page 88
- [Assigning Unix groups directly to Unix user accounts](#) on page 89
- [One Identity Manager users for managing Unix-based target systems](#) on page 9

# Adding Unix groups to system roles

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

Use this task to add a group to system roles.

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

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

## To assign a group to system roles

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

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

### To remove an assignment

- Select the system role and double-click .
5. Save the changes.

## Related topics

- [Prerequisites for indirect assignment of Unix groups to Unix user accounts](#) on page 82
- [Assigning Unix groups to departments, cost centers and locations](#) on page 83
- [Assigning Unix groups to business roles](#) on page 85
- [Adding Unix groups to the IT Shop](#) on page 86
- [Assigning Unix user accounts directly to Unix groups](#) on page 88
- [Assigning Unix groups directly to Unix user accounts](#) on page 89

# Adding Unix groups to the IT Shop

Once a group has been assigned to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- The group must be labeled with the **IT Shop** option.
- The group must be assigned to a service item.
- If you want the group to be assigned only to identities through the IT Shop, the group

must also be marked with the **Only use in IT Shop**. Direct assignment to hierarchical roles may not be possible.

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

### **To add a group to the IT Shop**

1. In the Manager, select the **Unix > Groups** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > Unix groups** (role-based login) category.
2. Select the group in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, add to the IT Shop shelves.
5. Save the changes.

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

### **Related topics**

- [Prerequisites for indirect assignment of Unix groups to Unix user accounts](#) on page 82
- [General main data for Unix groups](#) on page 129
- [Removing Unix groups from an IT Shop shelf](#) on page 87
- [Removing Unix groups from all IT Shop shelves](#) on page 88
- [One Identity Manager users for managing Unix-based target systems](#) on page 9

## **Removing Unix groups from an IT Shop shelf**

### **To remove a group from individual IT Shop shelves**

1. In the Manager, select the **Unix > Groups** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > Unix groups** (role-based login) category.
2. Select the group in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
5. Save the changes.

## Related topics

- [Removing Unix groups from all IT Shop shelves](#) on page 88

# Removing Unix groups from all IT Shop shelves

## *To remove a group from all IT Shop shelves*

1. In the Manager, select the **Unix > Groups** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > Unix groups** (role-based login) category.
2. Select the group in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

## Related topics

- [Removing Unix groups from an IT Shop shelf](#) on page 87

# Assigning Unix user accounts directly to Unix groups

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

## *To assign user accounts directly to a group*

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

### *To remove an assignment*

- Select the user account and double-click .
5. Save the changes.

## Related topics

- [Assigning Unix groups directly to Unix user accounts on page 89](#)
- [Assigning Unix groups to departments, cost centers and locations on page 83](#)
- [Assigning Unix groups to business roles on page 85](#)
- [Adding Unix groups to system roles on page 86](#)
- [Adding Unix groups to the IT Shop on page 86](#)

# Assigning Unix groups directly to Unix user accounts

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

## *To assign groups directly to user accounts*

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

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

### **To remove an assignment**

- Select the group and double-click .
5. Save the changes.

## Related topics

- [Assigning Unix groups to Unix user accounts on page 81](#)

# Effectiveness of membership in Unix user groups

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

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

**NOTE:**

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

The effectiveness of the assignments is mapped in the UNXAccountInUNXGroup and BaseTreeHasUNXGroup tables by the XIsInEffect column.

**Example: The effect of group memberships**

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

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

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

**Table 11: Specifying excluded groups (UNXGroupExclusion table)**

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

**Table 12: Effective assignments**

Identity	Member in role	Effective group
Pat Identity1	Marketing	Group A

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

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

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

**Table 13: Excluded groups and effective assignments**

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

## Prerequisites

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

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

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

- Mutually exclusive groups belong to the same host.

### To exclude a group

- In the Manager, select the **Unix > Groups** category.
- Select a group in the result list.
- Select the **Exclude groups** task.

4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.
  - OR -
  - In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.
5. Save the changes.

## Unix group inheritance based on categories

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

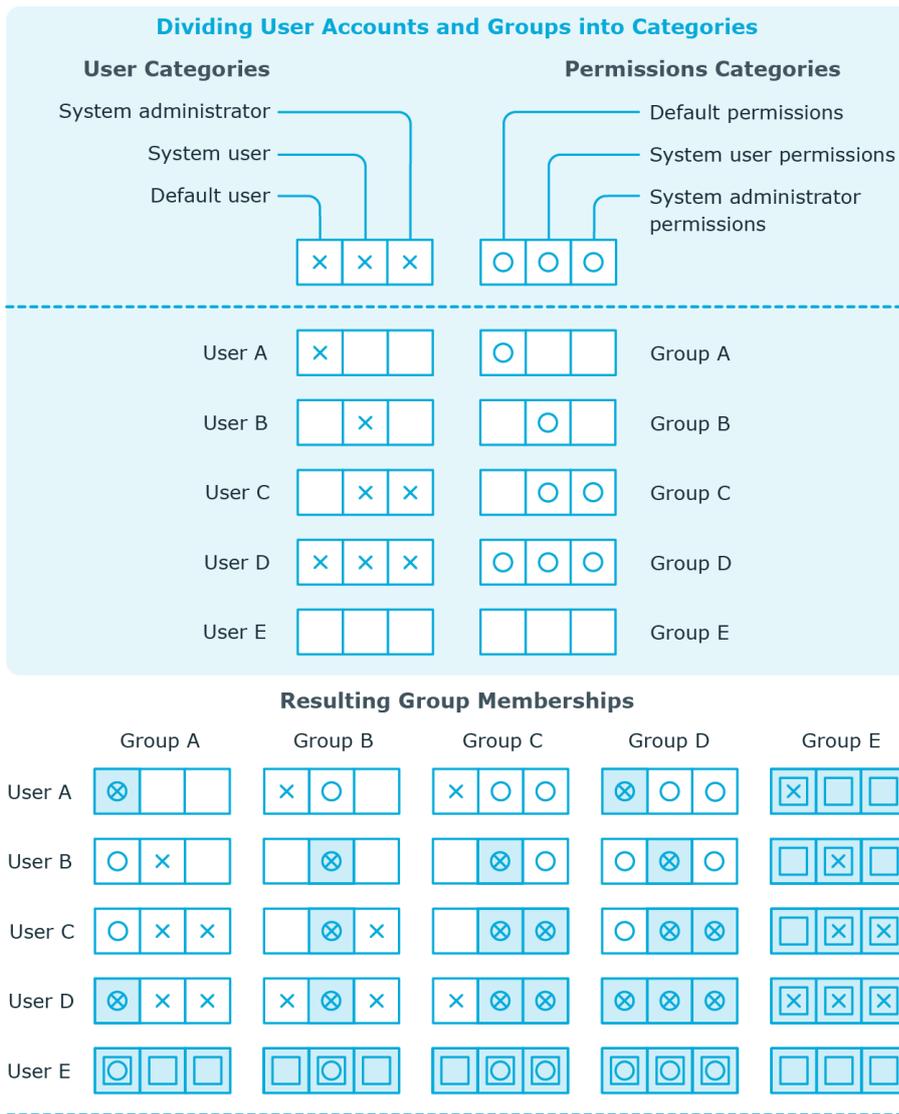
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or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

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

**Table 14: Category examples**

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	System user permissions
3	System administrator	System administrator permissions

**Figure 2: Example of inheriting through categories.**



**Key:**

<p>⊗ Inherits due to matching categories</p> <p>□ Inherits because user account and group are not categorized</p>	<p>⊙ Inherits because user account is not categorized</p> <p>⊗ Inherits because group is not categorized</p>
---	--

**To use inheritance through categories**

- In the Manager, define the categories in the Unix host.
- Assign categories to user accounts through their main data.
- Assign categories to groups through their main data.

## Related topics

- [Defining categories for the inheritance of entitlements](#) on page 112
- [General main data of Unix user accounts](#) on page 116
- [General main data for Unix groups](#) on page 129

# Overview of all assignments

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

### Example:

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

### *To display detailed information about assignments*

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

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

- Double-click a control to show all child roles belonging to the selected role.

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

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



**Table 15: Meaning of icons in the report toolbar**

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

## Login credentials for Unix user accounts

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

### Detailed information about this topic

- [Password policies for Unix user accounts](#) on page 96
- [Initial password for new Unix user accounts](#) on page 108
- [Email notifications about login data](#) on page 108

## Password policies for Unix user accounts

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

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

### Detailed information about this topic

- [Predefined password policies](#) on page 97
- [Using password policies](#) on page 98
- [Creating password policies](#) on page 99
- [Editing password policies](#) on page 100

- [Custom scripts for password requirements](#) on page 104
- [Password exclusion list](#) on page 107
- [Checking a password](#) on page 107
- [Testing password generation](#) on page 107

## Predefined password policies

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

### Password for logging in to One Identity Manager

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

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

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

### Password policy for forming identities' central passwords

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

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

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

### Password policies for user accounts

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

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

**NOTE:** When you update One Identity Manager version 7.x to One Identity Manager version 9.2, the configuration parameter settings for forming passwords are passed on to the target system-specific password policies.

The **UnixPassword policy** is predefined for Unix-based target systems. You can apply this password policy to Unix user accounts (UNXUser.Password) of a Unix host.

If the hosts' password requirements differ, it is recommended that you set up your own password policies for each host.

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

## Using password policies

The **UnixPassword policy** is predefined for Unix-based target systems. You can apply this password policy to Unix user accounts (UNXUser.Password) of a Unix host.

If the hosts' password requirements differ, it is recommended that you set up your own password policies for each host.

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

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's host.
4. The **One Identity Manager password policy** (default policy).

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

### *To reassign a password policy*

1. In the Manager, select the **Unix > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.
  - **Apply to:** Application scope of the password policy.

#### *To specify an application scope*

1. Click **→** next to the field.
2. Select one of the following references under **Table**:

- The table that contains the base objects of synchronization.
  - To apply the password policy based on the account definition, select the **TSBAccountDef** table.
  - To apply the password policy based on the manage level, select the **TSBBehavior** table.
3. Under **Apply to**, select the table that contains the base objects.
    - If you have selected the table containing the base objects of synchronization, next select the specific target system.
    - If you have selected the **TSBAccountDef** table, next select the specific account definition.
    - If you have selected the **TSBBehavior** table, next select the specific manage level.
  4. Click **OK**.
    - **Password column**: Name of the password column.
    - **Password policy**: Name of the password policy to use.
  5. Save the changes.

### ***To change a password policy's assignment***

1. In the Manager, select the **Unix > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

## **Creating password policies**

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

### ***To create a password policy***

1. In the Manager, select the **Unix > Basic configuration data > Password policies** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

## Detailed information about this topic

- [General main data for password policies](#) on page 100
- [Policy settings](#) on page 102
- [Character classes for passwords](#) on page 101
- [Custom scripts for password requirements](#) on page 104
- [Editing password policies](#) on page 100

# Editing password policies

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

### *To edit a password policy*

1. In the Manager, select the **Unix > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.

## Detailed information about this topic

- [General main data for password policies](#) on page 100
- [Policy settings](#) on page 102
- [Character classes for passwords](#) on page 101
- [Custom scripts for password requirements](#) on page 104
- [Creating password policies](#) on page 99

# General main data for password policies

Enter the following main data of a password policy.

**Table 16: main data for a password policy**

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.

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

## Character classes for passwords

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

**Table 17: Character classes for passwords**

Property	Meaning
Required number of character classes	<p>Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for <b>Min. number letters</b>, <b>Min. number lowercase</b>, <b>Min. number uppercase</b>, <b>Min. number digits</b>, and <b>Min. number special characters</b>.</p> <p>That means:</p> <ul style="list-style-type: none"> <li>• Value <b>0</b>: All character class rules must be fulfilled.</li> <li>• Value <b>&gt;0</b>: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value <b>&gt;0</b>.</li> </ul> <p><b>NOTE:</b> Generated passwords are not tested for this.</p>
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.

<b>Property</b>	<b>Meaning</b>
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

## Policy settings

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

**Table 18: Policy settings**

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

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

## Custom scripts for password requirements

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

### Detailed information about this topic

- [Checking passwords with a script](#) on page 104
- [Generating passwords with a script](#) on page 105

## Checking passwords with a script

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

### Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

#### Example: Script that checks a password

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

```

Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or
'!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in
password")#)
        End If
    End If
End Sub

```

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

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

### **Related topics**

- [Generating passwords with a script](#) on page 105

## **Generating passwords with a script**

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

## Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

### Example: Script that generates a password

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

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

```
    Dim pwd = spwd.ToInsecureArray()  
    ' replace invalid characters at first position  
    If pwd.Length>0  
        If pwd(0)="?" Or pwd(0)="!"  
            spwd.SetAt(0, CChar("_"))  
        End If  
    End If  
End Sub
```

### To use a custom script for generating a password

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

### Related topics

- [Checking passwords with a script](#) on page 104

# Password exclusion list

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

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

## *To add a term to the restricted list*

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

# Checking a password

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

## *To verify if a password conforms to the password policy*

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

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

# Testing password generation

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

## *To generate a password that conforms to the password policy*

1. In the Manager, select the **Unix > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.

3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.  
This generates and displays a password.

## Initial password for new Unix user accounts

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

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - In the Designer, set the **TargetSystem | Unix | Accounts | InitialRandomPassword** configuration parameter.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which identity will receive the initial password by email.

### Related topics

- [Password policies for Unix user accounts](#) on page 96
- [Email notifications about login data](#) on page 108

## Email notifications about login data

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

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

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
2. In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.

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

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

### ***To send initial login data by email***

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

By default, the message sent uses the mail template **Identity - new user account created**. The message contains the name of the user account.

4. In the Designer, set the **TargetSystem | Unix | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

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

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

## Mapping Unix objects in One Identity Manager

One Identity Manager maps the user accounts and groups of a Unix host. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

### Detailed information about this topic

- [Unix hosts](#) on page 110
- [Unix user accounts](#) on page 114
- [Unix groups](#) on page 128

## Unix hosts

The target system of synchronization with a Unix-based target system is the host. Hosts are added as the base objects of the synchronization in One Identity Manager. They are used to configure provisioning processes, automatic assignment of identities to user accounts, and to pass down Unix user groups to user accounts.

**NOTE:** One Identity Manager sets up the domains in the Synchronization Editor database. After initial synchronization of the hosts, you must enter the primary group, which will be used by default to set up the user accounts.

### *To edit the main data for a Unix host*

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

## Related topics

- [General main data of Unix hosts on page 111](#)
- [Defining categories for the inheritance of entitlements on page 112](#)
- [Editing the synchronization project for a Unix host on page 113](#)
- [Displaying the Unix hosts overview on page 113](#)
- [Displaying Unix login shells on page 114](#)
- [Synchronizing single objects on page 39](#)

# General main data of Unix hosts

Enter the following general main data.

**Table 19: General main data for a host**

Property	Description
Host name	Name of the host.
Primary group	User account's primary group. This group is used as primary group when creating a user account.
Time zone	Time zone of the host. The time zone is taken into account when determining the last login time for user accounts.
Device	The computer is connected to this device. Specify a new device using the  button next to the menu.
AIX system	Specifies whether this host is an IBM AIX system. The following properties are offered additionally for user accounts on IBM AIX systems.
Account definition (initial)	<p>Initial account definition for creating user accounts. This account definition is used if automatic assignment of identities to user accounts is used for this host and user accounts should be created that are already managed (<b>Linked configured</b> state). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the identity (<b>Linked</b>) if no account definition is given. This is the case on initial synchronization, for example.</p>
Target system managers	<p>Application role, in which target system managers are specified for the host. Target system managers only edit the objects from hosts that are assigned to them. Therefore, each host can have a different target system manager assigned to it.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this host. Use the  button to add a</p>

Property	Description									
	new application role.									
Synchronized by	Type of synchronization through which the data is synchronized between the host and One Identity Manager. As soon as objects for this host are available in One Identity Manager, the type of synchronization can no longer be changed.  If you create a host with the Synchronization Editor, <b>One Identity Manager</b> is used.									
<b>Table 20: Permitted values</b>										
	<table border="1"> <thead> <tr> <th>Value</th> <th>Synchronization by</th> <th>Provisioned by</th> </tr> </thead> <tbody> <tr> <td>One Identity Manager</td> <td>Unix connector</td> <td>Unix connector</td> </tr> <tr> <td>No synchronization</td> <td>none</td> <td>none</td> </tr> </tbody> </table>	Value	Synchronization by	Provisioned by	One Identity Manager	Unix connector	Unix connector	No synchronization	none	none
Value	Synchronization by	Provisioned by								
One Identity Manager	Unix connector	Unix connector								
No synchronization	none	none								
	<b>NOTE:</b> If you select <b>No synchronization</b> , you can define custom processes to exchange data between One Identity Manager and the target system.									
Operating system description	Description of the operating system.									
Distribution	Installed distribution of the operating system.									
Distribution version	Version of the installed distribution.									
Kernel version	Current version of the kernel.									
Operating system type	Type of operating system, such as Linux, AIX, or UNIX.									

## Defining categories for the inheritance of entitlements

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

### **To define a category**

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

### **Detailed information about this topic**

- [Unix group inheritance based on categories](#) on page 92

## **Editing the synchronization project for a Unix host**

Synchronization projects in which a host is already used as a base object can also be opened in the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

**NOTE:** The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

### **To open an existing synchronization project in the Synchronization Editor**

1. In the Manager, select the **Unix > Hosts** category.
2. Select the host in the result list. Select the **Change main data** task.
3. Select the **Edit synchronization project** task.

### **Related topics**

- [Customizing the synchronization configuration](#) on page 26

## **Displaying the Unix hosts overview**

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

### ***To obtain an overview of a host***

1. In the Manager, select the **Unix > Hosts** category.
2. Select the host in the result list.
3. Select **Unix host overview**.

## **Displaying Unix login shells**

This information about a host's login shells is loaded into One Identity Manager and cannot be edited. You can use login shells when setting up user accounts.

### ***To display login shells***

1. In the Manager, select the **Unix > Hosts > <host name> > Login shells** category.
2. Select the login shell in the result list.
3. Select the **Unix login shell overview** task.

### **Related topics**

- [Creating mapping rules for IT operating data](#) on page 55
- [General main data of Unix user accounts](#) on page 116

## **Unix user accounts**

You can use One Identity Manager to manage your local Unix-based target system user accounts. User accounts obtain the required access permissions to the resources through membership in groups.

### **Detailed information about this topic**

- [Managing Unix user accounts and identities](#) on page 47
- [Managing memberships in Unix groups](#) on page 81
- [Creating and editing Unix user accounts](#) on page 115
- [General main data of Unix user accounts](#) on page 116
- [User account main data for AIX systems](#) on page 120
- [Assigning extended properties to Unix user accounts](#) on page 125
- [Deleting and restoring Unix user accounts](#) on page 127
- [Disabling AIX system user accounts](#) on page 126

- [Displaying the Unix user account overview](#) on page 128
- [Synchronizing single objects](#) on page 39

## Creating and editing Unix user accounts

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

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

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

### ***To create a user account***

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

### ***To edit main data of a user account***

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

### ***To manually assign a user account for an identity***

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

### **Detailed information about this topic**

- [General main data of Unix user accounts](#) on page 116
- [User account main data for AIX systems](#) on page 120

## Related topics

- [Account definitions for Unix user accounts](#) on page 48
- [Supported user account types](#) on page 74
- [Managing Unix user accounts and identities](#) on page 47

# General main data of Unix user accounts

Enter the following general main data.

**Table 21: Additional main data of a user account**

Property	Description
Host	The user account's host.
Identity	<p>Identity that uses this user account.</p> <ul style="list-style-type: none"><li>• An identity is already entered if the user account was generated by an account definition.</li><li>• If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account.</li><li>• If you create the user account manually, you can select an identity in the menu.</li></ul> <p>The menu displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the <b>QER   Person   HideDeactivatedIdentities</b> configuration parameter.</p> <p><b>NOTE:</b> If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.</p> <p>You can create a new identity for a user account with an identity of type <b>Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity</b>. To do this, click  next to the input field and enter the required identity main data. Which login data is required depends on the selected identity type.</p>
No link to an identity required	<p>Specifies whether the user account is intentionally not assigned an identity. The option is automatically set if a user account is included in the exclusion list for automatic identity assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an identity (for example, if several identities use the user account).</p> <p>If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an identity can be filtered according to</p>

Property	Description
	various criteria.
Not linked to an identity	<p>Indicates why the <b>No link to an identity required</b> option is enabled for this user account. Possible values:</p> <ul style="list-style-type: none"> <li>• <b>By administrator:</b> The option was set manually by the administrator.</li> <li>• <b>By attestation:</b> The user account was attested.</li> <li>• <b>By exclusion criterion:</b> The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter <b>PersonExcludeList</b>).</li> </ul>
Account definition	<p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned identity and enters it in the corresponding fields in the user account.</p> <p><b>NOTE:</b> The account definition cannot be changed once the user account has been saved.</p> <p><b>NOTE:</b> Use the user account's <b>Remove account definition</b> task to reset the user account to <b>Linked</b> status. This removes the account definition from both the user account and the identity. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (X0origin=1).</p>
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Login shell	Shell that is run if a user logs in to Unix using a terminal-based login.
User name	Name of the user account for logging in to a Unix host. If an account definition is assigned, this field is automatically filled with the identity's central user account depending on the manage level.
User ID	User ID for the user account in the Unix host.
Last login	Time of the last log in. The time is calculated taking the host time zone and the target system specific string for the login ( <b>Last login (Unix value)</b> ) into account.
Last login (Unix value)	Character string specified in the target system for logging in that is converted depending on the system in the value of the <b>Last login</b> property.

Property	Description
Password	<p>Password for the user account. The identity's central password can be mapped to the user account password. For more information about an identity's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created.</p> <p>The password is deleted from the database after publishing to the target system.</p> <p><b>NOTE:</b> 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.</p>
Password confirmation	Reconfirm password.
Password last changed	Date of last password change. The date is read in from the Unix system and cannot be changed.
Primary group ID	Identifier of the user account's primary group.
Primary group	<p>Name of the user account's primary group. This defines the group ownership of files created by the user.</p> <p>A user account's primary group is determined as follows:</p> <ul style="list-style-type: none"> <li>• If you entered a primary group in the host, the group is used as primary group when a user account is created.</li> <li>• If you did not enter a primary group, a new group is created with the display name of the new user account assigned as the primary group.</li> </ul>
Home directory	The user's full home directory path. For example, /home/user001.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
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.
Comment (GECOS)	Text field for additional explanation. Additional information about the user account, which is found in the GECOS in /etc/passwd. If an account definition is assigned, this field is automatically filled with the

Property	Description
	identity's internal name depending on the manage level.
Identity type	<p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> <li>• <b>Primary identity:</b> Identity's default user account.</li> <li>• <b>Organizational identity:</b> Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</li> <li>• <b>Personalized administrator identity:</b> User account with administrative permissions, used by one identity.</li> <li>• <b>Sponsored identity:</b> User account to use for a specific purpose. Training, for example.</li> <li>• <b>Shared identity:</b> User account with administrative permissions, used by several identities. Assign all identities that use this user account.</li> <li>• <b>Service identity:</b> Service account.</li> </ul>
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> <li>• If you add an identity with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.</li> <li>• If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.</li> </ul>
Privileged user account	Specifies whether this is a privileged user account.

## Related topics

- [Account definitions for Unix user accounts on page 48](#)
- [Assigning identities automatically to Unix user accounts on page 69](#)
- [Password policies for Unix user accounts on page 96](#)
- [Initial password for new Unix user accounts on page 108](#)
- [Unix group inheritance based on categories on page 92](#)
- [Supported user account types on page 74](#)
- [General main data of Unix hosts on page 111](#)
- [Disabling AIX system user accounts on page 126](#)
- [Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 82](#)

# User account main data for AIX systems

You can enter additional main data of user accounts in an IBM AIX system, like limits, password data, security data or information about encrypting the file system. This data is shown if the host is labeled with the **AIX system** option.

## Detailed information about this topic

- [Limits for user accounts](#) on page 120
- [Password data for user accounts](#) on page 121
- [Security-related main data for user accounts](#) on page 122
- [Main data for user accounts on an encrypted file system](#) on page 124
- [General main data of Unix hosts](#) on page 111

## Limits for user accounts

Enter the following limits for resources of the user's processes in an AIX system. This data is mapped in `/etc/security/limits`.

**Table 22: Limits for user accounts in an AIX system**

Property	Description
Core size (soft)	Soft limit for the size of the core dump file that can be created by a user process. (Parameter <code>core</code> ).
Core size (hard)	Absolute maximum limit for the size of the core dump file that can be created by a user process. (Parameter <code>core_hard</code> ).
CPU time (soft)	Soft limit for the time (in seconds) a user process may take. (Parameter <code>cpu</code> ).
CPU time (hard)	Maximum amount of time (in seconds) the user process may take. (Parameter <code>cpu_hard</code> ).
Data size (soft)	Soft limit for the size of the process' data segment for a user process. (Parameter <code>data</code> ).
Data size (hard)	Maximum size of a process' data segment for a user process. (Parameter <code>data_hard</code> ).
File size (soft)	Soft limit for the size of a file a user process can create or extend. (Parameter <code>fsize</code> ).
File size (hard)	Absolute maximum size of a file a user process can create or extend. (Parameter <code>fsize_hard</code> ).
Memory size	Soft limit for the maximum amount of physical memory a user process can

Property	Description
(soft)	take up. (Parameter <code>rss</code> ).
Memory size (hard)	Maximum amount of physical memory a user process can take up. (Parameter <code>rss_hard</code> ).
Stack size (soft)	Soft limit for the size of the process' stack segment for a user process. (Parameter <code>stack</code> ).
Stack size (hard)	Maximum size of a process' stack segment for a user process. (Parameter <code>stack_hard</code> ).
File descriptors (soft)	Soft limit for the number of file descriptors a user process can have open at the same time. (Parameter <code>nfiles</code> ).
File descriptors (hard)	Absolute maximum number of file descriptors a user process can have open at the same time. (Parameter <code>nfiles_hard</code> ).
Threads (soft)	Soft limit for the number of threads per process. (Parameter <code>threads</code> ).
Threads (hard)	Absolute maximum number of threads per process. (Parameter <code>threads_hard</code> ).
Processes (soft)	Soft limit for the number of processes per user. (Parameter <code>nproc</code> ).
Processes (hard)	Absolute maximum for the number of processes per user. (Parameter <code>nproc_hard</code> ).

## Password data for user accounts

Enter the following additional information for the password of a user account in an AIX system. This data is mapped in `/etc/security/user`.

**Table 23: Password data for user accounts in an AIX system**

Property	Description
<code>minlen</code>	Minimum number of characters a password must have. (Parameter <code>minlen</code> ).
<code>maxrepeats</code>	Maximum number of characters that can be repeated in passwords. The default value 8 specifies that a maximum has not been fixed. (Parameter <code>maxrepeats</code> ).
<code>mindiff</code>	Minimum number of unique characters that passwords must contain. (Parameter <code>mindiff</code> ).

Property	Description
minalpha	Specifies the minimum number of alphabetical characters the password must contain. (Parameter minalpha).
minloweralpha	Specifies the minimum number of lowercase letters the password must contain. (Parameter minloweralpha).
minupperalpha	Specifies the minimum number of uppercase letters the password must contain. (Parameter minupperalpha).
mindigit	Specifies the minimum number of digits the password must contain. (Parameter mindigit).
minspecialchar	Specifies the minimum number of special characters the password must contain. (Parameter minspecialchar).
minother	Specifies the minimum number of non-alphabetical characters a new password must contain. (Parameter minother).
dictionlist	Dictionary file of passwords that are not allowed. (Parameter dictionlist).
histexpire	Number of weeks before a password can be reused. (Parameter histexpire).
histsize	Number of password iterations allowed before an old password can be used again. (Parameter histsize).
minage	Minimum number of weeks before a password can be changed. (Parameter minage).
maxage	Maximum number of weeks before a password must be changed. (Parameter maxage).
maxexpired	Maximum number of weeks beyond maxage that an expired password can be changed by the user. (Parameter maxexpired).
pwdchecks	Methods to apply to new passwords that check the password quality. The value contains a comma delimited list of method names. (Parameter pwdchecks).
pwdwarntime	Number of days before the system issues a warning that a password change is required. (Parameter pwdwarntime).

## Security-related main data for user accounts

Enter the following additional security-related information for a user account in an AIX system. This data is mapped in `/etc/security/user`.

**Table 24: Additional security-related data for user accounts in an AIX system**

<b>Property</b>	<b>Description</b>
account_locked	Specifies whether the user account is locked. (Parameter account_locked).
admin	Specifies the administrative status of the user. (Parameter admin).
admgroups	Lists the groups the user administrates. (Parameter admgroups).
auditclasses	The user account's audit classes. (Parameter auditclasses).
auth1	Additional mandatory methods for authenticating the user. (Parameter auth1).
auth2	Additional optional methods for authenticating the user. (Parameter auth2).
core_compress	Enables or disables core file compression. (Parameter core_compress).
core_path	Enables or disables core file path specification. (Parameter core_path). If this attribute has a value of On, core files will be placed in the given directory. otherwise, core files are placed in the user's current working directory.
core_naming	Naming conventions for the core file. If this option is set, the core file is stamped with a process ID, time, and date. (Parameter core_naming).
daemon	Specifies whether the user can run programs using the cron daemon or the src (system resource controller) daemon. (Parameter daemon).
dce_export	Specifies whether the DCE registry can overwrite the local user information with the DCE user information during a DCE export operation. (Parameter dce_export).
expires	Expiration date of the user account. (Parameter expires).
login	Specifies whether the user can log in to the system with the login command. (Parameter login).
logintimes	Times, days, or both, the user is allowed to access the system. (Parameter logintimes).
loginretries	Number of unsuccessful login attempts allowed after the last successful login before the system locks the account. (Parameter loginretries). A value of 0 or a negative value, indicates no maximum age.
projects	List of projects that the user's processes can be assigned to. The value is a list of comma-delimited project names. (Parameter projects).
registry	Defines the authentication registry where the user is administered. (Parameter registry).

Property	Description
rlogin	Specifies whether access is permitted to the account from a remote location with the telnet or rlogin commands. (Parameter rlogin).
su	Specifies whether another user can switch to the specified user account with the su command. (Parameter su).
sugroups	Groups that can use the su command to switch to the specified user. (Parameter sugroups).
SYSTEM	System's authentication mechanism for the user. (Parameter SYSTEM).
tpath	The user's trusted path status. (Parameter tpath).
ttys	Lists the terminals that can access the user. (Parameter ttys).
umask	Determines file permissions. (Parameter umask). The default value is 022.

## Related topics

- [Disabling AIX system user accounts](#) on page 126

## Main data for user accounts on an encrypted file system

Enter the following additional information for using the encrypted file system (EFS) for a user account in an AIX system. This data is mapped in /etc/security/user.

**Table 25: User account main data of encrypted file systems**

Property	Description
efs_adminks_access	Defines the efs_admin keystore location (Parameter efs_adminks_access). Permitted values: <ul style="list-style-type: none"> <li>• file</li> <li>• ldap</li> </ul>
efs_allowksmodechangebyuser	Specifies whether the user can change the mode or not. (Parameter efs_allowksmodechangebyuser).
efs_file_algo	Algorithm used to generate the file protection key. (Parameter efs_file_algo). Permitted values: <ul style="list-style-type: none"> <li>• AES_128_CBC</li> <li>• AES_192_CBC</li> <li>• AES_256_CBC</li> </ul>
efs_initialks_mode	Initial mode of the user keystore. (Parameter efs_

Property	Description
	initialks_mode). Permitted values: <ul style="list-style-type: none"> <li>guard</li> <li>admin</li> </ul>
efs_keystore_access	User keystore location. (Parameter efs_keystore_access). Permitted values: <ul style="list-style-type: none"> <li>none</li> <li>file</li> </ul>
efs_keystore_algo	Algorithm used to generate the user private key when the keystore is created. (Parameter efs_keystore_algo). Permitted values: <ul style="list-style-type: none"> <li>RSA_1024</li> <li>RSA_2048</li> <li>RSA_4096</li> </ul>

## Assigning extended properties to Unix user accounts

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

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

### To specify extended properties for a user account

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

#### To remove an assignment

- Select the extended property and double-click .
5. Save the changes.

# Disabling AIX system user accounts

**NOTE:** The behavior described in the following, only applies to user accounts in an AIX system.

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

## **Scenario: The user accounts are linked to identities and are managed through account definitions.**

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

## **Scenario: The user accounts are linked to identities. No account definition is applied.**

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

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

### ***To disable the user account when the configuration parameter is disabled***

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **Security** tab, set the **account\_locked** option.
5. Save the changes.

## **Scenario: The user accounts are not linked to identities.**

### ***To disable a user account that is no longer linked to an identity***

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **Security** tab, set the **account\_locked** option.
5. Save the changes.

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

## Related topics

- [Account definitions for Unix user accounts](#) on page 48
- [Creating manage levels](#) on page 53
- [Deleting and restoring Unix user accounts](#) on page 127

# Deleting and restoring Unix user accounts

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

In the Manager, you can delete a user account that was not created using an account definition in the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

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

### **To delete a user account that is not managed using an account definition**

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

### **To restore a user account**

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

## Related topics

- [Disabling AIX system user accounts](#) on page 126
- [Specifying deferred deletion for Unix user accounts](#) on page 80

# Displaying the Unix user account overview

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

## **To obtain an overview of a user account**

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select the **Unix user account overview** task.

## Unix groups

In the Unix host, user accounts can be gathered into groups that can be used to regulate access to resources. Local groups are loaded into One Identity Manager by synchronization. You can set up new groups or edit existing groups.

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

### **Detailed information about this topic**

- [Managing memberships in Unix groups](#) on page 81
- [Creating and editing Unix groups](#) on page 128
- [General main data for Unix groups](#) on page 129
- [Adding Unix groups to Unix groups](#) on page 130
- [Assigning extended properties to Unix groups](#) on page 131
- [Displaying the Unix group overview](#) on page 131
- [Synchronizing single objects](#) on page 39

## Creating and editing Unix groups

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

### **To create a group**

1. In the Manager, select the **Unix > Groups** category.
2. Click  in the result list.

3. On the main data form, edit the main data of the group.
4. Save the changes.

### To edit group main data

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

### Detailed information about this topic

- [General main data for Unix groups](#) on page 129

## General main data for Unix groups

Enter the following general main data.

**Table 26: General main data**

Property	Description
Group name	Name of the group.
Group ID	Group's identifier.
Host	Group's host.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range <b>0</b> to <b>1</b> . This input field is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is activated.  For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .

Property	Description
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.

## Related topics

- [Unix group inheritance based on categories](#) on page 92
- For more information about preparing groups for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

# Adding Unix groups to Unix groups

Use this task to add a group to another group. This means that the groups can be hierarchically structured.

## ***To assign groups directly to a group as members***

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** category.
4. Select the **Has members** tab.
5. Assign child groups in **Add assignments**.

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

### ***To remove an assignment***

- Select the group and double-click .
6. Save the changes.

## ***To add a group as a member of other groups***

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** task.
4. Select the **Is member of** tab.
5. In the **Add assignments** pane, assign parent groups.

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

### **To remove an assignment**

- Select the group and double-click .
6. Save the changes.

## Assigning extended properties to Unix groups

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

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

### **To specify extended properties for a group**

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

### **To remove an assignment**

- Select the extended property and double-click .
5. Save the changes.

## Deleting Unix groups

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

### **To delete a group**

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

## Displaying the Unix group overview

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

### To obtain an overview of a group

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Unix group overview** task.

## Reports about Unix objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for Unix-based target systems.

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

**Table 27: Data quality target system report**

<b>Report</b>	<b>Published for</b>	<b>Description</b>
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history.  Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	group	This report finds all roles containing identities who have the selected system entitlement.
Show overview	group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	group	This report shows an overview of the system entitlement and including its history.  Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.

Report	Published for	Description
Show entitlement drifts	Host	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Host	This report returns all the user accounts with their permissions including a history.  Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average number of system entitlements	Host	This report contains all user accounts with an above average number of system entitlements.
Show identities with multiple user accounts	Host	This report shows all the identities that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Host	This report shows the system entitlements with the assigned user accounts including a history.  Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Host	This report finds all roles containing identities with at least one user account in the selected target system.
Show unused user accounts	Host	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Host	This report shows all user accounts to which no identity is assigned.

**Table 28: Additional reports for the target system**

Report	Description
Unix user account and group administration	This report contains a summary of user account and group distribution in all host systems. You can find this report in the <b>My One Identity Manager</b> category.
Data quality summary for Unix user accounts	This report contains different evaluations of user account data quality in all host systems. You can find this report in the <b>My One Identity Manager</b> category.

## Handling of Unix objects in the Web Portal

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

- Managing user accounts and identities

An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized identity, such as a manager.

- Managing group assignments

When a group is assigned to an IT Shop shelf, the group can be requested by the customers of the shop in the Web Portal. The request undergoes a defined approval process. The group is not assigned until it has been approved by an authorized identity.

In the Web Portal, managers and administrators of organizations can assign groups to the departments, cost centers, or locations for which they are responsible. The groups are passed on to all persons who are members of these departments, cost centers, or locations.

If the Business Roles Module is available, managers, and administrators of business roles can assign groups in the Web Portal to the business roles for which they are responsible. The groups are passed on to all persons who are members of these business roles.

If the System Roles Module is available, supervisors of system roles can assign groups to the system roles in the Web Portal. The groups are passed on to all persons to whom these system roles are assigned.

- Attestation

If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

If the Compliance Rules Module is available, you can define rules that identify the invalid group memberships and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check rule violations and to grant exception approvals.

If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

You can use the risk index of groups to evaluate the risk of entitlement assignments for the company. One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

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

For more information about the named topics, see [Managing Unix user accounts and identities](#) on page 47, [Managing memberships in Unix groups](#) on page 81, and the following guides:

- *One Identity Manager Web Designer Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

## Basic data for Unix-based target systems

The following base data is relevant for managing a Unix-based target system in One Identity Manager.

- Account definitions

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

For more information, see [Account definitions for Unix user accounts](#) on page 48.

- Password policy

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

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

For more information, see [Password policies for Unix user accounts](#) on page 96.

- Initial password for new user accounts

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

For more information, see [Initial password for new Unix user accounts](#) on page 108.

- 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 108.

- Target system types

Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

For more information, see [Post-processing outstanding objects](#) on page 40.

- Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all Unix hosts in One Identity Manager.

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

For more information, see [Target system managers for Unix-based systems](#) on page 137.

- Servers

Servers must be informed of your server functionality in order to handle Unix-specific processes in One Identity Manager. For example, the synchronization server.

For more information, see [Job server for Unix-specific process handling](#) on page 139.

## Target system managers for Unix-based systems

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all Unix hosts in One Identity Manager.

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

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

### Implementing application roles for target system managers

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

Target system managers with the default application role are authorized to edit all the Unix hosts in One Identity Manager.

3. Target system managers can authorize other identities within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual Unix hosts.

**Table 29: Default application roles for target system managers**

User	Tasks
Target system managers	<p>Target system managers must be assigned to the <b>Target systems   Unix</b> application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assume administrative tasks for the target system.</li> <li>• Create, change, or delete target system objects.</li> <li>• Edit password policies for the target system.</li> <li>• Prepare groups to add to the IT Shop.</li> <li>• Can add identities that do not have the <b>Primary identity</b> identity type.</li> <li>• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.</li> <li>• Edit the synchronization's target system types and outstanding objects.</li> <li>• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.</li> </ul>

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

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

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

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

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

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

### ***To specify target system managers for individual hosts***

1. Log in to the Manager as a target system manager.
2. Select the **Unix > Hosts** category.
3. Select the host in the result list.
4. Select the **Change main data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

- OR -

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

- a. Enter the application role name and assign the **Target systems | Unix** parent application role.
  - b. Click **OK** to add the new application role.
6. Save the changes.
  7. Assign identities to this application role who are permitted to edit the host in One Identity Manager.

### **Related topics**

- [One Identity Manager users for managing Unix-based target systems](#) on page 9
- [General main data of Unix hosts](#) on page 111

## **Job server for Unix-specific process handling**

Servers must be informed of your server functionality in order to handle Unix-specific processes in One Identity Manager. For example, the synchronization server.

You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the

*One Identity Manager Configuration Guide.*

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

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

**NOTE:** One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

### **To edit a Job server and its functions**

1. In the Manager, select the **Unix > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.
4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

### **Detailed information about this topic**

- [General main data for a Job server](#) on page 140
- [Server functions of a Job server](#) on page 143

## **General main data for a Job server**

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

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

**Table 30: Job server properties**

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

Property	Meaning
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. <b>NOTE:</b> The <b>Server is cluster</b> and <b>Server belongs to cluster</b> properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported.  If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled.  This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values <b>Win32</b> , <b>Windows</b> , <b>Linux</b> , and <b>Unix</b> are

Property	Meaning
	permitted. If no value is specified, <b>Win32</b> is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.  The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks.  You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> .
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed.  For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i> .
No automatic software update	Specifies whether to exclude the server from automatic software updating.  <b>NOTE:</b> Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.

Property	Meaning
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

## Related topics

- [Server functions of a Job server](#) on page 143

# Server functions of a Job server

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

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

**Table 31: Permitted server functions**

Server function	Remark
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks.  The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.

Server function	Remark
	Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the ScriptComponent process component.
Generic database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for synchronizing an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.
Unix connector	This server can connect to a Unix system using SSH.
AIX connector	This server can connect to an AIX system using SSH.

## Related topics

- [General main data for a Job server](#) on page 140

## Configuration parameters for managing Unix-based target systems

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

**Table 32: Configuration parameters**

Configuration parameter	Description
TargetSystem   Unix	<p>Preprocessor relevant configuration parameter to control component parts for Unix-based custom target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p>
TargetSystem   Unix   Accounts	Allows configuration of user account data.
TargetSystem   Unix   Accounts   InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem   Unix   Accounts   InitialRandomPassword   SendTo	Identity to receive an email with the random generated password (manager cost center/department/location/role, identity's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the <b>TargetSystem   Unix   DefaultAddress</b> configuration parameter.

Configuration parameter	Description
TargetSystem   Unix   Accounts   InitialRandomPassword   SendTo   MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The <b>Identity - new user account created</b> mail template is used.
TargetSystem   Unix   Accounts   InitialRandomPassword   SendTo   MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The <b>Identity - initial password for new user account</b> mail template is used.
TargetSystem   Unix   Accounts   MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The <b>Identity - new user account with default properties created</b> mail template is used.
TargetSystem   Unix   Accounts   PrivilegedAccount	Allows configuration of privileged Unix user account settings.
TargetSystem   Unix   Accounts   PrivilegedAccount   AccountName_Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem   Unix   Accounts   PrivilegedAccount   AccountName_Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem   Unix   DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem   Unix   MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem   Unix   PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem   Unix   PersonAutoDisabledAccounts	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem   Unix   PersonAutoFullSync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.

Configuration parameter	Description
TargetSystem   Unix   PersonExcludeList	<p>Listing of all user account without automatic identity assignment. Names are listed in a pipe ( ) delimited list that is handled as a regular search pattern.</p> <p>Example:</p> <pre>ADMINISTRATOR GUEST KRBTGT TSINTERNETUSER IUSR_.* IWAM_.*  SUPPORT_.* . *   \$</pre>

## Default project template for Unix-based target systems

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

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

The project template uses mappings for the following schema types.

**Table 33: Mapping Unix schema types to tables in the One Identity Manager schema**

<b>Schema type in Unix-based target system</b>	<b>Table in the One Identity Manager Schema</b>
Group	UNXGroup
Host	UNXHost
LoginShell	UNXLoginShell
User	UNXAccount

## Unix connector settings

The following settings are configured for the system connection with the Unix connector.

**Table 34: Unix connector settings**

Setting	Description
Server or IP	Server name or IP address of the host. Variable: CP_Host
Host name	Name of the host. Variable: Hostname
Port	Communications port for establishing the SSH connection. The default communications port is the TCP port <b>22</b> . Variable: CP_Port
User account	When the authentication method is <b>Password</b> . User account for SSH login in the host. Variable: CP_SSHUser
Password	When the authentication method is <b>Password</b> . Password for SSH login on the host. Variable: CP_SSHPassword
Private key	When the authentication method is <b>Private key</b> . Private key for logging in to the host. Variable: CP_PrivateKey
Passphrase	When the authentication method is <b>Private key</b> . Passphrase for logging in to the host. Variable: CP_PrivateKeyPassphrase
Change to administrative context	Method to use to gain administrative permissions. Permitted values are: <ul style="list-style-type: none"><li>• <b>Default</b>: If the user already possesses administrative permissions, select the <b>Default</b> method.</li></ul>

Setting	Description
	<ul style="list-style-type: none"> <li>• <b>Sudo</b>: If the current user logged in on the host can run administrative tasks as an administrative user, select the <b>Sudo</b> method. Enter the alternative user, such as <b>root</b>.</li> <li>• <b>Su</b>: If administrative tasks should be run using a different user, select the <b>su</b> method. Enter the user's login credentials. The default user is <b>root</b>.</li> </ul> <p>Variable: CP_EvaluationMethod</p>
User name	<p>User name if the <b>Sudo</b> or <b>Su</b> methods are used.</p> <p>Variable: CP_EvaluationUser</p> <p>Default: <b>root</b></p>
Password	<p>Password for the user if the <b>Su</b> method is used.</p> <p>Variable: CP_EvaluationPassword</p>

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

## Contacting us

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

## Technical support resources

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

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

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## A

- account definition 48
  - add to IT Shop 64
  - assign automatically 61
  - assign to all identities 61
  - assign to business role 61
  - assign to cost center 60
  - assign to department 60
  - assign to identities 59, 62
  - assign to location 60
  - assign to system roles 63
  - assign to Unix host 66
  - create 49
  - delete 66
  - edit 49
  - IT operating data 55, 57
  - manage level 52-53
- architecture overview 8

## B

- base object 29, 33

## C

- calculation schedule 36
  - deactivate 37
- configuration parameter 145
- convert connection parameter 29

## D

- direction of synchronization
  - direction target system 22, 27
  - in the Manager 22

## E

- email notification 108
- exclusion definition 89

## I

- identity 74
- identity assignment
  - automatic 69
  - manual 72
  - remove 72
  - search criteria 71
    - table column 71
- IT operating data
  - change 58
- IT Shop shelf
  - assign account definition 64

## J

- Job server
  - edit 15
  - load balancing 34

## L

load balancing 34  
login data 108

## M

membership  
    modify provisioning 32

## N

notification 108

## O

object  
    delete immediately 40  
    outstanding 40  
    publish 40  
offline mode 44  
One Identity Manager  
    administrator 9  
    target system administrator 9  
    target system manager 9, 137  
    user 9  
outstanding object 40

## P

password  
    initial 108  
password policy 96  
    assign 98  
    character sets 101  
    check password 107  
    conversion script 104-105

    default policy 98, 100  
    display name 100  
    edit 99-100  
    error message 100  
    excluded list 107  
    failed logins 102  
    generate password 107  
    initial password 102  
    name components 102  
    password age 102  
    password cycle 102  
    password length 102  
    password strength 102  
    predefined 97  
    test script 104  
project template 148  
provisioning  
    accelerate 34  
    members list 32

## S

schema  
    changes 31  
    shrink 31  
    update 31  
single object synchronization 33, 39  
    accelerate 34  
start up configuration 29  
synchronization  
    authorizations 13  
    base object  
        create 28  
    calculation schedule 36  
    configure 22, 26  
    connection parameter 22, 26, 28

- different hosts 28
- extended schema 28
- prevent 37
- scope 26
- set up 12
- start 22, 36
- synchronization project
  - create 19, 22
- target system schema 28
- user 13
- variable 26
- variable set 28
- workflow 22, 27
- synchronization configuration
  - customize 26-28
- synchronization log 38
  - contents 25
  - create 25
- synchronization project
  - create 19, 22
  - deactivate 37
  - edit 113
  - project template 148
- synchronization server
  - configure 15
  - install 15
  - Job server 15
- synchronization workflow
  - create 22, 27
- synchronize single object 39
- system connection
  - change 29
  - enabled variable set 30

## T

- target system
  - not available 44
- target system synchronization 40
- template
  - IT operating data, modify 58

## U

- Unix group
  - add to IT Shop 86
  - add to system role 86
  - assign extended properties 131
  - assign group 130
  - assign to business role 85
  - assign to cost center 83
  - assign to department 83
  - assign to location 83
  - assign user account 81, 88-89
  - category 92, 129
  - delete 131
  - edit 128
  - effective 89
  - exclusion 89
  - group ID 129
  - host 129
  - primary group 111, 116
  - remove from IT Shop 87-88
  - risk index 129
  - service item 129
- Unix host 113
  - account definition 111
  - account definition (initial) 66
  - AIX system 111

- application roles 9
- category 92, 112
- identity assignment 71
- overview of all assignments 94
- primary group 111
- report 132
- set up 110
- synchronization 111
- target system manager 9, 111, 137

Unix login shell 114

Unix user account

- account definition 66, 116
- administrative user account 76
- assign extended properties 125
- assign group 88-89
- assign identity 47, 69, 115-116
- category 92, 116
- comment (Gecos) 116
- default user accounts 75
- deferred deletion 80
- delete 127
- disable (AIX system) 126
- EFS (AIX system) 124
- encrypted file system (AIX system) 124
- group ID 116
- groups can be inherited 55
- home directory 116
- host 116
- identity 55, 116
- inherit group 116
- limits (AIX system) 120
- lock 127
- login shell 55, 116
- manage level 73, 116
- password 116
  - initial 108
- password data (AIX system) 121
- primary group 111, 116
- privileged user account 55, 78, 116
- restore 127
- risk index 116
- security (AIX system) 122
- set up 115
- user account UID 116
- user name 116

user account

- administrative user account 76-77
- apply template 58
- default user accounts 75
- identity 74
- password
  - notification 108
- privileged user account 74, 78
- type 74

**V**

- variable set 29
  - active 30