



One Identity Manager 8.1.5

Administration Guide for Connecting Unix-Based Target Systems

Copyright 2021 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

 **WARNING:** A WARNING icon 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.

Contents

Managing Unix-based systems	7
Architecture overview	7
One Identity Manager users for managing Unix-based target systems	8
Setting up synchronization with a Unix-based target system	11
Users and permissions for synchronizing with a Unix-based target system	12
Configuring Unix the host	13
Setting up the synchronization server	13
Creating a synchronization project for initial synchronization of a Unix host	16
Information required for setting up a synchronization project	17
Setting up an initial synchronization project	19
Displaying synchronization results	23
Configuring the retention period for logs	24
Customizing the synchronization configuration	24
Configuring Unix host synchronization	25
Configuring synchronization of several Unix hosts	26
Updating schemas	26
Post-processing outstanding objects	27
Configuring the provisioning of memberships	30
Accelerating provisioning and single object synchronization	31
Help for the analysis of synchronization issues	32
Disabling synchronization	32
Basic data for Unix-based target systems	34
Setting up account definitions	35
Creating an account definition	36
Master data for an account definition	36
Creating manage levels	38
Creating a formatting rule for IT operating data	41
Collecting IT operating data	43
Modify IT operating data	44
Assigning account definitions to employees	45
Assigning account definitions to departments, cost centers, and locations	46

Assigning an account definition to business roles	47
Assigning account definitions to all employees	48
Assigning account definitions directly to employees	48
Assigning account definitions to system roles	49
Adding account definitions to the IT Shop	50
Assigning account definitions to a target system	51
Deleting an account definition	52
Password policies for Unix user accounts	54
Predefined password policies	54
Using password policies	56
Editing password policies	58
General master data for password policies	58
Policy settings	59
Character classes for passwords	60
Custom scripts for password requirements	61
Script for checking passwords	61
Script for generating a password	62
Password exclusion list	64
Checking a password	64
Testing password generation	64
Initial password for new Unix user accounts	65
Email notifications about login data	65
Target system managers	66
Editing a server	69
Master data for a Job server	69
Server functions of a Job server	72
Unix host	74
General master data for Unix hosts	74
Specifying categories for inheriting permissions	76
How to edit a synchronization project	76
Displaying the Unix host overview	77
Displaying Unix login shells	77
Unix user accounts	78
Linking user accounts to employees	78

Supported user account types	79
Default user accounts	81
Administrative user accounts	82
Providing administrative user accounts for one employee	82
Providing administrative user accounts for several employees	83
Privileged user accounts	84
Entering master data for Unix user accounts	85
General master data of a Unix user account	86
User account master data for AIX systems	89
User account limits	90
User account password data	91
Security-relevant user account master data	92
Master data for a user account on an encrypted file system	94
Additional tasks for managing Unix user accounts	95
Displaying the Unix user account overview	95
Changing the manage level of Unix user accounts	95
Assigning Unix groups directly to a Unix user account	96
Assigning extended properties to Unix user accounts	96
Automatic assignment of employees to Unix user accounts	97
Editing search criteria for automatic employee assignment	99
Disabling user accounts for AIX systems	101
Deleting and restoring Unix user accounts	103
Unix groups	104
Entering master data for Unix groups	104
General master data for a Unix group	104
Assigning Unix groups to Unix user accounts	105
Assigning Unix groups to departments, cost centers and locations	106
Assigning Unix groups to business roles	107
Assigning Unix user accounts directly to a Unix group	108
Adding Unix groups to system roles	109
Adding Unix groups to the IT Shop	110
Removing a Unix group from an IT Shop shelf	110
Removing a Unix group from all IT Shop shelves	111
Additional tasks for managing Unix groups	111
Displaying the Unix group overview	111

Adding Unix groups to Unix groups	111
Effectiveness of group memberships	112
Unix group inheritance based on categories	114
Assigning extended properties to Unix groups	117
Deleting Unix groups	117
Reports about Unix objects	118
Overview of all assignments	119
Appendix: Configuration parameters for managing a Unix environment	121
Appendix: Default project template for Unix-based target systems	124
About us	125
Contacting us	125
Technical support resources	125
Index	126

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

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 Authentication Services](#).

Architecture overview

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

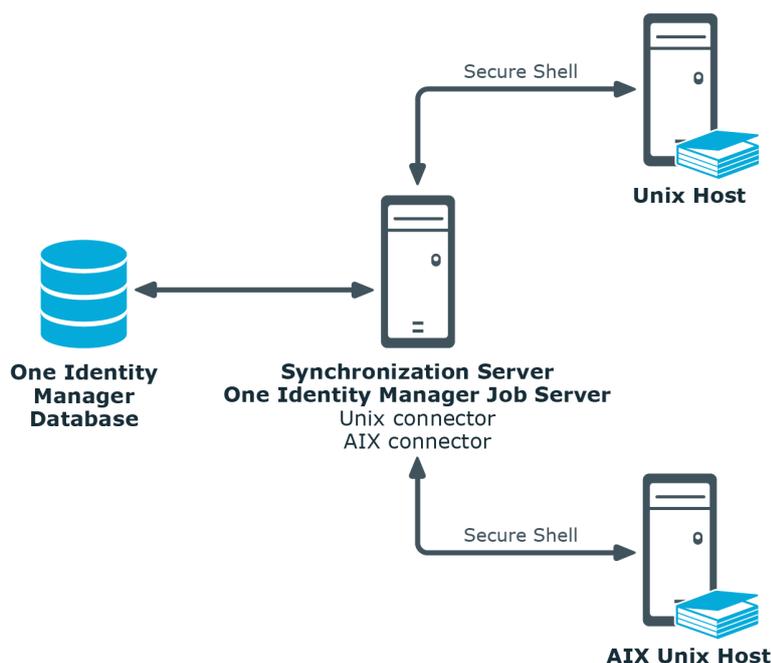
- Unix host

Unix host, which holds the directory. 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 system. The One Identity Manager Service with "Unix" is installed on this server. "Unix" 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

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

User	Tasks
Target system managers	<ul style="list-style-type: none"> • Do not assume any administrative tasks within the target system. <p>Target system managers must be assigned to the Target systems Unix application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other identity than the Primary identity. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	<ul style="list-style-type: none"> • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	<p>Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to IT Shop structures.
Administrators for	Administrators must be assigned to the Identity Management

User	Tasks
organizations	<p data-bbox="539 264 1257 293"> Organizations Administrators application role.</p> <p data-bbox="539 309 962 338">Users with this application role:</p> <ul data-bbox="587 365 1265 427" style="list-style-type: none"> <li data-bbox="587 365 1265 427">• Assign groups to departments, cost centers, and locations.
Business roles administrators	<p data-bbox="539 454 1398 517">Administrators must be assigned to the Identity Management Business roles Administrators application role.</p> <p data-bbox="539 533 962 562">Users with this application role:</p> <ul data-bbox="587 589 1046 624" style="list-style-type: none"> <li data-bbox="587 589 1046 624">• Assign groups to business roles.

Setting up synchronization with a Unix-based target system

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.
 - 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 12
- [Configuring Unix the host](#) on page 13
- [Setting up the synchronization server](#) on page 13
- [Creating a synchronization project for initial synchronization of a Unix host](#) on page 16
- [Disabling synchronization](#) on page 32
- [Customizing the synchronization configuration](#) on page 24
- [Configuration parameters for managing a Unix environment](#) on page 121
- [Default project template for Unix-based target systems](#) on page 124

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

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

Table 2: Users for synchronization

User	Permissions
User for accessing the Unix host	<p>You must provide a user account with the following 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">• Permissions for establishing a Secure Shell (SSH) connection to the host.• Administration permission for executing write operation in the Unix objects.
One Identity Manager Service user account	<p>The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited).</p> <ul style="list-style-type: none">• The user account must belong to the "Domain Users" group.• The user account must have the "Log on as a service" extended user permissions.• The user account requires access rights to the internal web service. <p>NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/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">• %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)• %ProgramFiles%\One Identity (on 64-bit operating systems)

User	Permissions
User for accessing the One Identity Manager database	The Synchronization default system user is provided to execute synchronization with an application server.

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 the 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 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
 - Microsoft .NET Framework Version 4.7.2 or later
- One Identity Manager Service, Unix connector
 - Install One Identity Manager components with the installation wizard.
 1. Select the **Select installation modules with existing database** option.
 2. Select the **Server | Job server | Unix** machine role.

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

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

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

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

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

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

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

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

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.
3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.
 - a. Select a Job server from the **Server** menu.
- OR -
To create a new Job server, click **Add**.
 - b. Enter the following data for the Job server.
 - **Server:** Name of the Job server.
 - **Queue:** Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this

unique queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.

- **Full server name:** Full server name in accordance with DNS syntax.

Syntax:

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

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

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

- For a direct connection to the database:
 - a. Select **Process collection | sqlprovider**.
 - b. Click the **Connection parameter** entry, then click the **Edit** button.
 - c. Enter the connection data for the One Identity Manager database.
 - For a connection to the application server:
 - a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
 - b. Click the **Connection parameter** entry, then click the **Edit** button.
 - c. Enter the connection data for the application server.
 - d. Click the **Authentication data** entry and click the **Edit** button.
 - e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
7. To configure remote installations, click **Next**.
 8. Confirm the security prompt with **Yes**.
 9. On the **Select installation source** page, select the directory with the install files.
 10. On the **Select private key file** page, select the file with the private key.

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

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

Installation of the service occurs automatically and may take some time.
 13. Click **Finish** on the last page of the Server Installer.

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

Creating a synchronization project for initial synchronization of 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 detailed 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 17
- [Setting up an initial synchronization project](#) on page 19
- [Default project template for Unix-based target systems](#) on page 124

Information required for setting up a synchronization project

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

Table 3: Information required for setting 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.
User account and password for logging onto the host	User account and password for logging onto the host. This user account is used to access the host by SSH. The user account requires permissions for establishing an SSH connection.
Method, user name and password for escalating permissions	<p>Executing 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">• Default The user who logs in to the host already has administrative permissions.• Sudo The user logged in on the host can execute administrative tasks with another user's permissions, such as "root". The configuration for this is done in the sudoer file on the host.• su This method uses the su command to change the context. Another user with administrative permissions is required.
Synchronization server of the Unix-based target system	<p>All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>The One Identity Manager Service with the Unix connector must be installed on the synchronization server.</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</p>

Data	Explanation
	server.

Table 4: Additional properties for the Job server

Property	Value
Server function	Unix connector AIX connector
Machine role	Server/Job server/Unix

One Identity Manager database connection data	<ul style="list-style-type: none"> • Database server • Database • SQL Server login and password • Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
---	--

Remote connection server	<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. 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"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • Unix connector or AIX connector is installed <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well.</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 12
- [Setting up the synchronization server](#) on page 13

Setting up an initial synchronization project

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

- Executed in default mode
- Started from the Launchpad

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

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

1. Start the Launchpad and log in to the One Identity Manager database.
NOTE: If synchronization is executed by an application server, connect the database through the application server.
2. Select the **Target system type Unix** entry and click **Start**.
This starts the Synchronization Editor's project wizard.
3. On the **System access** page, specify how One Identity Manager can access the target system.
 - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
 - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.
Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
4. On the **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. Enter the user account and password for SSH login on the host.
 - d. Click **Test** to test the connection. The system tries to connect to the host.
5. In the **Verify connection** pane, click **Test** to test the connection to the host.
6. 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** field, enter an alternative user, such as "root".
 - If administrative tasks should be executed 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".
7. 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.
8. 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.
9. 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
Read-only access to target system.	<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"> • Synchronization is in the direction of One Identity Manager. • Processing methods in the synchronization steps are only defined for synchronization in the direction of One Identity Manager.
Read/write access to target system. Provisioning available.	<p>Specifies whether a provisioning workflow is to be 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"> • Synchronization is in the direction of the Target system. • Processing methods are only defined in the

Option	Meaning
--------	---------

synchronization steps for synchronization in the direction of the **Target system**.

- Synchronization steps are only created for such schema classes whose schema types have write access.

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

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

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

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

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

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

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

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

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

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

NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

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

To configure the content of the synchronization log

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

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

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

7. Click **OK**.

To synchronize on a regular basis

1. Open the synchronization project in the Synchronization Editor.
2. Select the **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**.

To start initial synchronization manually

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

NOTE:

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

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

To select user accounts through account definitions

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

- [Displaying synchronization results](#) on page 23
- [Customizing the synchronization configuration](#) on page 24
- [Setting up account definitions](#) on page 35
- [Automatic assignment of employees to Unix user accounts](#) on page 97

Displaying synchronization results

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

To display a synchronization log

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

To display a provisioning log

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

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

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

Configuring the retention period for logs

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Customizing the synchronization configuration

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

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.

- Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
 - Use the schedule to ensure that the start up configurations are run in sequence.
 - Group start up configurations with the same start up behavior.

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

Detailed information about this topic

- [Configuring Unix host synchronization](#) on page 25
- [Configuring synchronization of several Unix hosts](#) on page 26
- [Updating schemas](#) on page 26

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

To create a synchronization configuration for synchronizing a Unix host

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

Detailed information about this topic

- [Configuring synchronization of several Unix hosts](#) on page 26

Configuring synchronization of several 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. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other host. Use the wizard to attach a base object.
 - In the wizard, select the Unix or AIX connector and declare the connection parameters. The connection parameters are saved in a special variable set. A start up configuration is created that uses the newly created variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related topics

- [Configuring Unix host synchronization](#) on page 25

Updating schemas

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

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

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

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

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Target system** category.
- OR -
Select the **Configuration | One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.
Opens the Mapping Editor. For more detailed information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

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.

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

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

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

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

TIP:

To display object properties of an outstanding object

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

Table 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. The Outstanding label is removed from the object.

Icon	Method	Description
		Indirect memberships cannot be deleted.
	Publish	<p>The object is added to the target system. The Outstanding label is removed from the object.</p> <p>The method triggers the <code>HandleOutstanding</code> event. This runs a target system specific process that triggers the provisioning process for the object.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The Outstanding label is removed for the object.

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

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

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

To disable bulk processing

- In the form's toolbar, click  to disable bulk processing.

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

To add custom tables to target system synchronization

1. In the Manager, select the **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.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the **Connection is read-only** option must not be set for the target system connection.

Configuring the provisioning of memberships

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

- Memberships are saved in the target system as an object property in list form.
- 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.
 - This option can only be enabled for assignment tables that have a base table with an `XDateSubItem` column.
 - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Merge mode**.
6. Save the changes.

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

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

You can restrict single provisioning of memberships with a condition. Once merge mode has been disabled for a table, the condition is deleted. Tables that have had the condition

deleted or edited are marked with the following icon: . You can restore the original condition at any time.

To restore the default condition

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

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

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
 - Assign the **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 detailed information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Editing a server](#) on page 69

Help for the analysis of synchronization issues

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

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

To generate a synchronization analysis report

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

Disabling synchronization

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

To prevent regular synchronization

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

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Detailed information about this topic

- [Creating a synchronization project for initial synchronization of a Unix host](#) on page 16

Basic data for Unix-based target systems

The following base data is relevant for managing a Unix-based target system in One Identity Manager.

- Configuration parameter

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

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

For more information, see [Configuration parameters for managing a Unix environment](#) on page 121.

- Account definitions

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

For more information, see [Setting up account definitions](#) on page 35.

- Password policy

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password 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 54.

- Initial password for new user accounts

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

For more information, see [Initial password for new Unix user accounts](#) on page 65.

- 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 65.

- Target system types

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

For more information, see [Post-processing outstanding objects](#) on page 27.

- Target system managers

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

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

For more information, see [Target system managers](#) on page 66.

- Server

Servers must know your server functionality in order to handle Unix specific processes in One Identity Manager. For example, the synchronization server.

For more information, see [Editing a server](#) on page 69.

Setting up account definitions

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

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

data required for user accounts included in the default installation. You can customize templates as required.

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

The following steps are required to implement an account definition:

- [Creating an account definition](#)
- [Creating manage levels](#)
- [Creating a formatting rule for IT operating data](#)
- [Collecting IT operating data](#)
- [Assigning account definitions to employees](#)
- [Assigning account definitions to a target system](#)

Creating an account definition

To create a new account definition

1. In the Manager, select the **Unix | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list. Select the **Change master data** task.
-OR-
Click  in the result list.
3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- [Master data for an account definition](#) on page 36

Master data for an account definition

Enter the following data for an account definition:

Table 7: Master data for an account definition

Property	Description
Account definition	Account definition name.
User	Table in the One Identity Manager schema that maps user accounts.

Property	Description
account table	
Target system	Target system to which the account definition applies.
Required account definition	Required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. Leave empty for 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 account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The can also be assigned directly to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.

Property	Description
Retain account definition if permanently disabled	<p>Specifies the account definition assignment to permanently disabled employees.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: 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 disabled employees.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: 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 employees.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on security risk	<p>Specifies the account definition assignment to employees posing a security risk.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: 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.

Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

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

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

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

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

To assign manage levels to an account definition

1. In the Manager, select the **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 levels.
- OR -
In the **Remove assignments** pane, remove the manage levels.
5. Save the changes.

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

To edit a manage level

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

Related topics

- [Master data for manage levels](#) on page 40

Master data for manage levels

Enter the following data for a manage level.

Table 8: Master data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <ul style="list-style-type: none">• Never: Data is not updated.• Always: Data is always updated.• Only initially: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.

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

Creating a formatting rule for IT operating data

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

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

- 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 and enter the following data.

Table 9: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the <code>TSB_ITDataFromOrg</code> script in their template. For detailed information, see the <i>One Identity Manager Target System Base Module Administration Guide</i> .
Source	<p>Specifies which roles to use in order to find the user account properties. You have the following options:</p> <ul style="list-style-type: none"> • Primary department • Primary location • Primary cost center • Primary business roles <p>NOTE: Only use the primary business role if the Business Roles Module is installed.</p> <ul style="list-style-type: none"> • Empty <p>If you select a role, you must specify a default value and set the Always use default value option.</p>
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The Employee - new user account with default properties created mail template is used. To change the mail template, adjust the TargetSystem Unix Accounts MailTemplateDefaultValues configuration parameter.

4. Save the changes.

Related topics

- [Collecting IT operating data](#) on page 43

Collecting IT operating data

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

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

Example

Normally, each employee in department A obtains a default user account in the host A. In addition, certain employees 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. Specify the "Department" property in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

Specify the effective IT operating data of department A for the 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.

Table 10: IT operating data

Property	Description
Effects on	<p>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.</p> <p>To specify an application scope</p> <ol style="list-style-type: none">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	<p>User account property for which the value is set.</p> <p>In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the <i>One Identity Manager Target System Base Module Administration Guide</i>.</p>
Value	<p>Concrete value which is assigned to the user account property.</p>

4. Save the changes.

Related topics

- [Creating a formatting rule for IT operating data](#) on page 41

Modify IT operating data

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

Prerequisites

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

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

To execute the template

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

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

Old value: Current value of the object property.

New value: Value that the object property would have following modification of the IT operating data.

Selection: Specifies whether or not the new value is transferred to the user account.

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

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

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

Detailed information about this topic

- [Assigning account definitions to departments, cost centers, and locations](#) on page 46
- [Assigning an account definition to business roles](#) on page 47
- [Assigning account definitions to all employees](#) on page 48
- [Assigning account definitions directly to employees](#) on page 48
- [Assigning account definitions to system roles](#) on page 49
- [Adding account definitions to the IT Shop](#) on page 50

Assigning account definitions to departments, cost centers, and locations

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 an account definition to business roles](#) on page 47
- [Assigning account definitions to all employees](#) on page 48
- [Assigning account definitions directly to employees](#) on page 48
- [Assigning account definitions to system roles](#) on page 49
- [Adding account definitions to the IT Shop](#) on page 50

Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In the Manager, select the **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, 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 46
- [Assigning account definitions to all employees](#) on page 48
- [Assigning account definitions directly to employees](#) on page 48
- [Assigning account definitions to system roles](#) on page 49
- [Adding account definitions to the IT Shop](#) on page 50

Assigning account definitions to all employees

To assign an account definition to all employees

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

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

5. Save the changes.

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

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

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 46
- [Assigning an account definition to business roles](#) on page 47
- [Assigning account definitions directly to employees](#) on page 48
- [Assigning account definitions to system roles](#) on page 49
- [Adding account definitions to the IT Shop](#) on page 50

Assigning account definitions directly to employees

To assign an account definition directly to employees

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

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

To remove an assignment

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

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 46
- [Assigning an account definition to business roles](#) on page 47
- [Assigning account definitions to all employees](#) on page 48
- [Assigning account definitions to system roles](#) on page 49
- [Adding account definitions to the IT Shop](#) on page 50

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

1. In the Manager, select the **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 46
- [Assigning an account definition to business roles](#) on page 47
- [Assigning account definitions to all employees](#) on page 48
- [Assigning account definitions directly to employees](#) on page 48
- [Adding account definitions to the IT Shop](#) on page 50

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

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

To add an account definition to the IT Shop

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

To remove an account definition from individual IT Shop shelves

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

To remove an account definition from all IT Shop shelves

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

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

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

Related topics

- [Master data for an account definition on page 36](#)
- [Assigning account definitions to departments, cost centers, and locations on page 46](#)
- [Assigning an account definition to business roles on page 47](#)
- [Assigning account definitions to all employees on page 48](#)
- [Assigning account definitions directly to employees on page 48](#)
- [Assigning account definitions to system roles on page 49](#)

Assigning account definitions to a target system

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

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

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

To assign the account definition to a target system

1. In the Manager, select the host in the **Unix | Hosts** category.
2. Select the **Change master 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

- [Automatic assignment of employees to Unix user accounts](#) on page 97

Deleting an account definition

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
 - a. In the Manager, select the **Unix | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change master data** task.
 - d. On the **General** tab, disable the **Automatic assignment to employees** option.
 - e. Save the changes.
2. Remove direct assignments of the account definition to employees.
 - a. In the Manager, select the **Unix | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign to employees** task.
 - d. In the **Remove assignments** pane, remove the employees.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **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.

In the **Remove assignments** pane, remove the business roles.
 - d. Save the changes.
 5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

To remove an account definition from all IT Shop shelves

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

- OR -

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

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.
6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. In the Manager, select the **Unix | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change master data** task.
 - d. From the **Required account definition** menu, remove the account definition.
 - e. Save the changes.

7. Remove the account definition's assignments to target systems.
 - a. In the Manager, select the host in the **Unix | Hosts** category.
 - b. Select the **Change master data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
8. Delete the account definition.
 - a. In the Manager, select the **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.

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

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

Detailed information about this topic

- [Predefined password policies](#) on page 54
- [Using password policies](#) on page 56
- [Editing password policies](#) on page 58
- [Custom scripts for password requirements](#) on page 61
- [Password exclusion list](#) on page 64
- [Checking a password](#) on page 64
- [Testing password generation](#) on page 64

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

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

The **UnixPassword policy** is predefined for Unix-based target systems. You can apply this password policy to Unix user accounts (`UNIXUser.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 (UNIXUser.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 account definition of the user account.
2. Password policy of the manage level of the user account.
3. Password policy for the host of the user account.
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 the **Assign objects** task.

- Click **Add** in the **Assignments** section and enter the following data.

Table 11: Assigning a password policy

Property	Description
Apply to	Application scope of the password policy. To specify an application scope <ol style="list-style-type: none">Click → next to the field.Select one of the following references under Table:<ul style="list-style-type: none">The table that contains the base objects of synchronization.To apply the password policy based on the account definition, select the <code>TSBAccountDef</code> table.To apply the password policy based on the manage level, select the <code>TSBBehavior</code> table.Under Apply to, select the table that contains the base objects.<ul style="list-style-type: none">If you have selected the table containing the base objects of synchronization, next select the specific target system.If you have selected the <code>TSBAccountDef</code> table, next select the specific account definition.If you have selected the <code>TSBBehavior</code> table, next select the specific manage level.Click OK.
Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

- Save the changes.

To change a password policy's assignment

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

Editing password policies

To edit 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 and select **Change master data**.
- OR -
Click  in the result list.
3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

- [General master data for password policies](#) on page 58
- [Policy settings](#) on page 59
- [Character classes for passwords](#) on page 60
- [Custom scripts for password requirements](#) on page 61

General master data for password policies

Enter the following master data for a password policy.

Table 12: Master data for a password policy

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

Policy settings

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

Table 13: Policy settings

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

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

Character classes for passwords

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

Table 14: Character classes for passwords

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

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

Custom scripts for password requirements

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

Detailed information about this topic

- [Script for checking passwords](#) on page 61
- [Script for generating a password](#) on page 62

Script for checking passwords

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example of a script that checks a password

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

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

To use a custom script for checking a password

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

Related topics

- [Script for generating a password](#) on page 62

Script for generating a password

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

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

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

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

```
End Sub
```

To use a custom script for generating a password

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

Related topics

- [Script for checking passwords](#) on page 61

Password exclusion list

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

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

To add a term to the restricted list

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

Checking a password

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

To check if a password conforms to the password policy

1. In the Manager, select the **Unix | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select the **Change master data** task.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.
A display next to the password shows whether it is valid or not.

Testing password generation

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

To generate a password that conforms to the password policy

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

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

This generates and displays a password.

Initial password for new Unix user accounts

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

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

Related topics

- [Password policies for Unix user accounts](#) on page 54
- [Email notifications about login data](#) on page 65

Email notifications about login data

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

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

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the *One Identity Manager Installation Guide*.

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

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

To send initial login data by email

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

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

Target system managers

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

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

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

Implementing application roles for target system managers

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

Target system managers with the default application role are authorized to edit all the Unix hosts in One Identity Manager.

3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual Unix hosts.

Table 15: Default application roles for target system managers

User	Tasks
Target system managers	<p>Target system managers must be assigned to the Target systems Unix application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects like user accounts or groups.• Edit password policies for the target system.• Prepare groups to add to the IT Shop.• Can add employees who have an other identity than the Primary identity.• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.• Edit the synchronization's target system types and outstanding objects.• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

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

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

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

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

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

To specify target system managers for individual 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 master data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

- OR -

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

- a. Enter the application role name and assign the **Target systems | Unix** parent application role.
 - b. Click **OK** to add the new application role.
6. Save the changes.
 7. Assign employees to this application role who are permitted to edit the host in One Identity Manager.

Related topics

- [One Identity Manager users for managing Unix-based target systems](#) on page 8
- [General master data for Unix hosts](#) on page 74

Editing a server

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 detailed information, see *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 master data category.

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

Detailed information about this topic

- [Master data for a Job server](#) on page 69
- [Server functions of a Job server](#) on page 72

Master data for a Job server

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

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

Table 16: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: <Name of server>.<Fully qualified domain name>
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The Server is cluster and Server belongs to cluster properties are mutually exclusive.
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

Property Meaning

	steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	<p>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.</p> <p>The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.</p>
Stop One Identity Manager Service	<p>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.</p> <p>You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i>.</p>
No automatic software update	<p>Specifies whether to exclude the server from automatic software updating.</p> <p> NOTE: Servers must be manually updated if this option is set.</p>
Software update running	Specifies whether a software update is currently running.
Last fetch time	Last time the process was collected.
Last timeout check	The time of the last check for loaded process steps with a dispatch value that exceeds the one in the Common Jobservice LoadedJobsTimeOut configuration parameter.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- [Server functions of a Job server](#) on page 72

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 17: 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. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the ScriptComponent process component.
Native database connector	This server can connect to an ADO.Net database.
One Identity Manager	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.

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

- [Master data for a Job server](#) on page 69

Unix host

If you use a default project template, the Synchronization Editor sets up the domains in the One Identity Manager database.

NOTE: 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 master data for a Unix host

1. Select the **Unix | Hosts** category.
2. Select the host in the result list.
3. Select the **Change master data** task.
4. Edit the host's master data.
5. Save the changes.

Related topics

- [General master data for Unix hosts](#) on page 74

General master data for Unix hosts

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

Table 18: General master 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.
Device	The computer is connected to this device. Specify a new device using the  button next to the menu.

Property	Description									
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 employees to user accounts is used for this host and user accounts should be created that are already managed (Linked configured state). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the employee (Linked state) if no account definition is given. This is the case on initial synchronization, for example.</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 new application role.</p>									
Synchronized by	<p>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.</p> <p>If you create a host with the Synchronization Editor, One Identity Manager is used.</p> <p>Table 19: Permitted values</p> <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> <p>NOTE: If you select No synchronization, you can define custom processes to exchange data between One Identity Manager and the target system.</p>	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								
Operating system description	Description of the operating system.									
Distribution	Installed distribution of the operating system.									
Distribution version	Version of the installed distribution.									

Property	Description
Kernel version	Current version of the kernel.
Operating system type	Type of operating system, such as Linux, AIX, or UNIX.

Specifying categories for inheriting permissions

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

To define a category

1. In the Manager, select the host in the **Unix | Hosts** category.
2. Select the **Change master 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 114

How to edit a synchronization project

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. Select the **Unix | Hosts** category.
2. Select the host in the result list. Select the **Change master data** task.
3. Select the **Edit synchronization project...** task.

Related topics

- [Customizing the synchronization configuration](#) on page 24

Displaying the Unix host overview

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

To obtain an overview of a host

1. Select **Unix | Hosts**.
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. 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 a formatting rule for IT operating data](#) on page 41
- [General master data of a Unix user account](#) on page 86

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 rights to the resources through membership in groups.

Detailed information about this topic

- [Linking user accounts to employees](#) on page 78
- [Supported user account types](#) on page 79
- [Entering master data for Unix user accounts](#) on page 85
- [Automatic assignment of employees to Unix user accounts](#) on page 97

Linking user accounts to employees

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

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

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a host, a new user account is created. This is done by assigning account definitions to an employee

using the integrated inheritance mechanism and subsequent process handling.

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

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

Related topics

- [Entering master data for Unix user accounts](#) on page 85
- [Setting up account definitions](#) on page 35
- [Automatic assignment of employees to Unix user accounts](#) on page 97
- For more detailed information about handling and administration of employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

Supported user account types

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

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

- Identity

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

Table 20: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts	Organizational

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

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

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

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

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

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

- Privileged user account

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

Detailed information about this topic

- [Default user accounts](#) on page 81
- [Administrative user accounts](#) on page 82
- [Providing administrative user accounts for one employee](#) on page 82

- [Providing administrative user accounts for several employees](#) on page 83
- [Privileged user accounts](#) on page 84

Default user accounts

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

To create default user accounts through account definitions

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

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

Which IT operating data is required depends on the target system. The following 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 employees.

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

Related topics

- [Setting up account definitions](#) on page 35

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 employee](#) on page 82
- [Providing administrative user accounts for several employees](#) on page 83

Providing administrative user accounts for one employee

Prerequisites

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

To prepare an administrative user account for a person

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

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

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

Related topics

- [Providing administrative user accounts for several employees](#) on page 83
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

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

To prepare an administrative user account for multiple employees

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

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

- c. Select the **Assign employees authorized to use** task.
- d. In the **Add assignments** pane, add employees.

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

To remove an assignment

- Select the employee and double-click .

Related topics

- [Providing administrative user accounts for one employee](#) on page 82
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

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

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

To create privileged users through account definitions

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

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

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

- In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
 - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
 - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.
5. Enter the effective IT operating data for the target system.
- Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
6. Assign the account definition directly to employees who work with privileged user accounts.
- When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

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

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

Related topics

- [Setting up account definitions](#) on page 35

Entering master data for Unix user accounts

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

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

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

To create a user account

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

To edit master data for a user account

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

To manually assign or create a user account for an employee

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

Detailed information about this topic

- [General master data of a Unix user account](#) on page 86
- [User account master data for AIX systems](#) on page 89

Related topics

- [Setting up account definitions](#) on page 35
- [Supported user account types](#) on page 79
- [Linking user accounts to employees](#) on page 78

General master data of a Unix user account

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

Table 21: Additional master data for a user account

Property	Description
Host	The user account's host.
Employee	<p>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account.</p> <p>You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.</p>
Account definition	<p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account master data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p>NOTE: The account definition cannot be changed once the user account has been saved.</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 executed 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 employee's central user account depending on the manage level.
User ID	User ID for the user account in the Unix host.
Password	<p>Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>If you use an 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>NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.</p>

Property	Description
Password confirmation	Reconfirm password.
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"> • If you entered a primary group in the host, the group is used as primary group when a user account is created. • 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.
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 QER CalculateRiskIndex configuration parameter is set. For detailed 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 employee's internal name depending on the manage level.
Identity	<p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account that is used for a specific purpose, such as training. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this user account.

Property	Description
	<ul style="list-style-type: none"> • Service identity: Service account.
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Privileged user account	Specifies whether this is a privileged user account.

Related topics

- [Setting up account definitions](#) on page 35
- [Password policies for Unix user accounts](#) on page 54
- [Initial password for new Unix user accounts](#) on page 65
- [Unix group inheritance based on categories](#) on page 114
- [Supported user account types](#) on page 79
- [General master data for Unix hosts](#) on page 74
- [Disabling user accounts for AIX systems](#) on page 101

User account master data for AIX systems

You can enter additional master data for 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

- [User account limits](#) on page 90
- [User account password data](#) on page 91
- [Security-relevant user account master data](#) on page 92
- [Master data for a user account on an encrypted file system](#) on page 94
- [General master data for Unix hosts](#)

User account limits

On **Limits**, 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)	Soft limit for the maximum amount of physical memory a user process can take up. (Parameter <code>MEMLOCK</code>).
Memory size (hard)	Maximum amount of physical memory a user process can take up. (Parameter <code>MEMLOCK_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>NOFILES</code>).
File descriptors (hard)	Absolute maximum number of file descriptors a user process can have open at the same time. (Parameter <code>NOFILES_HARD</code>).
Threads	Soft limit for the number of threads per process. (Parameter <code>THREADS</code>).

Property	Description
(soft)	
Threads (hard)	Absolute maximum number of threads per process. (Parameter threads_hard).
Processes (soft)	Soft limit for the number of processes per user. (Parameter nproc).
Processes (hard)	Absolute maximum for the number of processes per user. (Parameter nproc_hard).

User account password data

On **Password**, enter the following additional information about a user account in the AIX system. This data is mapped in `/etc/security/user`.

Table 23: Password data for user accounts in an AIX system

Property	Description
minlen	Minimum number of characters a password must have. (Parameter minlen).
maxrepeats	Maximum number of characters that can be repeated in passwords. The default value 8 specifies that a maximum has not been fixed. (Parameter maxrepeats).
mindiff	Minimum number of unique characters that passwords must contain. (Parameter mindiff).
minalpha	Specifies the minimum number of alphabetical characters a new password must contain. (Parameter minalpha).
minloweralpha	Specifies the minimum number of lowercase letters a new password must contain. (Parameter minloweralpha).
minupperalpha	Specifies the minimum number of uppercase letters a new password must contain. (Parameter minupperalpha).
mindigit	Specifies the minimum number of digits a new password must contain. (Parameter mindigit).
minspecialchar	Specifies the minimum number of special characters a new 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 black listed passwords. Verifies passwords do not include standard Unix words. (Parameter dictionlist).

Property	Description
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-relevant user account master data

On **Security**, enter the following additional information about a user account in the AIX system. This data is mapped in /etc/security/user.

Table 24: Additional security relevant data for user accounts in an AIX system

Property	Description
account_locked	Specifies whether the user account is locked. (Parameter account_locked).
admin	Defines 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

Property	Description
	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 execute 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).
rlogin	Permits access 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 user accounts for AIX systems on page 101](#)

Master data for a user account on an encrypted file system

On the **Encrypted File System** tab, enter the following additional information for using encrypted file system (EFS) for a user account in an AIX system. This data is mapped in `/etc/security/user`.

Table 25: User account master data for encrypted file systems

Property	Description
<code>efs_adminks_access</code>	Defines the <code>efs_admin</code> keystore location (Parameter <code>efs_adminks_access</code>). Permitted values: <ul style="list-style-type: none">fileldap
<code>efs_allowksmodechangebyuser</code>	Specifies whether the user can change the mode or not. (Parameter <code>efs_allowksmodechangebyuser</code>).
<code>efs_file_algo</code>	Algorithm used to generate the file protection key. (Parameter <code>efs_file_algo</code>). Permitted values: <ul style="list-style-type: none">AES_128_CBCAES_192_CBCAES_256_CBC
<code>efs_initialks_mode</code>	Initial mode of the user keystore. (Parameter <code>efs_initialks_mode</code>). Permitted values: <ul style="list-style-type: none">guardadmin
<code>efs_keystore_access</code>	User keystore location. (Parameter <code>efs_keystore_access</code>). Permitted values: <ul style="list-style-type: none">nonefile
<code>efs_keystore_algo</code>	Algorithm used to generate the user private key when the keystore is created. (Parameter <code>efs_keystore_algo</code>). Permitted values: <ul style="list-style-type: none">RSA_1024RSA_2048RSA_4096

Additional tasks for managing Unix user accounts

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

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

Changing the manage level of Unix user accounts

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

To change the manage level for a user account

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

Related topics

- [Entering master data for Unix user accounts](#) on page 85

Assigning Unix groups directly to a Unix user account

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

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

To assign groups directly to user accounts

1. In the Manager, select the **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 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 105

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.

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

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

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

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

Automatic assignment of employees to Unix user accounts

Table 26: Configuration parameters for automatic employee assignment

Configuration parameter	Meaning
TargetSystem Unix PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem Unix PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem Unix PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe () delimited list that is handled as a regular search pattern. Example: ROOT
TargetSystem Unix PersonAutoDisabledAccounts	This configuration parameter specifies whether employees are automatically assigned to disabled user accounts. User accounts do not obtain an account definition.

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

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

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

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the "TargetSystem | Unix | PersonAutoFullsync" configuration parameter and select the required mode.
- If you want employees 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, specify the user accounts that must not be assigned automatically to employees.

Example:

ROOT

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

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

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

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

To select user accounts through account definitions

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

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

Related topics

- [Creating an account definition](#) on page 36
- [Assigning account definitions to a target system](#) on page 51
- [Editing search criteria for automatic employee assignment](#) on page 99

Editing search criteria for automatic employee assignment

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

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

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

It is not recommended to make assignments to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user accounts for the respective user account.

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

To specify criteria for employee assignment

1. Select the **Unix | Host** category.
2. Select the host in the result list.
3. Select the **Define search criteria for employee assignment** task.

- Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 27: Default search criteria for user accounts and contacts

Apply to	Column for employee	Column for user account
Unix user accounts	Central user account (CentralAccount)	User name (AccountName)

- Save the changes.

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

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

Table 28: Manual assignment view

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

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

To apply search criteria to user accounts

- Click **Reload**.

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

To assign employees directly using a suggestion list

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

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

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

To remove assignments

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

The assigned employees are removed from the selected user accounts.

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

Related topics

- [Automatic assignment of employees to Unix user accounts](#) on page 97

Disabling user accounts for AIX systems

NOTE: The behavior described in the following, only applies to user account in an AIX system.

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

Scenario:

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

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

Scenario:

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

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

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

To disable the user account when the configuration parameter is disabled

1. In the Manager, select the **Unix | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **Security** tab, set the **account_locked** option.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

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

1. In the Manager, select the **Unix | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **Security** tab, set the **account_locked** option.
5. Save the changes.

Related topics

- [Setting up account definitions](#) on page 35
- [Creating manage levels](#) on page 38
- [Deleting and restoring Unix user accounts](#) on page 103
- For more detailed information about deactivating and deleting employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

Deleting and restoring Unix user accounts

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

To delete a user account

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

To restore a user account

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

Configuring deferred deletion

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

Related topics

- [Disabling user accounts for AIX systems](#) on page 101
- For more detailed information about deactivating and deleting employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

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 to edit already existing groups.

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

Detailed information about this topic

- [Entering master data for Unix groups](#) on page 104
- [Assigning Unix groups to Unix user accounts](#) on page 105

Entering master data for Unix groups

To edit group master data

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

Detailed information about this topic

- [General master data for a Unix group](#) on page 104

General master data for a Unix group

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

Table 29: General master 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 by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is activated. For more detailed information about risk assessment, see the One Identity Manager Risk Assessment Administration Guide.
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 114
- For more detailed information about preparing groups for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning Unix groups to Unix user accounts

Groups can be assigned directly or indirectly to user accounts. In the case of indirect assignment, employees, and groups are assigned to hierarchical roles, such as , departments, cost centers, locations, or business roles. The groups assigned to an employee are calculated from the position in the hierarchy and the direction of inheritance.

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

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

Groups can also be assigned to employees through IT Shop requests. So that groups can be assigned using IT Shop requests, employees are added to a shop as customers. All groups assigned to this shop can be requested by the customers. Requested groups are assigned to the employees after approval is granted.

Detailed information about this topic

- [Assigning Unix groups to departments, cost centers and locations](#) on page 106
- [Assigning Unix groups to business roles](#) on page 107
- [Assigning Unix user accounts directly to a Unix group](#) on page 108
- [Adding Unix groups to system roles](#) on page 109
- [Adding Unix groups to the IT Shop](#) on page 110

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

1. In the Manager, select the **Organizations | Departments** category.
- OR -
In the Manager, select the **Organizations | Cost centers** category.
- OR -
In the Manager, select the **Organizations | Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign 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

- [Assigning Unix groups to business roles](#) on page 107
- [Assigning Unix user accounts directly to a Unix group](#) on page 108
- [Adding Unix groups to system roles](#) on page 109
- [Adding Unix groups to the IT Shop](#) on page 110

Assigning Unix groups to business roles

Installed modules: Business Roles Module

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, assign business roles.

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

To remove an assignment

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

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

1. In the Manager, select the **Business roles | <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign 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

- [Assigning Unix groups to departments, cost centers and locations](#) on page 106
- [Assigning Unix user accounts directly to a Unix group](#) on page 108
- [Adding Unix groups to system roles](#) on page 109
- [Adding Unix groups to the IT Shop](#) on page 110

Assigning Unix user accounts directly to a Unix group

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

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

To assign a group directly to user accounts

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

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

To remove an assignment

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

Related topics

- [Assigning Unix groups directly to a Unix user account](#) on page 96
- [Assigning Unix groups to departments, cost centers and locations](#) on page 106
- [Assigning Unix groups to business roles](#) on page 107
- [Adding Unix groups to system roles](#) on page 109
- [Adding Unix groups to the IT Shop](#) on page 110

Adding Unix groups to system roles

Installed modules: System Roles Module

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

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

To assign a group to system roles

1. In the Manager, select the **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

- [Assigning Unix groups to departments, cost centers and locations](#) on page 106
- [Assigning Unix groups to business roles](#) on page 107
- [Assigning Unix user accounts directly to a Unix group](#) on page 108
- [Adding Unix groups to the IT Shop](#) on page 110

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 option **IT Shop**.
- The group must be assigned to a service item.
- If you want the group to be assigned only to employees 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. Select the **Unix | Groups** (non role-based login) category.
- OR -
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 detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related topics

- [General master data for a Unix group](#) on page 104
- [Removing a Unix group from an IT Shop shelf](#) on page 110
- [Removing a Unix group from all IT Shop shelves](#) on page 111

Removing a Unix group from an IT Shop shelf

To remove a group from individual IT Shop shelves

1. Select the **Unix | Groups** (non role-based login) category.
- OR -
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.

Removing a Unix group from all IT Shop shelves

To remove a group from all IT Shop shelves

1. Select the **Unix | Groups** (non role-based login) category.
- OR -
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.

Additional tasks for managing Unix groups

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

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. Select the **Unix | Groups** category.
2. Select the group in the result list.
3. Select the **Unix group overview** task.

Adding Unix groups to Unix groups

Use this task to add a group to another group.

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

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

To remove an assignment

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

Effectiveness of group memberships

Table 30: Configuration parameters for conditional inheritance

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

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

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

NOTE:

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

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

Example of 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.

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

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

Table 31: Specifying excluded groups (UNXGroupExclusion table)

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

Table 32: Effective assignments

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

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

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

Table 33: Excluded groups and effective assignments

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

Prerequisites

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

To exclude a group

1. In the Manager, select the **Unix | Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.
- OR -
In the **Remove assignments** pane, remove the groups that are not longer mutually exclusive.
5. Save the changes.

Unix group inheritance based on categories

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

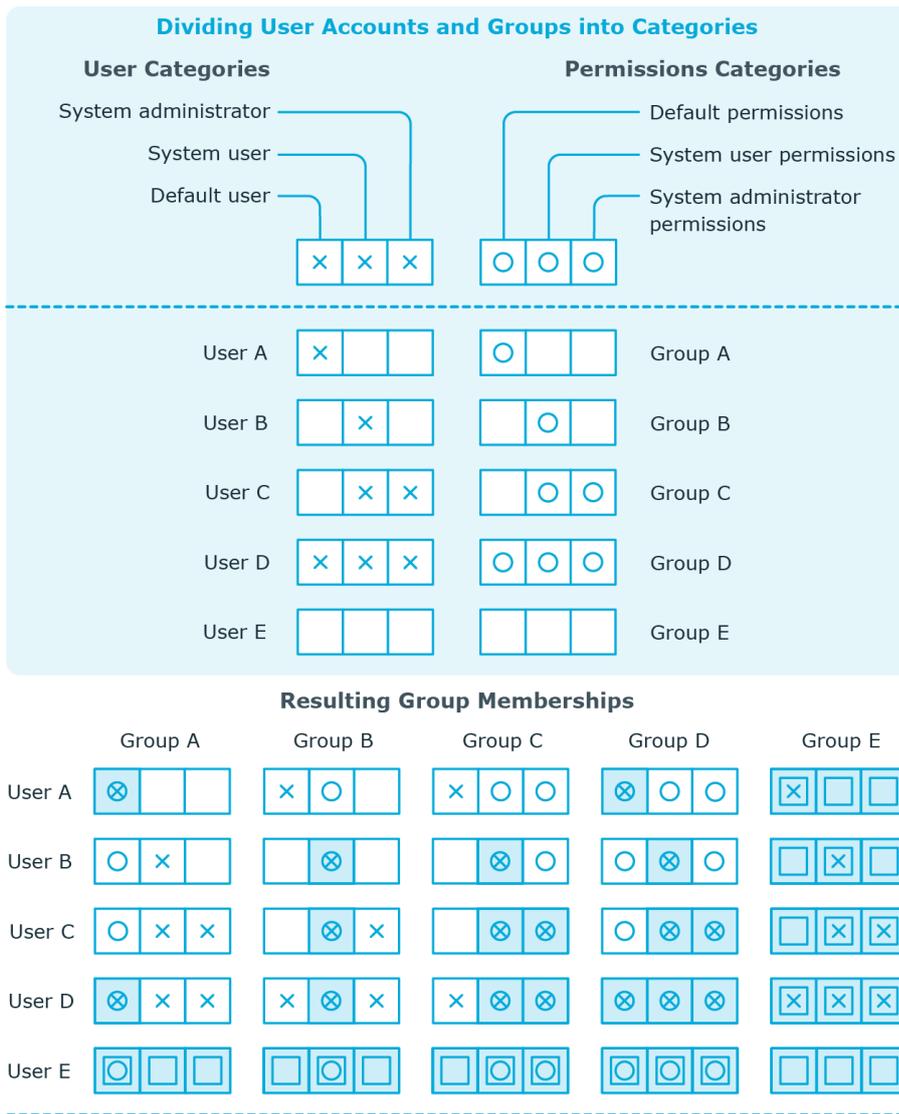
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or 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 34: 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 is not categorized</p>	<p>□ Inherits because user account and group are not categorized</p> <p>⊗ Inherits because group is not categorized</p>
--	---

To use inheritance through categories

- Define the categories in the host environment.
- Assign categories to user accounts through their master data.
- Assign categories to groups through their master data.

Related topics

- [Specifying categories for inheriting permissions](#) on page 76
- [General master data of a Unix user account](#) on page 86
- [General master data for a Unix group](#) on page 104

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.

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

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

To remove an assignment

- Select the extended property and double-click .
5. Save the changes.

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

Deleting Unix groups

To delete a group

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

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

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 35: Reports for the target system

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

Overview of all assignments

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

Examples

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

To display detailed information about assignments

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

All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the  icon in the report's toolbar.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the  button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to  to start a wizard that allows you to bookmark this list of employees for tracking. This creates a new business role to which the employees are assigned.

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



Table 36: 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.

Configuration parameters for managing a Unix environment

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

Table 37: Configuration parameters

Configuration parameter	Description
TargetSystem Unix	Preprocessor relevant configuration parameter to control the component parts for the managing Unix-based custom target systems. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
TargetSystem Unix Accounts	This configuration parameter permits configuration of user account data.
TargetSystem Unix Accounts InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem Unix Accounts InitialRandomPassword SendTo	This configuration parameter specifies to which employee the email with the randomly generated password should be sent (manager cost center/department/location/role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the "TargetSystem Unix DefaultAddress" configuration parameter.
TargetSystem Unix Accounts InitialRandomPassword SendTo MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The Employee - new user account created mail template is used.
TargetSystem Unix	This configuration parameter contains the name of the

Configuration parameter	Description
Accounts InitialRandomPassword SendTo MailTemplatePassword	mail template sent to provide users with information about their initial password. The Employee - initial password for new user account mail template is used.
TargetSystem Unix Accounts MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The Employee - new user account with default properties created mail template is used.
TargetSystem Unix Accounts PrivilegedAccount	This configuration parameter allows configuration of settings for privileged Unix user accounts.
TargetSystem Unix Accounts PrivilegedAccount AccountName_Postfix	This configuration parameter contains the postfix for formatting login names for privileged user accounts.
TargetSystem Unix Accounts PrivilegedAccount AccountName_Prefix	This configuration parameter contains the prefix for formatting login names for privileged user accounts.
TargetSystem Unix DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem Unix MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem Unix PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem Unix PersonAutoDisabledAccounts	This configuration parameter specifies whether employees are automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
TargetSystem Unix PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem Unix PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe () delimited list that is handled as a regular search

Configuration parameter	Description
--------------------------------	--------------------

pattern.

Example:

ROOT

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 template uses mappings for the following schema types.

Table 38: Mapping Unix schema types to tables in the One Identity Manager schema

Schema type in Unix-based target system	Table in the One Identity Manager Schema
Group	UNXGroup
Host	UNXHost
LoginShell	UNXLoginShell
User	UNXAccount

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

Contacting us

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

Technical support resources

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

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

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

A

- account definition 35
 - add to IT Shop 50
 - assign automatically 48
 - assign to all employees 48
 - assign to business role 47
 - assign to cost center 46
 - assign to department 46
 - assign to employee 45, 48
 - assign to location 46
 - assign to system roles 49
 - assign to Unix host 51
 - create 36
 - delete 52
 - IT operating data 41, 43
 - manage level 38
- architecture overview 7

C

- calculation schedule
 - disable 32
- configuration parameter 121

D

- direction of synchronization
 - direction target system 19, 25
 - in Manager 19

E

- email notification 65

- employee assignment
 - automatic 97
 - manual 100
 - remove 100
 - search criteria 99
 - table column 99
- exclusion definition 112

I

- identity 79
- IT operating data
 - change 44
- IT Shop shelf
 - assign account definition 50

J

- Job server
 - edit 13
 - load balancing 31

L

- load balancing 31
- login data 65

M

- membership
 - modify provisioning 30

N

notification 65

O

object

delete immediately 27

outstanding 27

publish 27

One Identity Manager

administrator 8

target system administrator 8

target system manager 8, 66

user 8

outstanding object 27

P

password

initial 65

password policy 54

assign 56

character sets 60

check password 64

conversion script 61-62

default policy 56, 58

display name 58

edit 58

error message 58

excluded list 64

failed logins 59

generate password 64

initial password 59

name components 59

password age 59

password cycle 59

password length 59

password strength 59

predefined 54

test script 61

project template 124

provisioning

accelerate 31

members list 30

S

schema

changes 26

shrink 26

update 26

single object synchronization

accelerate 31

synchronization

authorizations 12

base object

create 26

configure 19, 24

connection parameter 19, 24, 26

different hosts 26

extended schema 26

prevent 32

scope 24

set up 11

start 19

synchronization project

create 16, 19

target system schema 26

user 12

variable 24

variable set 26

- workflow 19, 25
- synchronization analysis report 32
- synchronization configuration
 - customize 24-26
- synchronization log 23
 - retention period 24
- synchronization project
 - create 16, 19
 - disable 32
 - edit 76
 - project template 124
- synchronization server
 - configure 13
 - install 13
 - Job server 13
- synchronization workflow
 - create 19, 25

T

- target system synchronization 27
- template
 - IT operating data, modify 44

U

- Unix group
 - add to IT Shop 110
 - add to system role 109
 - assign extended properties 117
 - assign group 111
 - assign to business role 107
 - assign to cost center 106
 - assign to department 106
 - assign to location 106
 - assign user account 96, 105, 108

- category 104, 114
- delete 117
- edit 104
- effective 112
- exclusion 112
- group ID 104
- host 104
- primary group 74, 86
- remove from IT Shop 110-111
- risk index 104
- service item 104

Unix host 77

- account definition 74
- account definition (initial) 51
- AIX system 74
- application roles 8
- category 76, 114
- employee assignment 99
- overview of all assignments 119
- primary group 74
- report 118
- set up 74
- synchronization 74
- target system manager 8, 66, 74

Unix login shell 77

Unix user account

- account definition 51, 86
- administrative user account 82
- assign employee 78, 85-86, 97
- assign extended properties 96
- assign group 96, 108
- category 86, 114
- comment (Gecos) 86
- default user accounts 81
- delete 103

- disable (AIX system) 101
- EFS (AIX system) 94
- employee 86
- encrypted file system (AIX system) 94
- group ID 86
- groups can be inherited 41
- home directory 86
- host 86
- identity 41, 86
- inherit group 86
- limits (AIX system) 90
- lock 103
- login shell 41, 86
- manage level 86, 95
- password 86
 - initial 65
- password data (AIX system) 91
- primary group 74, 86
- privileged user account 41, 84, 86
- restore 103
- risk index 86
- security (AIX system) 92
- set up 85
- user account UID 86
- user name 86
- user account
 - administrative user account 82-83
 - apply template 44
 - default user accounts 81
 - identity 79
 - password
 - notification 65
 - privileged user account 79, 84
 - type 79