One Identity Manager 8.2.1

Administration Guide for Connecting Unix-Based Target Systems

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

Legend

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

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

One Identity Manager Administration Guide for Connecting Unix-Based Target Systems
Updated - 03 June 2022, 03:29
Version - 8.2.1

Contents

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 Safeguard Authentication Services.

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

Architecture overview

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

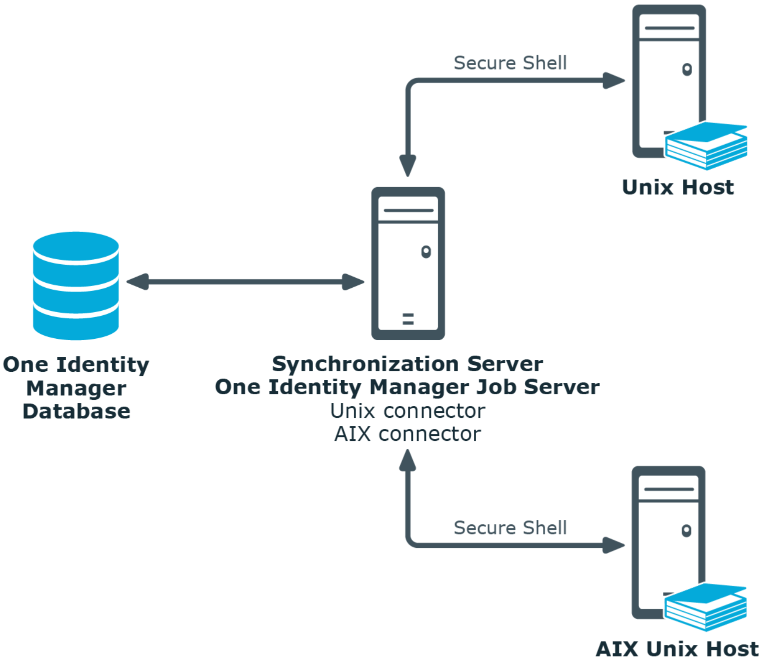
- Unix host

  Unix host where the directory is kept. This host is a selected live host with a good network connection to the synchronization server. The synchronization server connects to this host in order to access the Unix objects.

- Synchronization server

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

Figure 1: Architecture for synchronization



One Identity Manager users for managing Unix-based target systems

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

Table 1: Users

Users	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager.

Users	Tasks
	• 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. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Unix** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have another 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	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. One Identity Manager administrators: • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required.

Users	Tasks
	- Create custom processes in the Designer as required. - Create and configure schedules as required. - Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: - Assign groups to IT Shop structures.
Administrators for organizations	Administrators must be assigned to the **Identity Management | Organizations | Administrators** application role. Users with this application role: - Assign groups to departments, cost centers, and locations.
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role. Users with this application role: - Assign groups to business roles.

Configuration parameters for managing Unix-based target systems

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for 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 Unix-based target systems on page 143.

2

Synchronizing Unix-based target systems

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

This sections explains how to:

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

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

Detailed information about this topic

- Setting up initial synchronization with a Unix host on page 12
- Customizing the synchronization configuration on page 25
- Running synchronization on page 34
- Tasks following synchronization on page 38
- Troubleshooting on page 41

Setting up initial synchronization with a Unix host

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

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

1. Prepare a user account with sufficient permissions for synchronizing in the Unix-based target system.
2. One Identity Manager components for managing Unix-based target systems are available if the **TargetSystem | Unix** configuration parameter is set.
   - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

     > NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

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

Related topics

- Users and permissions for synchronizing with a Unix-based target system on page 13
- Configuring Unix the host on page 14
- Setting up a synchronization server for Unix-based target systems on page 15
- Creating a synchronization project for initial synchronization of a Unix host on page 18
- Configuration parameters for managing Unix-based target systems on page 143
- Default project template for Unix-based target systems on page 146

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	You must provide a user account with the following permissions for

User	Permissions
the Unix host	full synchronization of a Unix-based target system with the supplied One Identity Manager default configuration. • Permissions for establishing a Secure Shell (SSH) connection to the host. • Administration permission for running write operation in the Unix objects.
One Identity Manager Service user account	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires permissions for the internal web service. NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to run synchronization using an application server.

Configuring Unix the host

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

Setting up a synchronization server for Unix-based target systems

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

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

Detailed information about this topic

- System requirements for the Unix synchronization server on page 15
- Installing One Identity Manager Service with a Unix or AIX connector on page 15

System requirements for the Unix synchronization server

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

- Windows operating system

  The following versions are supported:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework Version 4.7.2 or later

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

Installing One Identity Manager Service with a Unix or AIX connector

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

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

Table 3: Properties of the Job server

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

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

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

- Sets up a Job server.
- Specifies machine roles and server function for the Job server.
- 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: The program performs a remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

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*.

> 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*.

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

     Syntax:

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

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

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

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

   - For a direct connection to the database:
     1. Select **Process collection > sqlprovider**.
     2. Click the **Connection parameter** entry, then click the **Edit** button.
     3. Enter the connection data for the One Identity Manager database.
   - For a connection to the application server:
     1. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
     2. Click the **Connection parameter** entry, then click the **Edit** button.
     3. Enter the connection data for the application server.
     4. Click the **Authentication data** entry and click the **Edit** button.
     5. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For

detailed information about 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. Change the directory if necessary.
10. If the database is encrypted, on the **Select private key file** page, select the file with the private key.
11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Enter the name or IP address of the server that the service is installed and started on.
    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.
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 19
- Creating an initial synchronization project for a Unix host on page 21
- Default project template for Unix-based target systems on page 146
- Unix connector settings on page 147

Information required for setting up a synchronization project

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

Table 4: Information required to set up a synchronization project

Data	Explanation
Server name or IP address of the host	Full name or IP address of the host for connecting to the synchronization server to provide access to Unix objects.
Host communications port	Communications port for establishing a Secure Shell (SSH) connection to the host. The default port is TCP port 22.
Authentication	The login data required depends on which authentication method you select. - Authentication method **Password**: User account and password to log in to the host. This user account is used to access the host by SSH. The user account requires permissions for establishing an SSH connection. - Authentication method **Private key**: File with the private key and the passphrase.
Method, user name and password for escalating permissions	Running commands requires an administrative context. Make a user account available with sufficient permissions. This user account is used to perform write operations on the Unix objects. Available methods are: - **Default**: The user who logs in to the host already has administrative permissions. - **Sudo**: The user logged in on the host can run 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.

Data	Explanation
Synchronization server of the Unix-based target system	All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The One Identity Manager Service must be installed on the synchronization server with the Unix connector. The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server. • Server function: **Unix connector or AIX connector** • Machine role: **Server | Jobserver | Unix**
One Identity Manager database connection data	• Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with 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. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed • Unix connector or AIX connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the **RemoteCon-**

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

Related topics

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

Creating an initial synchronization project for a Unix host

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

- Run in default mode
- Started from the Launchpad

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

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

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

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

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

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

   This starts the Synchronization Editor's project wizard.

3. On the **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. Select the authentication method. Depending on the method you choose, enter the other information for authentication.

        - For the **Password** authentication method, enter the user account and password for SSH login to the host.

        - For the **Private key** authentication method, you need the private key and the passphrase.

    d. Click **Test** to test the connection. The system tries to establish a connection to the host.

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 name** field, enter an alternative user, such as **root**.

    - If administrative tasks should be run using a different user, select the **su** method. In the **User** and **Password** fields, enter the login data of the other user. The default user is **root**.

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

10. On the **Synchronization server** page, select the synchronization server to run the 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 Job server for the target system in the One Identity Manager database.

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

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

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

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

> NOTE:
>
> - If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.
>
>   Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor‘s start page, click **Verify project**.
> - If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically option**. In this case, save the synchronization project manually before closing the Synchronization Editor.
> - The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

Related topics

- Information required for setting up a synchronization project on page 19
- Users and permissions for synchronizing with a Unix-based target system on page 13
- Setting up a synchronization server for Unix-based target systems on page 15
- Configuring the synchronization log on page 24
- Customizing the synchronization configuration on page 25
- Tasks following synchronization on page 38
- Default project template for Unix-based target systems on page 146
- Unix connector settings on page 147

Configuring the synchronization log

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

To configure the content of the synchronization log

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

   - OR -

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

2. Select the **General** view and click **Configure**.
3. Select the **Synchronization log** view and set **Create synchronization log**.
4. Enable the data to be logged.

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

5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- Displaying synchronization results on page 36

Customizing the synchronization configuration

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

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

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.
- Use variables to set up a synchronization project for synchronizing different hosts. Store a connection parameter as a variable for logging onto the hosts.
- To specify which Unix objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.

- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

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

Detailed information about this topic

- Configuring Unix host synchronization on page 26
- Configuring synchronization of several Unix hosts on page 27
- Changing system connection settings of Unix hosts on page 27
- Updating schemas on page 30
- Configuring the provisioning of memberships on page 31
- Configuring single object synchronization on page 32
- Accelerating provisioning and single object synchronization on page 33

Configuring Unix host synchronization

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

To create a synchronization configuration for synchronizing a Unix host

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

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

Detailed information about this topic

- Configuring synchronization of several Unix hosts on page 27

Configuring synchronization of several Unix hosts

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

Prerequisites

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

To customize a synchronization project for synchronizing another host

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

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

Related topics

- Configuring Unix host synchronization on page 26

Changing system connection settings of Unix hosts

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

a. Specify a specialized variable set and change the values of the affected variables.

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).

b. Edit the target system connection with the system connection wizard and change the effected values.

   The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- Editing connection parameters in the variable set on page 28
- Editing target system connection properties on page 29
- Unix connector settings on page 147

Editing connection parameters in the variable set

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

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

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.

   Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.

   All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on + in the variable set view's toolbar.
   - To rename the variable set, select the variable set and click the variable set view in the toolbar 🏷. Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.

12. Select the **Configuration > Base objects** category.
13. Select the base object and click ✎.

    - OR -

    To add a new base object, click ⊞ .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

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

Related topics

- Editing target system connection properties on page 29

Editing target system connection properties

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

> NOTE: In the following circumstances, the default values cannot be restored:
>
> - The connection parameters are not defined as variables.
> - The default variable set is selected as an active variable set.
>
> In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit connection parameters using the system connection wizard

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

    > NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection.**

    This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- Editing connection parameters in the variable set on page 28

Updating schemas

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

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

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

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

To update a system connection schema

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

   - OR -

   Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

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

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

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

Configuring the provisioning of memberships

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

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

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

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

To allow separate provisioning of memberships

1. In the Manager, select the **Unix > Basic configuration data > Target system types** category.
2. In the result list, select the **Unix** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.

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

6. Save the changes.

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

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

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

To restore the original condition

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

> NOTE: To create the reference to the added or deleted assignments in the condition, use the `i` table alias.
>
> Example of a condition on the `UNXAccountInUNXGroup` assignment table:
>
> ```
> exists (select top 1 1 from UNXGroup g
>      where g.UID_UNXGroup = i.UID_UNXGroup
>      and <limiting condition>)
> ```

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

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

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

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

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

1. In the Manager, select the **Unix > Basic configuration data > Target system types** category.
2. In the result list, select the **Unix** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

   Example: `FK(UID_UNXHost).XObjectKey`
8. Save the changes.

Related topics

- Synchronizing single objects on page 37
- Post-processing outstanding objects on page 38

Accelerating provisioning and single object synchronization

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

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

To configure load balancing

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

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

2. In the Synchronization Editor, assign a custom server function to the base object.

   This server function is used to identify all the Job servers being used for load balancing.

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

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

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

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- Job server for Unix-specific process handling on page 137

Running synchronization

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

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

Detailed information about this topic

- Starting synchronization on page 35
- Deactivating synchronization on page 36

- Displaying synchronization results on page 36
- Synchronizing single objects on page 37

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

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

Deactivating synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

1. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of a Unix host on page 18

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

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

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

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

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

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

Related topics

- Configuring the synchronization log on page 24
- Troubleshooting on page 41

Synchronizing single objects

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

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

To synchronize a single object

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

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

Features of synchronizing memberships

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

Example:

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

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

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

Detailed information about this topic

- Configuring single object synchronization on page 32

Tasks following synchronization

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

- Post-processing outstanding objects on page 38
- Adding custom tables to the target system synchronization on page 40
- Managing Unix user accounts through account definitions on page 41

Post-processing outstanding objects

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

Outstanding objects:

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

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

Start target system synchronization to do this.

To post-process outstanding objects

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

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

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

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

   - The synchronization log has already been deleted.

     - OR -

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

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

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

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

   > TIP:
   >
   > ***To display object properties of an outstanding object***
   >
   > 1. Select the object on the target system synchronization form.
   > 2. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.

4. Click on one of the following icons in the form toolbar to run the respective method.

Table 6: Methods for handling outstanding objects

Icon	Method	Description
✕	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
➔	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object.

Icon	Method	Description
		Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

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

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

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

Adding custom tables to the target system synchronization

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

To add custom tables to target system synchronization

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

Related topics

- Post-processing outstanding objects on page 38

Managing Unix user accounts through account definitions

In the default installation, after synchronizing, employees are automatically created for the user accounts.If an account definition for the host is not known at the time of synchronization, user accounts are linked with 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 manage user accounts through account definitions

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

Related topics

- Account definitions for Unix user accounts on page 45

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

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

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

- Logging messages

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

- Reset start information

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

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

Related topics

- Displaying synchronization results on page 36

Ignoring data error in synchronization

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

To ignoring data errors during synchronization in One Identity Manager

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

   This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

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

   Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.
5. Save the changes.

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

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

Managing Unix user accounts and employees

The main feature of One Identity Manager is to map employees together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to 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 main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

For more information about employee handling and administration, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Account definitions for Unix user accounts on page 45
- Assigning employees automatically to Unix user accounts on page 66
- Specifying deferred deletion for Unix user accounts on page 77
- Creating and editing Unix user accounts on page 113

Account definitions for Unix user accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees. 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 employees must have 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.

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.

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

The following steps are required to implement an account definition:

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

Detailed information about this topic

- Creating account definitions on page 46
- Editing account definitions on page 46
- Main data for an account definition on page 47
- Editing manage levels on page 49
- Creating manage levels on page 50
- Main data for manage levels on page 51
- Creating mapping rules for IT operating data on page 52
- Entering IT operating data on page 54
- Modify IT operating data on page 55
- Assigning account definitions to employees on page 56
- Assigning account definitions to Unix hosts on page 63
- Deleting account definitions on page 63

Creating account definitions

To create a new account definition

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

Detailed information about this topic

- Main data for an account definition on page 47

Editing account definitions

To edit an account definition

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

4. Enter the account definition's main data.
5. Save the changes.

Related topics

- Main data for an account definition on page 47
- Creating account definitions on page 46
- Assigning manage levels to account definitions on page 51

Main data for an account definition

Enter the following data for an account definition:

Table 7: Main data for an account definition

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

Property	Description
	by an employee through the Web Portal and distributed using a defined approval process. The resource 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 requested by an employee through the Web Portal and distributed using a defined approval process. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is automatically assigned to all internal employees. To automatically assign the account definition to all internal employee, use the **Enable automatic assignment to employees** The account definition is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this account definition. To automatically remove the account definition assignment from all employees, use the **Disable automatic assignment to employees**. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily deactivated employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.

Property	Description
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

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

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

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

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

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

To edit a manage level

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

Related topics

- Main data for manage levels on page 51
- Creating manage levels on page 50
- Assigning manage levels to account definitions on page 51

Creating manage levels

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

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

To create a manage level

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

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

Related topics

- Main data for manage levels on page 51
- Editing account definitions on page 46
- Assigning manage levels to account definitions on page 51

Assigning manage levels to account definitions

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

To assign manage levels to an account definition

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

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

5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 8: Main data for manage levels

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

Property	Description
	- **Never**: Data is not updated. (Default) - **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 deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the 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.
4. Click **Add** and enter the following information:
   - **Column**: User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
   - **Source**: Specifies which roles to use in order to find the user account properties. You have the following options:
     - Primary department
     - Primary location
     - Primary cost center
     - Primary business roles

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

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

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

Related topics

- Entering IT operating data on page 54

Entering 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.In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

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

To define IT operating data

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

     To specify an application scope

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

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

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

4. Save the changes.

Related topics

- Creating mapping rules for IT operating data on page 52

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, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

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

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

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

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

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

Assigning account definitions to 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.

> 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 account definition assignment is removed, the user account that was created from this account definition, is deleted.

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).

To configure assignments to roles of a role class

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

   - OR -

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

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

For 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 57
- Assigning account definitions to business roles on page 58
- Assigning account definitions to all employees on page 58
- Assigning account definitions directly to employees on page 59
- Assigning account definitions to system roles on page 60
- Adding account definitions to the IT Shop on page 60

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 account definitions to business roles on page 58
- Assigning account definitions to all employees on page 58
- Assigning account definitions directly to employees on page 59
- Assigning account definitions to system roles on page 60
- Adding account definitions to the IT Shop on page 60

Assigning account definitions to business roles

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

To add account definitions to hierarchical roles

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

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 57
- Assigning account definitions to all employees on page 58
- Assigning account definitions directly to employees on page 59
- Assigning account definitions to system roles on page 60
- Adding account definitions to the IT Shop on page 60

Assigning account definitions to all employees

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

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

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 main data** task.
4. Select the **Disable automatic assignment to employees** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all employees, run the DISABLE AUTOMATIC ASSIGNMENT TO EMPLOYEES task. 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 57
- Assigning account definitions to business roles on page 58
- Assigning account definitions directly to employees on page 59
- Assigning account definitions to system roles on page 60
- Adding account definitions to the IT Shop on page 60

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 57
- Assigning account definitions to business roles on page 58
- Assigning account definitions to all employees on page 58
- Assigning account definitions to system roles on page 60
- Adding account definitions to the IT Shop on page 60

Assigning account definitions to system roles

> NOTE: This function is only available if the System Roles Module is installed.
>
> 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 57
- Assigning account definitions to business roles on page 58
- Assigning account definitions to all employees on page 58
- Assigning account definitions directly to employees on page 59
- Adding account definitions to the IT Shop on page 60

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 (role-based login)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related topics

- Main data for an account definition on page 47
- Assigning account definitions to departments, cost centers, and locations on page 57
- Assigning account definitions to business roles on page 58
- Assigning account definitions to all employees on page 58

- Assigning account definitions directly to employees on page 59
- Assigning account definitions to system roles on page 60

Assigning account definitions to Unix hosts

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 main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Detailed information about this topic

- Assigning employees automatically to Unix user accounts on page 66

Deleting account definitions

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 main data** task.
   d. Select the **Disable automatic assignment to employees** task.

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

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

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

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

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

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

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

b. Select an account definition in the result list.

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

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

e. Click **OK**.

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

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

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

    b. Select an account definition in the result list.

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

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

    e. Save the changes.

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

    a. In the Manager, select the host in the **Unix > Hosts** category.

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

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

    d. Save the changes.

8. Delete the account definition.

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

    b. Select an account definition in the result list.

    c. Click to delete an account definition.

Assigning employees automatically to Unix user accounts

When you add a user account, an existing employee can automatically be assigned to it. If necessary, a new employee can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either manually or through synchronization.After synchronization, identities are automatically assigned to all new user accounts. If no matching identity can be found, a new identity is created using existing user main data.

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 main data** to assign employees to administrative user accounts for the respective user account.

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

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, define the user accounts for which no automatic assignment to employees shall take place.

  Example:

  ```
  ROOT
  ```

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

To edit the exclude list for automatic employee assignment

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

   This opens the **Exclude list for Unix user accounts** dialog.
3. To add a new entry, click **Add**.

   To edit an entry, select it and click **Edit**.
4. Enter the name of the user account that does not allow employees to be assigned automatically.

   Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.
5. To delete an entry, select it and click **Delete**.
6. Click **OK**.

- Use the **TargetSystem | Unix | PersonAutoDisabledAccounts** configuration parameter to specify whether 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:

In the default installation, after synchronizing, employees are automatically created for the user accounts.If an account definition for the host is not known at the time of synchronization, user accounts are linked with 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.

For more information, see Managing Unix user accounts through account definitions on page 41.

Related topics

- Creating account definitions on page 46
- Assigning account definitions to Unix hosts on page 63

- Changing manage levels for Unix user accounts on page 71
- Editing search criteria for automatic employee assignment on page 68

Editing search criteria for automatic employee assignment

> 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.

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

To specify criteria for employee assignment

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

Table 9: 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`)

5. Save the changes.

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

Related topics

- Finding employees and directly assigning them to user accounts on page 69
- Assigning employees automatically to Unix user accounts on page 66

Finding employees and directly assigning them to user accounts

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

Table 10: 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.

To apply search criteria to user accounts

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

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

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

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

To assign employees directly over a suggestion list

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

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

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

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

To remove assignments

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

     The assigned employees are removed from the selected user accounts.

Changing manage levels for Unix user accounts

The default manage level is applied if you create user accounts using automatic 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 main data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Related topics

- Creating and editing Unix user accounts on page 113

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 11: 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 with other functional areas.	Organizational

Identity	Description	Value of the IdentityType column
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by 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, shared identity, or service identity are linked to pseudo employees that do not refer to a real employee. These pseudo employees are needed so that permissions can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether pseudo employees need to be considered separately.

For more 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 73
- Administrative user accounts on page 73
- Providing administrative user accounts for one employee on page 74
- Providing administrative user accounts for several employees on page 75
- Privileged user accounts on page 76

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 IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

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

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

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

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

Related topics

- Account definitions for Unix user accounts on page 45

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 74
- Providing administrative user accounts for several employees on page 75

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 main 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 main 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 75
- For more 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 pseudo employee must exist. The pseudo 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 main data** task.
   d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to a pseudo employee.
   a. In the Manager, select the **Unix > User accounts** category.
   b. Select the user account in the result list.
   c. Select the **Change main data** task.
   d. On the **General** tab, select the pseudo employee from the **Employee** menu.

      > TIP: If you are the target system manager, you can choose + to create a new pseudo 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 74
- 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 IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

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

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

default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.

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

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

6. Assign the account definition directly to 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, specify how the login names are formatted in the template.
>
> - To use a prefix for the login name, in the Designer, set the **TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName_Prefix** configuration parameter.
> - To use a postfix for the login name, in the Designer, set the **TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName_Postfix** configuration parameter.
>
> These configuration parameters are evaluated in the default installation, if a user account is marked with the **Privileged user account** property (`IsPrivilegedAccount` column). The user account login names are renamed according to the formatting rules. This also occurs if the user accounts are labeled as privileged using the **Mark selected user accounts as privileged** schedule. If necessary, modify the schedule in the Designer.

Related topics

- Account definitions for Unix user accounts on page 45

Specifying deferred deletion for Unix user accounts

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

You have the following options for configuring deferred deletion.

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

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

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

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

Example:

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

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

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

4

Managing memberships in Unix groups

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

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

Detailed information about this topic

- Assigning Unix groups to Unix user accounts on page 79
- Effectiveness of membership in Unix user groups on page 88
- Unix group inheritance based on categories on page 90
- Overview of all assignments on page 92

Assigning Unix groups to Unix user accounts

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

In the case of indirect assignment, employees and Unix groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. The Unix 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 Unix user account, the Unix user account is added to the Unix group.

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

Through system roles, Unix groups can be grouped together and assigned to employees and workdesks as a package. You can create system roles that contain only Unix groups. You can also group any number of company resources into a system role.

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

For detailed information see the following guides:

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

Detailed information about this topic

- Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 80
- Assigning Unix groups to departments, cost centers and locations on page 81
- Assigning Unix groups to business roles on page 83
- Adding Unix groups to system roles on page 84
- Adding Unix groups to the IT Shop on page 84
- Assigning Unix user accounts directly to Unix groups on page 86
- Assigning Unix groups directly to Unix user accounts on page 87

Prerequisites for indirect assignment of Unix groups to Unix user accounts

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

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

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

To configure assignments to roles of a role class

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

      - OR -

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

   b. Select the **Configure role assignments** task and configure the permitted assignments.

      - To generally allow an assignment, enable the **Assignments allowed** column.
      - To allow direct assignment, enable the **Direct assignments permitted** column.

   c. Save the changes.

2. Settings for assigning Unix groups to Unix user accounts.

   - The Unix user account is linked to an employee.
   - The Unix user account is labeled with the **Groups can be inherited** option.

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

Related topics

- Creating and editing Unix user accounts on page 113
- General main data of Unix user accounts on page 114

Assigning Unix groups to departments, cost centers and locations

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

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

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

4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

5. Save the changes.

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

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

   - OR -

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

   - OR -

   In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign Unix groups** task.
4. In the **Add assignments** pane, assign groups.

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

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 80
- Assigning Unix groups to business roles on page 83
- Adding Unix groups to system roles on page 84
- Adding Unix groups to the IT Shop on page 84
- Assigning Unix user accounts directly to Unix groups on page 86
- Assigning Unix groups directly to Unix user accounts on page 87
- One Identity Manager users for managing Unix-based target systems on page 9

Assigning Unix groups to business roles

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

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

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

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

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

5. Save the changes.

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

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

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

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 80
- Assigning Unix groups to departments, cost centers and locations on page 81
- Adding Unix groups to system roles on page 84
- Adding Unix groups to the IT Shop on page 84
- Assigning Unix user accounts directly to Unix groups on page 86
- Assigning Unix groups directly to Unix user accounts on page 87
- One Identity Manager users for managing Unix-based target systems on page 9

Adding Unix groups to system roles

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

Use this task to add a group to system roles.

If you assign a system role to employees, all Unix user accounts owned by this employee inherit the group.

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

To assign a group to system roles

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

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

   To remove an assignment

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

Related topics

- Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 80
- Assigning Unix groups to departments, cost centers and locations on page 81
- Assigning Unix groups to business roles on page 83
- Adding Unix groups to the IT Shop on page 84
- Assigning Unix user accounts directly to Unix groups on page 86
- Assigning Unix groups directly to Unix user accounts on page 87

Adding Unix groups to the IT Shop

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

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

- If you want the group to be assigned only to 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. In the Manager, select the **Unix > Groups** (non role-based login) category.

   - OR -

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

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

Related topics

- Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 80
- General main data for Unix groups on page 126
- Removing Unix groups from an IT Shop shelf on page 85
- Removing Unix groups from all IT Shop shelves on page 86
- One Identity Manager users for managing Unix-based target systems on page 9

Removing Unix groups from an IT Shop shelf

To remove a group from individual IT Shop shelves

1. In the Manager, select the **Unix > Groups** (non role-based login) category.

   - OR -

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

Related topics

- Removing Unix groups from all IT Shop shelves on page 86

Removing Unix groups from all IT Shop shelves

To remove a group from all IT Shop shelves

1. In the Manager, select the **Unix > Groups** (non role-based login) category.

   - OR -

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

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

Related topics

- Removing Unix groups from an IT Shop shelf on page 85

Assigning Unix user accounts directly to Unix groups

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is done by allocating the employee and groups into company structures such as departments, cost centers, locations, or business roles. If the employee has a user account in 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. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign user accounts directly to a group

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

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

To remove an assignment

- Select the user account and double-click ✓.

5. Save the changes.

Related topics

- Assigning Unix groups directly to Unix user accounts on page 87
- Assigning Unix groups to departments, cost centers and locations on page 81
- Assigning Unix groups to business roles on page 83
- Adding Unix groups to system roles on page 84
- Adding Unix groups to the IT Shop on page 84

Assigning Unix groups directly to Unix user accounts

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. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign groups directly to user accounts

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

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

   To remove an assignment

   - Select the group and double-click ✓.

5. Save the changes.

Related topics

- Assigning Unix groups to Unix user accounts on page 79

Effectiveness of membership in Unix user groups

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: 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 12: Specifying excluded groups (`UNXGroupExclusion` table)

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

Table 13: 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 14: Excluded groups and effective assignments

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

Prerequisites

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

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

  > NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of

> preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive groups belong to the same host.

To exclude a group

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 no longer mutually exclusive.
5. Save the changes.

Unix group inheritance based on categories

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

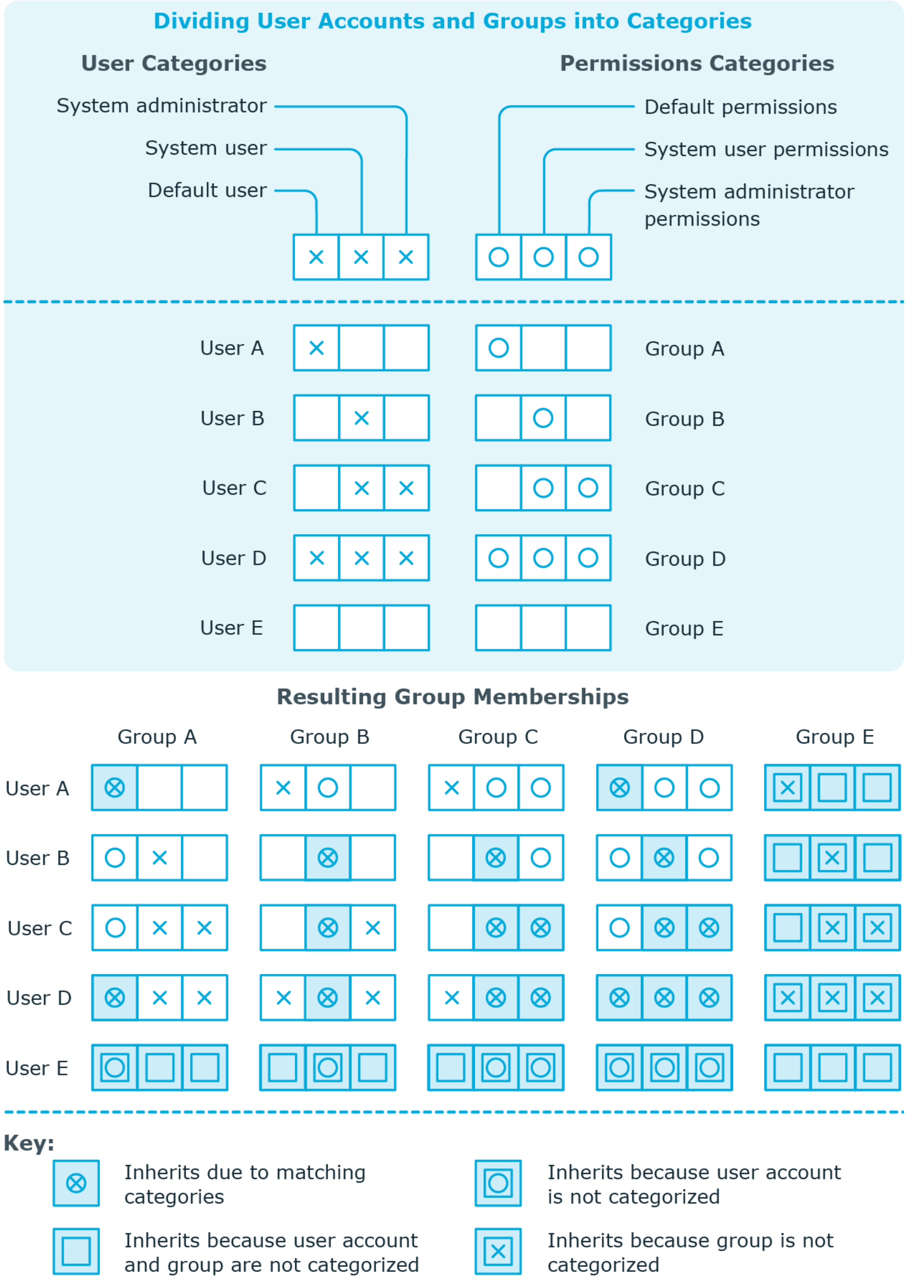
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or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

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

Table 15: 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.



	Default user	System user	System administrator
User A	×		
User B		×	
User C		×	×
User D	×	×	×
User E			

	Default permissions	System user permissions	System administrator permissions
Group A	○		
Group B		○	
Group C		○	○
Group D	○	○	○
Group E			

	Group A			Group B			Group C			Group D			Group E		
User A	⊗			×	○		×	○	○	⊗	○	○	☒	□	□
User B	○	×			⊗			⊗	○	○	⊗	○	□	☒	□
User C	○	×	×		⊗	×		⊗	⊗	○	⊗	⊗	□	☒	☒
User D	⊗	×	×	×	⊗	×	×	⊗	⊗	⊗	⊗	⊗	☒	☒	☒
User E	⧇	□	□	□	⧇	□	□	⧇	⧇	⧇	⧇	⧇	□	□	□

Key:

⊗ Inherits due to matching categories

⧇ Inherits because user account is not categorized

□ Inherits because user account and group are not categorized

☒ Inherits because group is not categorized

To use inheritance through categories

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

Related topics

- Defining categories for the inheritance of entitlements on page 110
- General main data of Unix user accounts on page 114
- General main data for Unix groups on page 126

Overview of all assignments

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

Examples:

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

To display detailed information about assignments

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

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

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

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

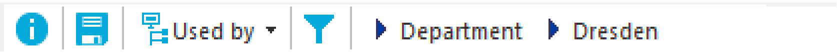


Table 16: Meaning of icons in the report toolbar

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

Login information for Unix user accounts

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

Detailed information about this topic

- Password policies for Unix user accounts on page 94
- Initial password for new Unix user accounts on page 106
- Email notifications about login data on page 106

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 polices apply not only when the user enters a password but also when random passwords are generated.

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

Detailed information about this topic

- Predefined password policies on page 95
- Using password policies on page 96
- Creating password policies on page 97
- Editing password policies on page 98

- Custom scripts for password requirements on page 102
- Password exclusion list on page 105
- Checking a password on page 105
- Testing password generation on page 106

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 8.2.1, the configuration parameter settings for forming passwords are passed on

> to the target system-specific password policies.

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

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

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

Using password policies

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

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

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

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

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

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

To reassign a password policy

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

      To specify an application scope

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

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

To change a password policy's assignment

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

Creating password policies

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

To create a password policy

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

Detailed information about this topic

- General main data for password policies on page 98
- Policy settings on page 101
- Character classes for passwords on page 99
- Custom scripts for password requirements on page 102
- Editing password policies on page 98

Editing password policies

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

To edit a password policy

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

Detailed information about this topic

- General main data for password policies on page 98
- Policy settings on page 101
- Character classes for passwords on page 99
- Custom scripts for password requirements on page 102
- Creating password policies on page 97

General main data for password policies

Enter the following main data of a password policy.

Table 17: main data for a password policy

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

Property	Meaning
Description	Text field for additional explanation. Translate the given text using the 🌐 button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the 🌐 button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. 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.

Character classes for passwords

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

Table 18: Character classes for passwords

Property	Meaning
Required number of character classes	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for **Min. number letters**, **Min. number lowercase**, **Min. number uppercase**, **Min. number digits**, and **Min. number special characters**. That means: • Value **0**: All character class rules must be fulfilled. • Value **>0**: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value **>0**. NOTE: Generated passwords are not tested for this.
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.	Specifies the minimum number of uppercase letters the password must

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

Policy settings

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

Table 19: 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. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into account. 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 exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.
Max. days valid	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then the password does not expire.
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. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3**

Property	Meaning
	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 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 information, see the *One Identity Manager Configuration Guide*.

Custom scripts for password requirements

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

Detailed information about this topic

- Checking passwords with a script on page 102
- Generating passwords with a script on page 104

Checking passwords with a script

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

Syntax of check scripts

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

With parameters:

`policy` = password policy object

`spwd` = password to check

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

Example: Script that checks a password

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

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

      Dim pwd = spwd.ToInsecureArray()

      If pwd.Length>0

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

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

            End If

      End If

      If pwd.Length>2

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

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

            End If

      End If

End Sub
```

To use a custom script for checking a password

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

Related topics

- Generating passwords with a script on page 104

Generating passwords with a script

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

Syntax for generating script

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

With parameters:

`policy` = password policy object

`spwd` = generated password

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

Example: Script that generates a password

The script replaces invalid **?** 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 main data** task.

d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.

e. Save the changes.

Related topics

- Checking passwords with a script on page 102

Password exclusion list

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

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

To add a term to the restricted list

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

Checking a password

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

To verify if a password conforms to the password policy

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

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

Testing password generation

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

To generate a password that conforms to the password policy

1. In the Manager, select the **Unix > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new Unix user accounts

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

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

Related topics

- Password policies for Unix user accounts on page 94
- Email notifications about login data on page 106

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

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

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

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

6

Mapping of Unix objects in One Identity Manager

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

Detailed information about this topic

- Unix host on page 108
- Unix user accounts on page 112
- Unix groups on page 125

Unix host

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

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

To edit the main data for a Unix host

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

Related topics

- General main data of Unix hosts on page 109
- Defining categories for the inheritance of entitlements on page 110
- Editing the synchronization project for a Unix host on page 111
- Displaying the Unix hosts overview on page 111
- Displaying Unix login shells on page 112
- Synchronizing single objects on page 37

General main data of Unix hosts

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

Table 20: General main data for a host

Property	Description
Host name	Name of the host.
Primary group	User account's primary group. This group is used as primary group when creating a user account.
Device	The computer is connected to this device. Specify a new device using the + button next to the menu.
AIX system	Specifies whether this host is an IBM AIX system. The following properties are offered additionally for user accounts on IBM AIX systems.
Account definition (initial)	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. User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role, in which target system managers are specified for the 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. 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.
Synchronized by	Type of synchronization through which the data is synchronized between the host and One Identity Manager. As soon as objects for this host are available in One Identity Manager, the type of synchronization can no

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>longer be changed.
If you create a host with the Synchronization Editor, <b>One Identity Manager</b> is used.
<b>Table 21: Permitted values</b>
<table>
<tr><th>Value</th><th>Synchronization by</th><th>Provisioned by</th></tr>
<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>
</table>
NOTE: If you select <b>No synchronization</b>, you can define custom processes to exchange data between One Identity Manager and the target system.</td></tr>
<tr><td>Operating system description</td><td>Description of the operating system.</td></tr>
<tr><td>Distribution</td><td>Installed distribution of the operating system.</td></tr>
<tr><td>Distribution version</td><td>Version of the installed distribution.</td></tr>
<tr><td>Kernel version</td><td>Current version of the kernel.</td></tr>
<tr><td>Operating system type</td><td>Type of operating system, such as Linux, AIX, or UNIX.</td></tr>
</table>

Defining categories for the inheritance of entitlements

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

To define a category

1. In the Manager, select the host in the **Unix > Hosts** category.
2. Select the **Change main data** task.

3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. To enable the category, double-click ⊗.
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- Unix group inheritance based on categories on page 90

Editing the synchronization project for a Unix host

Synchronization projects in which a host is already used as a base object can also be opened in the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

> NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

1. In the Manager, select the **Unix > Hosts** category.
2. Select the host in the result list. Select the **Change main data** task.
3. Select the **Edit synchronization project** task.

Related topics

- Customizing the synchronization configuration on page 25

Displaying the Unix hosts overview

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

To obtain an overview of a host

1. In the Manager, select the **Unix > Hosts** category.
2. Select the host in the result list.
3. Select **Unix host overview**.

Displaying Unix login shells

This information about a host's login shells is loaded into One Identity Manager and cannot be edited. You can use login shells when setting up user accounts.

To display login shells

1. In the Manager, select the **Unix > Hosts > <host name> > Login shells** category.
2. Select the login shell in the result list.
3. Select the **Unix login shell overview** task.

Related topics

- Creating mapping rules for IT operating data on page 52
- General main data of Unix user accounts on page 114

Unix user accounts

You can use One Identity Manager to manage your local Unix-based target system user accounts. User accounts obtain the required access permissions to the resources through membership in groups.

Detailed information about this topic

- Managing Unix user accounts and employees on page 44
- Managing memberships in Unix groups on page 79
- Creating and editing Unix user accounts on page 113
- General main data of Unix user accounts on page 114
- User account main data for AIX systems on page 117
- Assigning extended properties to Unix user accounts on page 122
- Deleting and restoring Unix user accounts on page 124
- Disabling AIX system user accounts on page 123
- Displaying the Unix user account overview on page 125
- Synchronizing single objects on page 37

Creating and editing 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 main data described in the following is mapped through templates from employee main 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 main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

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

To manually assign a user account for an employee

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

Detailed information about this topic

- General main data of Unix user accounts on page 114
- User account main data for AIX systems on page 117

Related topics

- Account definitions for Unix user accounts on page 45
- Supported user account types on page 71

- Managing Unix user accounts and employees on page 44

General main data of Unix user accounts

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

Table 22: Additional main data of a user account

Property	Description
Host	The user account's host.
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click + next to the input field and enter the required employee main data. Which login data is required depends on the selected identity type.
No link to an employee required	Specifies whether the user account is intentionally not assigned an employee. The option is automatically set if a user account is included in the exclusion list for automatic employee assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an employee (for example, if several employees use the user account). If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an employee can be filtered according to various criteria.
Not linked to an employee	Indicates why the **No link to an employee required** option is enabled for this user account. Possible values: • **By administrator**: The option was set manually by the administrator. • **By attestation**: The user account was attested. • **By exclusion criterion**: The user account is not associated with an employee due to an exclusion criterion. For example, the user account is included in the exclude list for automatic employee assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account main data and

Property	Description
	to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved. NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (`XOrigin=1`).
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Login shell	Shell that is run if a user logs in to Unix using a terminal-based login.
User name	Name of the user account for logging in to a Unix host. If an account definition is assigned, this field is automatically filled with the employee's central user account depending on the manage level.
User ID	User ID for the user account in the Unix host.
Password	Password for the user account. The employee’s central password can be mapped to the user account password. For detailed information about an employee’s central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
Password confirmation	Reconfirm password.
Primary group ID	Identifier of the user account's primary group.
Primary group	Name of the user account's primary group. This defines the group ownership of files created by the user. A user account's primary group is determined as follows: • If you entered a primary group in the host, the group is used as

Property	Description
	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 *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Comment (GECOS)	Text field for additional explanation. Additional information about the user account, which is found in the GECOS in `/etc/password`. If an account definition is assigned, this field is automatically filled with the employee's internal name depending on the manage level.
Identity	User account's identity type Permitted values are: - **Primary identity**: Employee's default user account. - **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. - **Personalized administrator identity**: User account with administrative permissions, used by one employee. - **Sponsored identity**: User account to use for a specific purpose. Training, for example. - **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this user account. - **Service identity**: Service account.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. - If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.

Property	Description
	- If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Privileged user account	Specifies whether this is a privileged user account.

Related topics

- Account definitions for Unix user accounts on page 45
- Assigning employees automatically to Unix user accounts on page 66
- Password policies for Unix user accounts on page 94
- Initial password for new Unix user accounts on page 106
- Unix group inheritance based on categories on page 90
- Supported user account types on page 71
- General main data of Unix hosts on page 109
- Disabling AIX system user accounts on page 123
- Prerequisites for indirect assignment of Unix groups to Unix user accounts on page 80

User account main data for AIX systems

You can enter additional main data of user accounts in an IBM AIX system, like limits, password data, security data or information about encrypting the file system. This data is shown if the host is labeled with the **AIX system** option.

Detailed information about this topic

- Limits for user accounts on page 117
- Password data for user accounts on page 119
- Security-relevant user account main data on page 120
- Main data for user accounts on an encrypted file system on page 121
- General main data of Unix hosts

Limits for user accounts

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 23: 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 `core`).
Core size (hart)	Absolute maximum limit for the size of the core dump file that can be created by a user process. (Parameter `core_hard`).
CPU time (soft)	Soft limit for the time (in seconds) a user process may take. (Parameter `cpu`).
CPU time (hard)	Maximum amount of time (in seconds) the user process may take. (Parameter `cpu_hard`).
Data size (soft)	Soft limit for the size of the process' data segment for a user process. (Parameter `data`).
Data size (hard)	Maximum size of a process' data segment for a user process. (Parameter `data_hard`).
File size (soft)	Soft limit for the size of a file a user process can create or extend. (Parameter `fsize`).
File size (hard)	Absolute maximum size of a file a user process can create or extend. (Parameter `fsize_hard`).
Memory size (soft)	Soft limit for the maximum amount of physical memory a user process can take up. (Parameter `rss`).
Memory size (hard)	Maximum amount of physical memory a user process can take up. (Parameter `rss_hard`).
Stack size (soft)	Soft limit for the size of the process' stack segment for a user process. (Parameter `stack`).
Stack size (hard)	Maximum size of a process' stack segment for a user process. (Parameter `stack_hard`).
File descriptors (soft)	Soft limit for the number of file descriptors a user process can have open at the same time. (Parameter `nofiles`).
File descriptors (hard)	Absolute maximum number of file descriptors a user process can have open at the same time. (Parameter `nofiles_hard`).
Threads (soft)	Soft limit for the number of threads per process. (Parameter `threads`).
Threads (hard)	Absolute maximum number of threads per process. (Parameter `threads_hard`).
Processes	Soft limit for the number of processes per user. (Parameter `nproc`).

Property	Description
(soft)	
Processes (hard)	Absolute maximum for the number of processes per user. (Parameter `nproc_hard`).

Password data for user accounts

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

Table 24: 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 the password must contain. (Parameter `minalpha`).
minloweralpha	Specifies the minimum number of lowercase letters the password must contain. (Parameter `minloweralpha`).
minupperalpha	Specifies the minimum number of uppercase letters the password must contain. (Parameter `minupperalpha`).
mindigit	Specifies the minimum number of digits the password must contain. (Parameter `mindigit`).
minspecialchar	Specifies the minimum number of special characters the password must contain. (Parameter `minspecialchar`).
minother	Specifies the minimum number of non-alphabetical characters a new password must contain. (Parameter `minother`).
dictionlist	Dictionary file of passwords that are not allowed. (Parameter `dictionlist`).
histexpire	Number of weeks before a password can be reused. (Parameter `histexpire`).
histsize	Number of password iterations allowed before an old password can be used again. (Parameter `histsize`).

Property	Description
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 main 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 25: 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	Specifies the administrative status of the user. (Parameter `admin`).
admgroups	Lists the groups the user administrates. (Parameter `admgroups`).
auditclasses	The user account's audit classes. (Parameter `auditclasses`).
auth1	Additional mandatory methods for authenticating the user. (Parameter `auth1`).
auth2	Additional optional methods for authenticating the user. (Parameter `auth2`).
core_ compress	Enables or disables core file compression. (Parameter `core_compress`).
core_path	Enables or disables core file path specification. (Parameter `core_path`). If this attribute has a value of On, core files will be placed in the given directory. otherwise, core files are placed in the user's current working directory.
core_ naming	Naming conventions for the core file. If this option is set, the core file is stamped with a process ID, time, and date. (Parameter `core_naming`).
daemon	Specifies whether the user can run programs using the cron daemon or the

Property	Description
	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	Specifies whether access is permitted to the account from a remote location with the `telnet` or `rlogin` commands. (Parameter `rlogin`).
su	Specifies whether another user can switch to the specified user account with the `su` command. (Parameter `su`).
sugroups	Groups that can use the `su` command to switch to the specified user. (Parameter `sugroups`).
SYSTEM	System's authentication mechanism for the user. (Parameter `SYSTEM`).
tpath	The user's trusted path status. (Parameter `tpath`).
ttys	Lists the terminals that can access the user. (Parameter `ttys`).
umask	Determines file permissions. (Parameter `umask`). The default value is 022.

Related topics

- Disabling AIX system user accounts on page 123

Main data for user accounts 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 26: User account main data of encrypted file systems

Property	Description
efs_adminks_access	Defines the `efs_admin` keystore location (Parameter `efs_adminks_access`). Permitted values: • file • ldap
efs_allowksmodechangebyuser	Specifies whether the user can change the mode or not. (Parameter `efs_allowksmodechangebyuser`).
efs_file_algo	Algorithm used to generate the file protection key. (Parameter `efs_file_algo`). Permitted values: • AES_128_CBC • AES_192_CBC • AES_256_CBC
efs_initialks_mode	Initial mode of the user keystore. (Parameter `efs_initialks_mode`). Permitted values: • guard • admin
efs_keystore_access	User keystore location. (Parameter `efs_keystore_access`). Permitted values: • none • file
efs_keystore_algo	Algorithm used to generate the user private key when the keystore is created. (Parameter `efs_keystore_algo`). Permitted values: • RSA_1024 • RSA_2048 • RSA_4096

Assigning extended properties to Unix user accounts

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

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

To specify extended properties for a user account

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

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

5. Save the changes.

Disabling AIX system user accounts

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

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

Scenario:

The user 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 main 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 main data** task.
4. On the **Security** tab, set the **account_locked** option.
5. Save the changes.

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

Related topics

- Account definitions for Unix user accounts on page 45
- Creating manage levels on page 50
- Deleting and restoring Unix user accounts on page 124

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 account definition assignment is removed, the user account that was created from this account definition, is deleted.

You can delete a user account that was not created using an account definition through the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

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

To delete a user account that is not managed using an account definition

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.

3. Click in the result list.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.

Related topics

- Disabling AIX system user accounts on page 123
- Specifying deferred deletion for Unix user accounts on page 77

Displaying the Unix user account overview

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

To obtain an overview of a user account

1. In the Manager, select the **Unix > User accounts** category.
2. Select the user account in the result list.
3. Select the **Unix user account overview** task.

Unix groups

In the Unix host, user accounts can be gathered into groups that can be used to regulate access to resources. Local groups are loaded into One Identity Manager by synchronization. You can set up new groups or 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

- Managing memberships in Unix groups on page 79
- Editing main data of Unix groups on page 126
- General main data for Unix groups on page 126
- Adding Unix groups to Unix groups on page 127
- Assigning extended properties to Unix groups on page 128

- Displaying the Unix group overview on page 129
- Synchronizing single objects on page 37

Editing main data of Unix groups

To edit group main data

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Detailed information about this topic

- General main data for Unix groups on page 126

General main data for Unix groups

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

Table 27: General main data

Property	Description
Group name	Name of the group.
Group ID	Group's identifier.
Host	Group's host.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested 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.

Property	Description
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range **0** to **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 90
- For more detailed information about preparing groups for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Adding Unix groups to Unix groups

Use this task to add a group to another group. This means that the groups can be hierarchically structured.

To assign groups directly to a group as members

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** category.
4. Select the **Has members** tab.
5. Assign child groups in **Add assignments**.

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

6. Save the changes.

To add a group as a member of other groups

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** task.
4. Select the **Is member of** tab.

5. In the **Add assignments** pane, assign parent groups.

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

6. Save the changes.

Assigning extended properties to Unix groups

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

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

To specify extended properties for a group

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

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

5. Save the changes.

Deleting Unix groups

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

To delete a group

1. In the Manager, select the **Unix > Groups** category.
2. Select the group in the result list.
3. Click ☒ in the result list.
4. Confirm the security prompt with **Yes**.

Displaying the Unix group overview

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

To obtain an overview of a group

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

Reports about Unix objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for Unix-based target systems.

NOTE: Other sections may be available depending on the which modules are installed.

Table 28: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	group	This report finds all roles containing employees who have the selected system entitlement.
Show overview	group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	group	This report shows an overview of the system entitlement and including its history.

Report	Published for	Description
		Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show entitlement drifts	Host	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Host	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average number of system entitlements	Host	This report contains all user accounts with an above average number of system entitlements.
Show employees with multiple user accounts	Host	This report shows all the employees that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Host	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Host	This report finds all roles containing employees with at least one user account in the selected target system.
Show unused user accounts	Host	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Host	This report shows all user accounts to which no employee is assigned.

Table 29: Additional reports for the target system

Report	Description
Unix user account and group	This report contains a summary of user account and group distribution in all host systems. You can find this report in the **My**

Report	Description
administration	**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.

7

Handling of Unix objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and employees

  An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized person, such as a manager.

- Managing group assignments

  When a group is assigned to an IT Shop shelf, the group can be requested by the customers of the shop in the Web Portal. The request undergoes a defined approval process. The group is not assigned until it has been approved by an authorized person.

  In the Web Portal, managers and administrators of organizations can assign groups to the departments, cost centers, or locations for which they are responsible. The groups are passed on to all persons who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, managers, and administrators of business roles can assign groups in the Web Portal to the business roles for which they are responsible. The groups are passed on to all persons who are members of these business roles.

  If the System Roles Module is available, supervisors of system roles can assign groups to the system roles in the Web Portal. The groups are passed on to all persons to whom these system roles are assigned.

- Attestation

  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

  If the Compliance Rules Module is available, you can define rules that identify the invalid group memberships and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check and resolve rule violations and to grant exception approvals.

  If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

  You can use the risk index of groups to evaluate the risk of entitlement assignments for the company.One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the employees, user accounts, and their entitlements and risks.

For more information about the named topics, see Managing Unix user accounts and employees on page 44, Managing memberships in Unix groups on page 79, and the following guides:

- *One Identity Manager Web Designer Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

8

Basic data for Unix-based target systems

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

- Account definitions

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

  For more information, see Account definitions for Unix user accounts on page 45.

- Password policy

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

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

  For more information, see Password policies for Unix user accounts on page 94.

- Initial password for new user accounts

  You have the different options for issuing an initial password for user accounts. Enter a password or use a random generated initial password when you create a user account.

  For more information, see Initial password for new Unix user accounts on page 106.

- 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 106.

- Target system types

Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

For more information, see Post-processing outstanding objects on page 38.

- Target system managers

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

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

  For more information, see Target system managers on page 135.

- Servers

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

  For more information, see Job server for Unix-specific process handling on page 137.

Target system managers

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

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

For 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 30: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Unix** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have another 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 main data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

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

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

   b. Click **OK** to add the new application role.
6. Save the changes.
7. Assign 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 9
- General main data of Unix hosts on page 109

Job server for Unix-specific process handling

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

You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **Unix > Basic configuration data > Server** category and edit the Job server main data.

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

> NOTE: One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

To edit a Job server and its functions

1. In the Manager, select the **Unix > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.
4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- General main data for a Job server on page 138
- Server functions of a Job server on page 140

General main data for a Job server

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

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

Table 31: Job server properties

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

Property	Meaning
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 steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.

Property	Meaning
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the `QBM_PJobQueueLoad` procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
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 140

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 32: 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.
Generic database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization	Server for running synchronization with an SMB-based target system.

Server function	Remark
Server	
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.
Unix connector	This server can connect to a Unix system using SSH.
AIX connector	This server can connect to an AIX system using SSH.

Related topics

- General main data for a Job server on page 138

Appendix A

Configuration parameters for managing Unix-based target systems

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

Table 33: Configuration parameters

Configuration parameter	Description
TargetSystem | Unix	Preprocessor relevant configuration parameter to control component parts for Unix-based custom target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
TargetSystem | Unix | Accounts	Allows configuration of user account data.
TargetSystem | Unix | Accounts | InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | Unix | Accounts | InitialRandomPassword | SendTo	Employee to receive an email with the random generated password (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.

Configuration parameter	Description
TargetSystem | Unix | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Employee - new user account created** mail template is used.
TargetSystem | Unix | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem | Unix | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | Unix | Accounts | PrivilegedAccount	Allows configuration of privileged Unix user account settings.
TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName_Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName_Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem | Unix | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | Unix | MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem | Unix | PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | Unix | PersonAutoDisabledAccounts	Specifies whether employees are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem | Unix | PersonAutoFullSync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by

<table>
<tr><th>Configuration parameter</th><th>Description</th></tr>
<tr><td></td><td>synchronization.</td></tr>
<tr><td>TargetSystem | Unix | PersonExcludeList</td><td>List of all user accounts that must not be automatically assigned to employees. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern.
Example:
<code>ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $</code></td></tr>
</table>

Appendix B

Default project template for Unix-based target systems

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

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

The project template uses mappings for the following schema types.

Table 34: 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

Appendix C

Unix connector settings

The following settings are configured for the system connection with the Unix connector.

Table 35: Unix connector settings

Setting	Description
Server or IP	Server name or IP address of the host. Variable: `CP_Host`
Host name	Name of the host. Variable: `Hostname`
Port	Communications port for establishing the SSH connection. The default communications port is the TCP port **22**. Variable: `CP_Port`
User account	When the authentication method is **Password**. User account for SSH login in the host. Variable: `CP_SSHUser`
Password	When the authentication method is **Password**. Password for SSH login on the host. Variable: `CP_SSHPassword`
Private key	When the authentication method is **Private key**. Private key for logging in to the host. Variable: `CP_PrivateKey`
Passphrase	When the authentication method is **Private key**. Passphrase for logging in to the host. Variable: `CP_PrivateKeyPassphrase`
Change to administrative context	Method to use to gain administrative permissions. Permitted values are: • **Default**: If the user already possesses administrative permissions, select the **Default** method.

Setting	Description
	• **Sudo**: If the current user logged in on the host can run administrative tasks as an administrative user, select the **Sudo** method. Enter the alternative user, such as **root**. • **Su**: If administrative tasks should be run using a different user, select the **su** method. Enter the user's login credentials. The default user is **root**. Variable: `CP_EvaluationMethod`
User name	User name if the **Sudo** or **Su** methods are used. Variable: `CP_EvaluationUser` Default: **root**
Password	Password for the user if the **Su** method is used. Variable: `CP_EvaluationPassword`

About us

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

Contacting us

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

Technical support resources

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

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

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

Index