



## One Identity Manager 9.1

# Administration Guide for Connecting to SharePoint

**Copyright 2022 One Identity LLC.**

**ALL RIGHTS RESERVED.**

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

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

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

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

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

**Patents**

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

**Trademarks**

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

**Legend**

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

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

One Identity Manager Administration Guide for Connecting to SharePoint  
Updated - 19 September 2022, 12:59

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

# Contents

|   |           |
|---|-----------|
| <b>Managing SharePoint environments</b>   | <b>8</b>  |
| Architecture overview   | 9         |
| One Identity Manager users for managing SharePoint                                  | 10        |
| Claims-based authentication   | 12        |
| <b>Setting up SharePoint farm synchronization</b>                                   | <b>13</b> |
| Users and permissions for synchronizing with a SharePoint farm                      | 14        |
| Setting up the synchronization server   | 15        |
| Creating a synchronization project for initial synchronization of a SharePoint farm | 18        |
| Special synchronization cases for valid permissions                                 | 25        |
| Displaying synchronization results  | 25        |
| Customizing the synchronization configuration                                       | 26        |
| How to configure SharePoint synchronization   | 27        |
| Configuring synchronization of several SharePoint farms                             | 28        |
| Changing system connection settings of SharePoint farms                             | 29        |
| Editing connection parameters in the variable set                                   | 29        |
| Editing target system connection properties   | 30        |
| Updating schemas  | 31        |
| Speeding up synchronization with revision filtering                                 | 32        |
| Post-processing outstanding objects   | 32        |
| Configuring the provisioning of memberships   | 35        |
| Configuring single object synchronization   | 36        |
| Accelerating provisioning and single object synchronization                         | 37        |
| Help for analyzing synchronization issues   | 38        |
| Disabling synchronization   | 39        |
| Synchronizing single objects  | 40        |
| Ignoring data error in synchronization  | 41        |
| Pausing handling of target system specific processes (Offline mode)                 | 41        |
| <b>Basic data for managing a SharePoint environment</b>                             | <b>44</b> |
| Authentication modes  | 45        |
| Prefixes  | 46        |
| Zones and alternative URLs  | 47        |

|   |           |
|---|-----------|
| SharePoint site templates .....   | 47        |
| SharePoint permissions .....  | 47        |
| SharePoint quotas .....   | 48        |
| SharePoint languages .....  | 48        |
| Editing a server .....  | 49        |
| Main data for a Job server .....  | 50        |
| Specifying server functions .....   | 52        |
| Target system managers .....  | 53        |
| Setting up account definitions .....  | 55        |
| Creating an account definition .....  | 56        |
| Main data for an account definition .....                                       | 56        |
| Creating manage levels .....  | 59        |
| Main data for manage levels .....   | 61        |
| Creating a formatting rule for IT operating data .....                          | 62        |
| Collecting IT operating data .....  | 63        |
| Modify IT operating data .....  | 64        |
| Assigning account definitions to employees .....                                | 65        |
| Assigning account definitions to departments, cost centers, and locations ..... | 66        |
| Assigning account definitions to business roles .....                           | 66        |
| Assigning account definitions to all employees .....                            | 67        |
| Assigning account definitions directly to employees .....                       | 68        |
| Assigning account definitions to system roles .....                             | 68        |
| Adding account definitions to the IT Shop .....                                 | 68        |
| Assigning account definitions to a target system .....                          | 71        |
| Deleting an account definition .....  | 71        |
| <b>SharePoint farms .....</b>   | <b>74</b> |
| General main data of a SharePoint farm .....                                    | 74        |
| Editing synchronization projects .....  | 75        |
| <b>SharePoint web applications .....</b>  | <b>77</b> |
| <b>SharePoint site collections and sites .....</b>                              | <b>78</b> |
| SharePoint site collections .....   | 78        |
| General main data of a site collection .....                                    | 79        |
| Specifying categories for inheriting SharePoint groups .....                    | 80        |
| SharePoint sites .....  | 80        |

|  |            |
|--|------------|
| General main data of a site .....  | 81         |
| Address data for a site .....  | 82         |
| Site design properties .....   | 83         |
| Additional tasks for managing sites .....                                    | 83         |
| Passing on permissions to child sites .....                                  | 84         |
| Setting up SharePoint site collections and sites .....                       | 84         |
| <b>SharePoint user accounts .....</b>  | <b>86</b>  |
| Supported user account types .....   | 88         |
| Entering main data of SharePoint user accounts .....                         | 92         |
| Group authenticated user account main data .....                             | 93         |
| User authenticated user account main data .....                              | 95         |
| Additional tasks for managing SharePoint user accounts .....                 | 99         |
| Displaying the SharePoint user account overview .....                        | 100        |
| Assigning SharePoint groups directly to a SharePoint user account .....      | 100        |
| Assigning SharePoint roles directly to user accounts .....                   | 101        |
| Assigning extended properties .....  | 101        |
| Using custom authentication modes .....                                      | 102        |
| Assigning employees automatically to SharePoint user accounts .....          | 102        |
| Editing search criteria for automatic employee assignment .....              | 104        |
| Deleting and restoring SharePoint user accounts .....                        | 106        |
| <b>SharePoint roles and groups .....</b>                                     | <b>108</b> |
| SharePoint groups .....  | 109        |
| Entering main data of SharePoint groups .....                                | 110        |
| Assigning SharePoint groups to SharePoint user accounts .....                | 112        |
| Assigning SharePoint groups to departments, cost centers and locations ..... | 113        |
| Assigning SharePoint groups to business roles .....                          | 114        |
| Assigning SharePoint user accounts directly to a SharePoint group .....      | 115        |
| Assigning SharePoint roles to SharePoint groups .....                        | 116        |
| Adding SharePoint groups to system roles .....                               | 116        |
| Adding SharePoint groups to the IT Shop .....                                | 117        |
| Adding SharePoint groups automatically to the IT Shop .....                  | 119        |
| Additional tasks for managing SharePoint groups .....                        | 121        |
| Displaying an overview of SharePoint groups .....                            | 121        |
| Effectiveness of group memberships .....                                     | 121        |

|   |            |
|---|------------|
| SharePoint group inheritance based on categories .....                                | 123        |
| Assigning extended properties to SharePoint groups .....                              | 125        |
| Deleting SharePoint groups .....  | 125        |
| Default solutions for requesting SharePoint groups .....                              | 126        |
| Adding SharePoint groups .....  | 126        |
| SharePointRequesting Groups Memberships .....   | 127        |
| SharePoint roles and permission levels .....  | 127        |
| Entering main data of SharePoint permission levels .....                              | 128        |
| Additional tasks for managing SharePoint permission levels .....                      | 129        |
| Displaying the SharePoint permission level overview .....                             | 129        |
| Assigning permissions .....   | 129        |
| Special synchronization cases for valid permissions .....                             | 130        |
| Entering main data of SharePoint roles .....  | 130        |
| Assigning SharePoint roles to SharePoint user accounts .....                          | 132        |
| Assigning SharePoint roles to departments, cost centers and locations .....           | 132        |
| Assigning SharePoint roles to business roles .....                                    | 134        |
| Assigning SharePoint user accounts directly to a SharePoint role .....                | 135        |
| Assigning SharePoint groups to SharePoint roles .....                                 | 135        |
| Adding SharePoint roles to system roles .....   | 136        |
| Adding SharePoint roles to the IT Shop .....  | 137        |
| Additional tasks for managing SharePoint roles .....                                  | 138        |
| Displaying the SharePoint rules overview .....  | 138        |
| Effectiveness of SharePoint roles .....   | 139        |
| Assigning extended properties to SharePoint roles .....                               | 139        |
| Deleting SharePoint roles and permission levels .....                                 | 140        |
| <b>Permissions for SharePoint web applications .....</b>                              | <b>141</b> |
| SharePoint permission policies .....  | 142        |
| SharePoint user policies .....  | 142        |
| <b>Reports about SharePoint objects .....</b>   | <b>145</b> |
| Overview of all assignments .....   | 147        |
| <b>Appendix: Configuration parameters for managing a SharePoint environment .....</b> | <b>149</b> |
| <b>Appendix: Default project template for SharePoint .....</b>                        | <b>151</b> |
| <b>About us .....</b>   | <b>153</b> |

**Contacting us ..... 154**

**Technical support resources ..... 155**

**Index ..... 156**

## Managing SharePoint environments

In One Identity Manager, components and access rights from SharePoint 2013, SharePoint 2016, SharePoint 2019, and the SharePoint Server Subscription Edition can be mapped. The aim of this is to guarantee company employees access to the SharePoint site. To achieve this, information about the following SharePoint components is loaded into the One Identity Manager database.

- The farm, as the top level of the logical architecture in the SharePoint environment  
The SharePoint farm is set up as the base object for synchronization in the One Identity Manager database.
- All web applications set up inside the farm with their user policies and permitted permissions
- All site collections for these web applications with their user accounts and groups
- All sites added in site collections in a hierarchical structure (but not their content)
- All permission levels and SharePoint roles that define permissions for individual sites

SharePoint roles, groups, and user accounts are mapped in the context of the SharePoint components for which they are set up. In the One Identity Manager, these objects provide SharePoint users with access permissions to the different websites. For that, you can use the different One Identity Manager mechanisms for linking employees with their SharePoint user accounts. The following objects are provisioned:

- SharePoint user accounts and their relations to SharePoint roles and groups
- SharePoint groups and their assignments to user accounts and roles
- SharePoint roles and their site permissions

To log into the SharePoint server, One Identity Manager supports classic Windows authentication as well as claims-based authentication. Every SharePoint user account that can log in with classic Windows authentication, is assigned either an Active Directory or an LDAP user account or an Active Directory or LDAP group in One Identity Manager. Login requires that the associated Active Directory or LDAP systems are also mapped in the One Identity Manager database. You can maintain information in One Identity Manager about authentication systems used by the SharePoint environment.

For every SharePoint user account connected to an Active Directory or LDAP user account, an additional employee defined in the One Identity Manager database can also be assigned. This makes it possible to maintain employee memberships in SharePoint roles

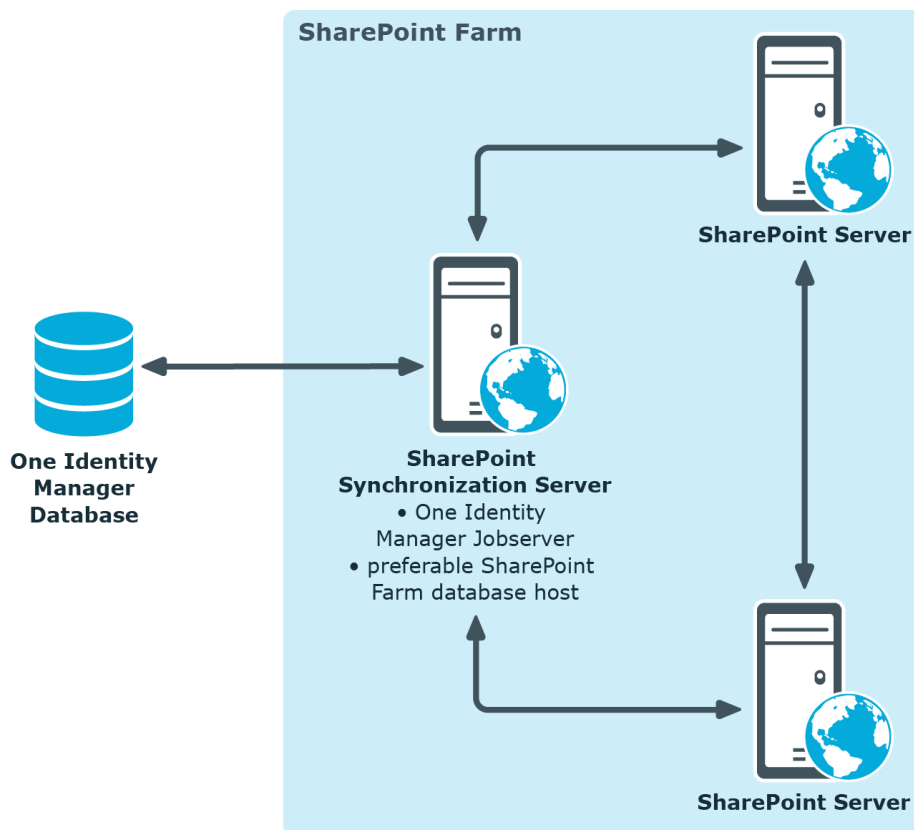


and groups. Employees can inherit SharePoint permissions by assigning SharePoint roles and groups to the organizational units. It is also possible to request permissions through the IT Shop. Permissions assigned to an employee can be monitored over compliance rules.

## Architecture overview

The SharePoint connector is used for synchronization and provisioning SharePoint. The connector communicates directly with a SharePoint farm's SharePoint servers.

**Figure 1: Connector paths for communicating with SharePoint**



To be able to synchronize and provision, the SharePoint farm, the One Identity Manager Service, the SharePoint connector, and the Synchronization Editor must be installed on one of the servers. In the following, this server is known as the synchronization server. 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.

### Detailed information about this topic

- [Setting up the synchronization server](#) on page 15

# One Identity Manager users for managing SharePoint

The following users are used setting up and administration of SharePoint with One Identity Manager.

**Table 1: Users**

| Users                        | Tasks  |
|------------------------------|--|
| Target system administrators | <p>Target system administrators must be assigned to the <b>Target systems   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"><li>• Administer application roles for individual target system types.</li><li>• Specify the target system manager.</li><li>• Set up other application roles for target system managers if required.</li><li>• Specify which application roles for target system managers are mutually exclusive.</li><li>• Authorize other employees to be target system administrators.</li><li>• Do not assume any administrative tasks within the target system.</li></ul>   |
| Target system managers       | <p>Target system managers must be assigned to the <b>Target systems   SharePoint</b> application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"><li>• Assume administrative tasks for the target system.</li><li>• Create, change, or delete target system objects.</li><li>• Edit password policies for the target system.</li><li>• Prepare system entitlements to add to the IT Shop.</li><li>• Can add employees who have another identity than the <b>Primary identity</b>.</li><li>• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.</li><li>• Edit the synchronization's target system types and outstanding objects.</li></ul> |

| Users                               | Tasks  |
|-------------------------------------|--|
|                                     | <ul style="list-style-type: none"> <li>• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.</li> </ul>  |
| One Identity Manager administrators | <p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> <li>• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.</li> <li>• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.</li> <li>• Enable or disable additional configuration parameters in the Designer as required.</li> <li>• Create custom processes in the Designer as required.</li> <li>• Create and configure schedules as required.</li> <li>• Create and configure password policies as required.</li> </ul> |
| Administrators for the IT Shop      | <p>Administrators must be assigned to the <b>Request &amp; Fulfillment   IT Shop   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assign system entitlements to IT Shop structures.</li> </ul>   |
| Product owners for the IT Shop      | <p>Product owners must be assigned to the <b>Request &amp; Fulfillment   IT Shop   Product owners</b> application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Approve through requests.</li> <li>• Edit service items and service categories under their management.</li> </ul>  |
| Administrators for organizations    | <p>Administrators must be assigned to the <b>Identity Management   Organizations   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assign system entitlements to departments, cost centers, and locations.</li> </ul>   |
| Business roles administrators       | <p>Administrators must be assigned to the <b>Identity Management   Business roles   Administrators</b> application role.</p>   |

Users with this application role:

- Assign system entitlements to business roles.

## Claims-based authentication

One Identity Manager supports claims-based authentication as well as classical Windows authentication for logging in to the SharePoint server. Information about the SharePoint provider and authentication modes are stored in the database for this purpose. Existing SharePoint providers for claims-based authentication are loaded into the database during synchronization. Registered providers are stored for each web application.

Every user account stores which authentication mode the user with this user account uses to log in. The default authentication mode depends on whether claims-based authentication is permitted with the associated web applications.

The authentication mode is required to add user accounts to One Identity Manager. The user account login name for claims-based authentication contains a prefix that depends on which authentication mode is used. These prefixes are maintained with the authentication modes.

### Related topics

- [Authentication modes](#) on page 45

## Setting up SharePoint farm synchronization

### ***To initially load SharePoint objects into the One Identity Manager database***

1. Prepare a user account with sufficient permissions for synchronizing in SharePoint.
2. Set the **TargetSystem | SharePoint** configuration parameter to make the One Identity Manager components for managing SharePoint environments available.

In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

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

Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.

3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Synchronize the Active Directory or LDAP system that SharePoint is going to run on.

For more information about synchronizing with Active Directory, see the One Identity Manager Administration Guide for Connecting to Active Directory. For more information about synchronizing with LDAP, see the One Identity Manager Administration Guide for Connecting to LDAP.

**IMPORTANT:** To prevent inconsistent data, the Active Directory or LDAP system that SharePoint is running on, must always be synchronized first. Once synchronization has been successfully completed, you can start the SharePoint farm synchronization.

If you cannot ensure synchronization, define custom processes for connecting SharePoint user accounts and user policies with the corresponding authentication objects.

5. Create a synchronization project with the Synchronization Editor.

**NOTE:** To create a synchronization project, start the Synchronization Editor on the synchronization server or a remote server. For more information about the archiving process, see the One Identity Manager Target System Synchronization Reference Guide.

### Detailed information about this topic

- [Users and permissions for synchronizing with a SharePoint farm](#) on page 14
- [Setting up the synchronization server](#) on page 15
- [Creating a synchronization project for initial synchronization of a SharePoint farm](#) on page 18
- [Configuration parameters for managing a SharePoint environment](#) on page 149

## Users and permissions for synchronizing with a SharePoint farm

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

**Table 2: Users for synchronization**

| User                                      | Permissions   |
|---|---|
| User for accessing the SharePoint farm    | <p>The connector uses the server farm account to log in to the SharePoint farm during synchronization. Ensure the server farm account login data is available.</p> <p>There is no sensible minimum configuration recommended, which effectively differentiates its permissions from the server account. Membership of the "Farm Administrators" group alone is <b>not</b> sufficient.</p>   |
| One Identity Manager Service user account | <p>The One Identity Manager Service farm's server farm account must be used as user account for SharePoint.</p> <p>The user account for the One Identity Manager Service requires additional user permissions to carry out operations at file level (adding and editing directories and files).</p> <p>The user account must belong to the <b>Domain users</b> group.</p> <p>The user account must have the <b>Login as a service</b> extended user permissions.</p> <p>The user account requires permissions for the internal web service.</p> <p><b>NOTE:</b> If the One Identity Manager Service runs under the network service (<b>NT Authority\NetworkService</b>), you can grant permissions for the internal web service with the following command line call:</p> |

| User   | Permissions   |
|--|---|
|  | <pre>netsh http add urlacl url=http://&lt;IP address&gt;:&lt;port number&gt;/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none"> <li>• %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)</li> <li>• %ProgramFiles%\One Identity (on 64-bit operating systems)</li> </ul> |
| User for accessing the One Identity Manager database | The <b>Synchronization</b> default system user is provided to run synchronization using an application server.  |

## Setting up the synchronization server

You will need a synchronization server to synchronize a SharePoint environment. You can use any SharePoint farm SharePoint server for this. The following software must to be installed on the synchronization sever.

**NOTE:** You must never use the same synchronization server to run synchronization projects in parallel. Different synchronization servers must never run synchronization projects for the same SharePoint farm in parallel.

If you distribute synchronization of a SharePoint farm over different start up configurations, ensure that they are run in sequence. For more information about setting up start up configurations, see the *One Identity Manager Target System Synchronization Reference Guide*. For more information, see [Customizing the synchronization configuration](#) on page 26.

### To synchronize SharePoint 2013, 2016, 2019, or the Subscription Edition

- Windows Server 2008 R2 or Windows Server 2012
  - Microsoft SharePoint Server 2013, 2016, 2019, or the Subscription Edition
  - Microsoft .NET Framework version 4.8 or later
- NOTE:** Take the target system manufacturer's recommendations into account.
- One Identity Manager Service, SharePoint connector
    - Install One Identity Manager components with the installation wizard.
      1. Select the **Select installation modules with existing database** option.

## 2. Select the **Server | Job Server | SharePoint** machine role.

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

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 more 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 more 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 **SharePoint**.
5. On the **Server functions** page, select **SharePoint connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

- For a direct connection to the database:
    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 more 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 One Identity Manager Service farm's server farm account must be used as user account for SharePoint.

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 SharePoint farm

Use the Synchronization Editor to set up synchronization between the One Identity Manager database and SharePoint. The following describes the steps for initial configuration of a synchronization project.

A synchronization project collects all the information required for synchronizing the One Identity Manager database with a target system. Connection data for target systems, schema types and properties, mapping, and synchronization workflows all belong to this.

After the initial configuration, you can customize and configure workflows within the synchronization project. Use the workflow wizard in the Synchronization Editor for this. The Synchronization Editor also provides different configuration options for a synchronization project.

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

**Table 3: Information required for setting up a synchronization project**

| Data               | Explanation   |
|--------------------|---|
| SharePoint version | One Identity Manager supports synchronization with SharePoint versions 2013, 2016, 2019, and with the SharePoint Server Subscription Edition. |

| Data  | Explanation   |
|---|---|
| User account and password for SharePoint farm login | To access SharePoint objects, the connector logs in with the server farm account to the SharePoint farm. The server farm account's user name and password are required. For more information, see <a href="#">Users and permissions for synchronizing with a SharePoint farm</a> on page 14.  |
| Domain  | Server farm account domain.   |
| synchronization server                              | <p>All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>Installed components:</p> <ul style="list-style-type: none"> <li>• SharePoint server</li> <li>• One Identity Manager Service (started)</li> <li>• Synchronization Editor</li> <li>• SharePoint connector</li> </ul> <p>The synchronization server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>For more information, see <a href="#">Setting up the synchronization server</a> on page 15.</p>  |
| Remote connection server                            | <p>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If the Synchronization Editor cannot be started directly on the synchronization server, you can set up a remote connection.</p> <p><b>To use a remote connection</b></p> <ol style="list-style-type: none"> <li>1. Provide a workstation on which the Synchronization Editor is installed.</li> <li>2. Install the <b>RemoteConnectPlugin</b> on the synchronization server.</li> </ol> <p>Thus the synchronization server simultaneously assumes the function of the remote connection server.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> |

| Data  | Explanation   |
|---|---|
|   | <ul style="list-style-type: none"> <li>• One Identity Manager Service is started</li> <li>• <b>RemoteConnectPlugin</b> is installed</li> <li>• SharePoint connector is installed</li> <li>• Target system specific components are installed</li> </ul> <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p> |
| One Identity Manager database connection data | <ul style="list-style-type: none"> <li>• Database server</li> <li>• Database name</li> <li>• SQL Server login and password</li> <li>• Specifies whether integrated Windows authentication is used</li> </ul> <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p>  |

There is a wizard to assist you with setting up a synchronization project. This wizard takes you through all the steps you need to set up initial synchronization with a target system. Click **Next** once you have entered all the data for a step.

**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 SharePoint farm***

1. Start the Launchpad on the synchronization server and log in to 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 SharePoint** 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 you started the Launchpad on the synchronization server, do not change any settings.
  - If you started the Launchpad on the gateway server, do not change any settings.Enable the **Connect using remote connection server** option and under **Job server** select the synchronization server with which the connection should be established.
4. Enter the connection data for the SharePoint farm in the system connection wizard. You can test the connection and save the connection data.
  - Enter the following connection data.

**Table 4: SharePoint farm connection data**

| Property                  | Description  |
|---------------------------|--|
| SharePoint version        | SharePoint version in use. <ul style="list-style-type: none"><li>• To connect to SharePoint Server Subscription Edition, select <b>2019</b>.</li></ul> |
| Domain                    | Domain of the server farm account.   |
| User account and password | User name and password for the server farm account.<br>This user account is used to synchronize SharePoint objects.                                    |

- Click **Test now** to test the connection data.  
The Synchronization Editor attempts to connect to the SharePoint farm.
  - To save the connection data, enable **Save connection data on local computer**. This can be reused when you set up other synchronization projects.
5. 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.
  6. 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.
  7. On the **Restrict target system access** page, specify how system access should work. You have the following options:

**Table 5: Specify target system access**

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

8. 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.

9. 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.

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

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

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

7. Click **OK**.

### ***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**.

### ***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**.

#### **NOTE:**

In the default installation, after synchronizing, employees are automatically assigned. If an account definition for the site collection 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 site collection.
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 **SharePoint > User accounts (user authenticated) > Linked but not configured > Site collection>** category.
  - b. In the Manager, select the **SharePoint Online > User accounts (user authenticated) > Linked but not configured > Site collection>** category.
  - c. Select the **Assign account definition to linked accounts** task.
  - d. In the **Account definition** menu, select the account definition.
  - e. Select the user accounts that contain the account definition.
  - f. Save the changes.

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

- For more information, see the One Identity Manager Target System Synchronization Reference Guide.

### **Related topics**

- [Setting up the synchronization server](#) on page 15
- [Users and permissions for synchronizing with a SharePoint farm](#) on page 14
- [Default project template for SharePoint](#) on page 151
- [Setting up account definitions](#) on page 55
- [Assigning employees automatically to SharePoint user accounts](#) on page 102



# Special synchronization cases for valid permissions

Valid permissions are mapped in the One Identity Manager database in the SPSWebAppHasPermission table; assignments of valid permissions to permission levels are mapped in the SPSRoleHasSPSPPermission table.

If you remove permissions from the list of valid permissions for a web application in SharePoint, the permissions cannot be assigned to permission levels within the web application from this point on. Assignments to permission levels that already exist for these permissions remain intact but are not active. These permissions are deleted from the SPSWebAppHasPermission table during synchronization. Assignments to permission levels that already exist for these permissions are not changed. Inactive permissions are displayed in the permission levels' overview.

## Related topics

- [SharePoint roles and permission levels](#) on page 127

# 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.

Synchronization logs are stored for a fixed length of time.

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

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

## **Customizing the synchronization configuration**

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

You must customize the synchronization configuration to be able to regularly compare the database with the SharePoint environment 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 farms. Store a connection parameter as a variable for logging in to the farms.
- To specify which SharePoint objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

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

### Detailed information about this topic

- [How to configure SharePoint synchronization](#) on page 27
- [Configuring synchronization of several SharePoint farms](#) on page 28
- [Updating schemas](#) on page 31
- [Changing system connection settings of SharePoint farms](#) on page 29
- One Identity Manager Target System Synchronization Reference Guide

## How to configure SharePoint 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 SharePoint farms*

1. In the Synchronization Editor, open the synchronization project.
 

**TIP:** You can start the Synchronization Editor on any server to modify an existing synchronization project. Set up a remote connection to communicate with farm servers.
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 SharePoint farms](#) on page 28

## Configuring synchronization of several SharePoint farms

### Prerequisites

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

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

1. Install and configure a synchronization server for the other farm. Declare this server as Job server in the One Identity Manager.
2. Prepare a user account with sufficient permissions for synchronizing in the other farm.
3. Synchronize the Active Directory or LDAP environment, the other farm is going to run on.
4. Start the Synchronization Editor on the synchronization server of the other farm and log in on the One Identity Manager database.
5. Open the synchronization project.
6. Create a new base object for the other farm.
  - Use the wizard to attach a base object.
  - In the wizard, select the SharePoint 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.

7. Change other elements of the synchronization configuration as required.
8. Save the changes.
9. Run a consistency check.

## Detailed information about this topic

- [Setting up the synchronization server](#) on page 15
- [Users and permissions for synchronizing with a SharePoint farm](#) on page 14
- [How to configure SharePoint synchronization](#) on page 27

# Changing system connection settings of SharePoint farms

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

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

## Detailed information about this topic

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

# 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 is used for synchronizing different SharePoint farms.


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

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

Some connection parameters can be converted to variables here. For other parameters, variables are already created.

4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.

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

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

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

## Related topics

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

## Editing target system connection properties

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

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

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

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

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

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

**NOTE:** If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.  
This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

### **Related topics**

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

## **Updating schemas**

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

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

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

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

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

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

### ***To edit a mapping***

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

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

## **Speeding up synchronization with revision filtering**

Synchronization with SharePoint does not support revision filtering.

## **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 **SharePoint > Target system synchronization: SharePoint** category.

The navigation view lists all the synchronization tables assigned to the **SharePoint** 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**

| <b>Icon</b>   | <b>Method</b> | <b>Description</b>  |
|---|---------------|---|
|  | Delete        | The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account.<br><br>Indirect memberships cannot be deleted. |
|  | Publish       | The object is added to the target system. The <b>Outstanding</b> label is removed from the object.  |

| Icon  | Method | Description  |
|---|--------|--|
|   |        | <p>This runs a target system specific process that triggers the provisioning process for the object.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• The table containing the object can be published.</li> <li>• The target system connector has write access to the target system.</li> </ul> |
|  | Reset  | The <b>Outstanding</b> label is removed for the object.  |

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.

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

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

# Configuring the provisioning of memberships

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

- Memberships are saved as an object property in list form in the target system.  
Example: List of user accounts in the Users property of a SharePoint group (SPGroup)
- 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 **SharePoint > Basic configuration data > Target system types** category.
2. In the result list, select the **SharePoint** 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.

Example: SPSGroupHasSPSRLAsgn and SPSUserHasSPSRLAsgn

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 SPSUserHasSPSRLAsgn assignment table:

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

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

## Configuring single object synchronization

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

### **Prerequisites**

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

Single object synchronization is fully configured for synchronization projects created using the default project template. If you want to incorporate custom tables into this type of synchronization project, you must configure single object synchronization for these tables.

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

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

1. In the Manager, select the **SharePoint > Basic configuration data > Target system types** category.
2. In the result list, select the **SharePoint** 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_SPSFarm).XObjectKey`
8. Save the changes.

### **Related topics**

- [Synchronizing single objects](#) on page 40
- [Post-processing outstanding objects](#) on page 32

## **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 **SharePoint connector** server function to the Job server.

All Job servers must access the same SharePoint farm as the synchronization server for the respective base object.

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

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

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

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

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

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

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

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

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

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

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

- [Editing a server](#) on page 49

## **Help for analyzing synchronization issues**

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

- Consistency check results
- Revision filter settings
- Scope applied

- Analysis of the data store
- Object access times in the One Identity Manager database and in the target system

### ***To generate a synchronization analysis report***

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Help > Generate synchronization analysis report** menu item and click **Yes** in the security prompt.

The report may take a few minutes to generate. It is displayed in a separate window.

3. Print the report or save it in one of the available output formats.

## **Disabling synchronization**

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

### ***To prevent regular synchronization***

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

Now you can only start synchronization manually.

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

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

### ***To deactivate the synchronization project***

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

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

- [Creating a synchronization project for initial synchronization of a SharePoint farm](#) on page 18
- [Pausing handling of target system specific processes \(Offline mode\)](#) 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 **SharePoint** 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 SharePoint user accounts to SharePoint 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 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.

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

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

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


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

## Prerequisites

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

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

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

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

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

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

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

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

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

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

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

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

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

## Related topics

- [Disabling synchronization](#) on page 39

## Basic data for managing a SharePoint environment

The following data is relevant for managing SharePoint in One Identity Manager.

- Configuration parameter

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

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

For more information, see [Configuration parameters for managing a SharePoint environment](#) on page 149.

- 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 [Setting up account definitions](#) on page 55.

- Authentication Modes

One Identity Manager supports claims-based authentication as well as classical Windows authentication for logging in to the SharePoint server. The authentication mode to use is defined for the web application and for the user accounts. Usable authentication modes are maintained in the One Identity Manager database.

For more information, see [Authentication modes](#) on page 45.

- Prefixes

Prefixes are URLs relative to a web application that can be stored under a site collection.

For more information, see [Prefixes](#) on page 46.


- **Zones and alternative URLs**  
All the zones that you can configure for a web application are stored in the One Identity Manager database.  
For more information, see [Zones and alternative URLs](#) on page 47.
- **Site templates**  
Use site templates to add sites.  
For more information, see [SharePoint site templates](#) on page 47.
- **Permissions**  
User permissions for a SharePoint site or a web application are authorized by SharePoint permissions. Permissions are grouped into permission levels and permission policies.  
For more information, see [SharePoint permissions](#) on page 47.
- **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 32.
- **Servers**  
In order to handle target system specific processes in One Identity Manager, the synchronization server and its server functionality must be declared.  
For more information, see [Editing a server](#) on page 49.
- **Target system managers**  
A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all SharePoint farms in One Identity Manager.  
Define additional application roles if you want to limit the permissions for target system managers to individual SharePoint farms. The application roles must be added under the default application role.  
For more information, see [Target system managers](#) on page 53.

## Authentication modes

One Identity Manager supports claims-based authentication as well as classical Windows authentication for logging in to the SharePoint server. The authentication mode to use is defined for the web application and for the user accounts. Usable authentication modes are maintained in the One Identity Manager database. One Identity Manager supplies the default authentication systems "Windows (Claims)" (=claims-based Windows authentication) and "Windows Classic Mode" (=classic Window authentication). If you use other authentication systems in your SharePoint environment, add them separately in the

One Identity Manager. This makes it possible to assign user accounts to authentication modes. Enter the user and group prefix data. This is required to add new SharePoint user accounts in One Identity Manager.

### ***To add an authentication mode***

1. Select the **SharePoint > Basic configuration data > Authentication modes** category.
2. Click  in the result list.
3. Enter the required data on the main data form.
4. Save the changes.

Enter the required data for your own authentication mode:

**Table 7: Authentication mode properties**

| Property              | Description   |
|-----------------------|---|
| System ID             | A identifier for the authentication mode.   |
| User prefix           | Prefix for formatting a login name for new user accounts. The associated authentication object is not a group. This means, the user account option <b>Group</b> is not set.                 |
| Group prefix          | Prefix for formatting a login name for new user accounts. The associated authentication object is a group. This means, the user account option <b>Group</b> is set.                         |
| Column for login name | Column in the table Person used to format the login name for new user accounts. This information is required if employees are linked to user accounts though automatic employee assignment. |

### ***To assign your own authentication modes automatically to user accounts***

- In the Designer, modify the template for the `SPSUser.UID_SPSAuthSystem` column.  
For more information, see the One Identity Manager Configuration Guide.

## **Prefixes**

Prefixes are URLs relative to a web application that can be stored under a site collection. Prefix properties such as relative path, absolute path and prefix type, are displayed on the overview form with the associated web application.

### ***To obtain an overview of a prefix***

1. Select the **SharePoint > Basic configuration data > Prefixes** category.
2. Select a profile in the result list.
3. Select the **SharePoint prefix overview** task.

# Zones and alternative URLs

All the zones that you can configure for a web application are stored in the One Identity Manager database. You can see the alternative URLs that are configured for accessing the web application on the zone's overview form.

## *To obtain an overview of a zone*

1. Select the **SharePoint > Basic configuration data > Zones** category.
2. Select the zone in the result list.
3. Select the **SharePoint zone overview** task.

## *To obtain an overview of alternative URL of a web application*

1. Select the **SharePoint > Hierarchical view > <farm> > Web applications > <web application> > URLs** category.
2. Select the URL in the result list.
3. Select the **SharePoint alternative URL overview** task.

# SharePoint site templates

Use site templates to add sites. If new sites are meant to be added with One Identity Manager, load the site template into the One Identity Manager database using synchronization. The languages in which site templates are available are displayed on the overview form.

## *To obtain an overview of a site template*

1. Select the **SharePoint > Basic configuration data > Site templates** category.
2. Select the site template in the result list.
3. Select the **Site template overview** task.

# SharePoint permissions

User permissions for a SharePoint site or a web application are authorized by SharePoint permissions. Permissions are grouped into permission levels and permission policies. All web application entitlement policies, explicitly granted or rejected for the permission, are displayed on the permissions overview form.

In SharePoint, you can limit the number of permissions that can be assigned to permission levels. You are shown an overview of web applications permitted for the permissions.

### ***To obtain an overview of permissions***

1. Select the **SharePoint > Basic configuration data > Permissions** category.
2. Select the entitlements in the result list.
3. Select the **SharePoint entitlements overview** task.

You can assign permissions to permission levels in One Identity Manager.

### ***To assign valid permissions to permission levels***

1. Select the **SharePoint > Basic configuration data > Permissions** category.
2. Select the entitlements in the result list.
3. Select the **Assign permission levels** task.
4. In the **Add assignments** pane, assign permission levels.
  - OR -
  - In the **Remove assignments** pane, remove permission levels.
5. Save the changes.

### **Related topics**

- [SharePoint roles and permission levels](#) on page 127

## **SharePoint quotas**

You can view the SharePoint farm and site collections that the quota is assigned to on the quota overview form.

### ***To obtain an overview of a quota***

1. Select the **SharePoint > Quotas** category.
2. Select the quota in the result list.
3. Select the **SharePoint quota overview** task.

## **SharePoint languages**

All the languages that have language packets installed in a SharePoint environment are mapped in the One Identity Manager database.

### ***To obtain an overview of a language***

1. Select the **SharePoint > Hierarchical view > <farm> > Languages** category.
2. Select the language in the result list.



3. Select the **SharePoint language overview** task.

## Editing a server

In order to handle target system specific processes in One Identity Manager, the synchronization server and its server functionality must be declared. 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 **SharePoint > 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 **SharePoint > 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**

- [Main data for a Job server](#) on page 50
- [Specifying server functions](#) on page 52

### **Related topics**

- [Setting up the synchronization server](#) on page 15

# 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 8: Job server properties**

| Property                  | Meaning  |
|---------------------------|--|
| Server                    | Job server name.   |
| Full server name          | Full server name in accordance with DNS syntax.<br>Syntax:<br><Name of servers>.<Fully qualified domain name>  |
| Target system             | Computer account target system.  |
| Language                  | Language of the server.  |
| Server is cluster         | Specifies whether the server maps a cluster.   |
| Server belongs to cluster | Cluster to which the server belongs.<br><b>NOTE:</b> The <b>Server is cluster</b> and <b>Server belongs to cluster</b> properties are mutually exclusive.  |
| IP address (IPv6)         | Internet protocol version 6 (IPv6) server address.   |
| IP address (IPv4)         | Internet protocol version 4 (IPv4) server address.   |
| 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.<br><br>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          | Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values <b>Win32</b> , <b>Windows</b> ,  |

| Property  | Meaning   |
|---|---|
| system  | <b>Linux</b> , and <b>Unix</b> are permitted. If no value is specified, <b>Win32</b> is used.   |
| Service account data                            | One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.                                      |
| One Identity Manager Service installed          | Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.<br><br>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.<br><br>You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> .            |
| Paused due to unavailability of a target system | Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed.<br><br>For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i> . |
| No automatic software update                    | Specifies whether to exclude the server from automatic software updating.<br><br><b>  NOTE:</b> 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

- [Specifying server functions](#) on page 52

# Specifying server functions

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

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

**Table 9: Permitted server functions**

| Server function                         | Remark  |
|---|---|
| Active Directory connector              | Server on which the Active Directory connector is installed. This server synchronizes the Active Directory target system.   |
| 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                           | <p>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.</p> <p>The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.</p> |
| SQL processing server                   | <p>It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.</p> <p>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.</p>                           |
| 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                            | Server on which a One Identity Manager Service is installed.  |

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

## Related topics

- [Main data for a Job server](#) on page 50

# Target system managers

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

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

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

## Implementing application roles for target system managers

1. The One Identity Manager administrator allocates 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 SharePoint farms 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 SharePoint farms.

**Table 10: Default application roles for target system managers**

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

***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 > SharePoint** 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 **SharePoint > 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 SharePoint farms***

1. Log in to the Manager as a target system manager.
2. Select the **SharePoint > Farms** category.
3. Select the farm 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 | SharePoint** 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 farm in One Identity Manager.

**Related topics**

- [One Identity Manager users for managing SharePoint](#) on page 10
- [General main data of a SharePoint farm](#) on page 74

## Setting up 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.

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

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


**NOTE:** Only SharePoint user accounts that are not marked as a group can be created with account definitions (`IsDomainGroup = 'false'`). However, it is recommended to create SharePoint user accounts based on target system groups. Only use account definitions for SharePoint if you are not following standard procedure. For more information, see [SharePoint user accounts](#) on page 86.

The following steps are required to implement an account definition:

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

## Creating an account definition

### **To create or edit an account definition**

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

## Main data for an account definition

Enter the following data for an account definition:



**Table 11: 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 | <p>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.</p> <p><b>TIP:</b> You can enter this account definition for the associated Active Directory or LDAP domain here. In this case, an Active Directory or LDAP user account is created for the employee first. If this exists, the SharePoint user account is added.</p> <p>Implement this behavior on a custom basis. Customize TSB_PersonHasAccountDef_AutoCreate_SPSUser to do this.</p> |
| Description                 | Text field for additional explanation.  |
| Manage level (initial)      | Manage level to use by default when you add new user accounts.  |
| Risk index                  | <p>Value for evaluating the risk of assigning the account definition to employees. Set a value in the range <b>0</b> to <b>1</b>. This input field is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set.</p> <p>For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>  |
| 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 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.  |

| Property  | Description  |
|---|--|
| Automatic assignment to employees                 | <p>Specifies whether the account definition is automatically assigned to all internal employees. To automatically assign the account definition to all internal employee, use the <b>Enable automatic assignment to employees</b>. 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.</p> <p>To automatically remove the account definition assignment from all employees, use the <b>Disable automatic assignment to employees</b>. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</p> |
| Retain account definition if permanently disabled | <p>Specifies the account definition assignment to permanently deactivated employees.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>   |
| Retain account definition if temporarily disabled | <p>Specifies the account definition assignment to temporarily deactivated employees.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>   |
| Retain account definition on deferred deletion    | <p>Specifies the account definition assignment on deferred deletion of employees.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>  |
| Retain account definition on security risk        | <p>Specifies the account definition assignment to employees posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.</p>  |
| Resource type                                     | Resource type for grouping account definitions.  |
| Spare field 01 - spare                            | Additional company-specific information. Use the Designer to   |

| Property                | Description   |
|-------------------------|---|
| field 10                | customize display names, formats, and templates for the input fields.   |
| Groups can be inherited | <p>Specifies whether the user account can inherit groups through the linked 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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> |
| Roles can be inherited  | <p>Specifies whether the user account can inherit SharePoint roles through the linked employee. If the option is set, the user account inherits the roles through hierarchical roles, in which the employee is a member, or through IT Shop requests.</p>   |

## Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

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

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

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For more 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.


**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 **SharePoint > 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.

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

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

# Main data for manage levels

Enter the following data for a manage level.

**Table 12: 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: <ul style="list-style-type: none"><li>• <b>Never:</b> Data is not updated. (Default)</li><li>• <b>Always:</b> Data is always updated.</li><li>• <b>Only initially:</b> Data is only determined at the start.</li></ul> |
| Retain groups if temporarily disabled         | Specifies whether user accounts of temporarily deactivated retain their group memberships.  |
| Lock user accounts if temporarily disabled *) | Specifies whether user accounts of temporarily deactivated 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.  |

**NOTE:**\*) SharePoint user accounts cannot be locked!

When an employee is disabled, deleted, or rated as a security risk their SharePoint user accounts remain enabled. For logging into a SharePoint site collection, you need to know if the user account referenced as an authentication object is locked or disabled. To prevent a disabled, deleted, or security risk employee logging into a SharePoint site

collection, manage the user accounts linked as authentication objects using account definitions.

## Creating a formatting rule for IT operating data

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

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

- SharePoint authentication mode
- SharePoint Online authentication mode
- Groups can be inherited
- Roles can be inherited
- Identity
- Privileged user account.

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

1. In the Manager, select the **SharePoint > 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 | SharePoint | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

## Collecting IT operating data

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

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

### Example:

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.

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**

- Click → next to the field.
  - Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.
  - Select the specific target system or account definition under **Effects on**.
  - 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.

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


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

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

1. In the Manager, select the **SharePoint > 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.

## **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 **SharePoint > 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.

## **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 **SharePoint > 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.


# Assigning account definitions directly to employees

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

1. In the Manager, select the **SharePoint > 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.

# 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 **SharePoint > 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 the system role assignment.

### *To remove an assignment*

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

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

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

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

**Related topics**

- [Main data for an account definition](#) on page 56
- [Assigning account definitions to departments, cost centers, and locations](#) on page 66
- [Assigning account definitions to business roles](#) on page 66
- [Assigning account definitions directly to employees](#) on page 68
- [Assigning account definitions to system roles](#) on page 68

# Assigning account definitions to a target system

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

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

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

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

1. In the Manager, select the site collection in the **SharePoint > Site collections** 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.

# Deleting an account definition

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

## *To delete an account definition*

1. Remove automatic assignments of the account definition from all employees.
  - a. In the Manager, select the **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 site collection in the **SharePoint > Site collections** 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 **SharePoint > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Click  to delete an account definition.

## SharePoint farms

**NOTE:** The Synchronization Editor sets up the farms in the One Identity Manager database.


### *To edit the main data of a farm*

1. Select the **SharePoint > Farms** category.
2. Select the farm in the result list. Select the **Change main data** task.
3. Edit the farm's main data.
4. Save the changes.

## General main data of a SharePoint farm

Enter the following main data of a farm.

**Table 13: General main data of a farm**

| Property               | Description  |
|------------------------|--|
| Name                   | Name of the SharePoint instance port. A distinguished name for internal user is formed from this.  |
| Domain                 | Name of the Active Directory or LDAP domain that is serves as security provider for SharePoint The user accounts and groups that are referenced are searched for in this domain.   |
| Display name           | The farm's display name.   |
| Target system managers | <p>Application role in which target system managers are specified for the farm. Target system managers only edit the objects from farms that are assigned to them. Each farm can have a different target system manager assigned to it.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this farm. Use the  button to add a new application role.</p> |

| Property  | Description  |
|---|--|
| Synchronized by   | <p>Type of synchronization through which data is synchronized between the farm and One Identity Manager. As soon as objects for this farm are available in One Identity Manager, the type of synchronization can no longer be changed.</p> <p>If you create a farm with the Synchronization Editor, it uses <b>One Identity Manager</b>.</p> |
| <b>Table 14: Permitted values</b>   |  |
| <b>Value</b>  | <b>Synchronization by</b> <b>Provisioned by</b>  |
| One Identity Manager  | SharePoint connector    SharePoint connector   |
| No synchronization  | none    none   |
| <b>NOTE:</b> If you select <b>No synchronization</b> , you can define custom processes to exchange data between One Identity Manager and the target system. |  |
| Build version   | The build version for SharePoint services for this farm are read in during synchronization.  |

## Related topics

- [Target system managers](#) on page 53

# Editing synchronization projects

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

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

## To open an existing synchronization project in the Synchronization Editor

1. Select the **SharePoint > Farms** category.
2. Select the farm in the result list. Select the **Change main data** task.
3. Select the **Edit synchronization project...** task.

## Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

## Related topics

- [Customizing the synchronization configuration](#) on page 26

## SharePoint web applications

SharePoint web applications provide permissions for SharePoint users that are valid across all websites within the web application. You can find information about SharePoint objects that the web application is linked to on the overview form. Defined users and permissions policies are shown for the web application. Valid SharePoint providers are displayed with the web applications for which they are registered.

In SharePoint, you can limit the amount of permissions that can be assigned to SharePoint permission levels. You can see all valid permissions for the web application on the overview form.

### *To obtain an overview of a web application*

1. Select the **SharePoint > Web applications** category.
2. Select the web application in the result list.
3. Select the **SharePoint web application overview** task.

### Related topics

- [SharePoint roles and permission levels](#) on page 127

## SharePoint site collections and sites

SharePoint sites are organized into site collections. A site collection manages access rights and characterization templates for all sites in the site collection. It consists of at least one site on the top level (root site). Other websites are arranged below this root site. They can be connected to hierarchies through simple task relationships. Properties (for example role definitions) can be inherited by child sites through this hierarchical structure.

Site collections and sites are mapped with their access rights to One Identity Manager. You cannot edit their properties in the One Identity Manager. You can edit access rights managed within a site collection in One Identity Manager. To do this, SharePoint roles, groups, and user accounts are loaded into the One Identity Manager database.

### Related topics

- [SharePoint roles and groups](#) on page 108
- [SharePoint user accounts](#) on page 86

## SharePoint site collections

A site collection groups sites together. User account and their access permissions are managed on the sites. To automatically assign used accounts and employees, assign an account definition to the site collection.

Authorized user accounts and groups are displayed on the site collection's overview as well as the web application and the root site linked to the site collection. The quota template, the site collection administrators and auditors assigned to the site collection are also visible on the overview form.

### *To edit site collection properties*

1. Select the **SharePoint > Site collections** category.
2. Select the site collection in the result list. Select the **Change main data** task.
3. Enter the required data on the main data form.
4. Save the changes.

## Detailed information about this topic

- [General main data of a site collection](#) on page 79
- [Specifying categories for inheriting SharePoint groups](#) on page 80

# General main data of a site collection

The following properties are displayed for site collections.

**Table 15: General main data of a site collection**

| Property                      | Description  |
|-------------------------------|--|
| Account definition            | <p>Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this site collection and if user accounts are to be created that are already managed (<b>Linked configured</b>). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the employee (<b>Linked</b>) if no account definition is given. This is the case on initial synchronization, for example.</p> |
| Server                        | Name of the SharePoint server that provides the site collection.   |
| Web application               | Unique ID for web application that belongs to the site collection.   |
| Root site                     | Link to the site collection root site. Links to a site that is set as <b>root site</b> .   |
| Administrator                 | Administrator user account for the site collection.  |
| Other administrator           | Additional administrator user account for the site collection.   |
| Used storage                  | Information about the storage taken up by the site collection on the server.   |
| Last security relevant change | Time of last security relevant change that was made to an object in this site collection.  |

On the **Addresses** tab, you can see the site collection URL and port and the URL of a portal linked to the site collection.


## Related topics

- [Setting up account definitions](#) on page 55

# Specifying categories for inheriting SharePoint groups

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 site collection in the **SharePoint > Site collections** 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

- [SharePoint group inheritance based on categories](#) on page 123
- One Identity Manager Target System Base Module Administration Guide

# SharePoint sites

You can structure sites hierarchically. There is always a site labeled as the "root site" in every site collection. The other sites in the site collection are sorted below the root site.

## *To display properties of a site*

1. Select the **SharePoint > Sites** category.
2. Select the site in the result list. Select the **Change main data** task.

## Detailed information about this topic

- [General main data of a site](#) on page 81
- [Address data for a site](#) on page 82



- [Site design properties](#) on page 83

## General main data of a site

The following main data is displayed for sites.

**Table 16: General main data of a site**

| Property                | Description   |
|-------------------------|---|
| Display name            | Display name of the site.   |
| Root site               | Specifies whether the site is the site collection root site.  |
| Parent site             | Unique ID for the parent site.  |
| Site collection         | Unique identifier for the site collection to which the site belongs.  |
| Unique role definition  | Specifies whether permission levels and associated permission can be defined for the site (tables <code>SPSRole</code> and <code>SPSRoleHasSPSPPermission</code> ). If the option is not set the role definitions are inherited from the parent site.   |
| Use roles from          | Unique identifier for the site from which the role definitions are inherited. If the site is assigned roles of its own, their permissions are overwritten by the inherited permissions.   |
| Unique role assignments | Specifies whether user accounts or groups can have direct access permissions to the site (tables <code>SPSUserHasSPSRLAsgn</code> and <code>SPSGroupHasSPSRLAsgn</code> ). If this option is not set, the role assignments are inherited from the parent site. No other user accounts or groups have permissions for this site. |
| Use assignments from    | Unique identifier for the site from which the role assignments are inherited.   |
| Author                  | Link to user account that created the site.   |
| Description             | Text field for additional explanation.  |
| Permit anonymous access | Specifies whether anonymous access is permitted to the site.  |

### Detailed information about this topic

- [SharePoint roles and groups](#) on page 108
- [SharePoint roles and permission levels](#) on page 127

# Address data for a site

On **Addresses** tab, the following address data is mapped.

**Table 17: Address data for a site**

| Properties             | Description  |
|------------------------|--|
| Prefix                 | Unique identifier of the prefix for the site collection under which you want the site to be added. A value is only shown if you add the site through One Identity Manager. |
| URL relative to server | URL for the site logo relative to the web application URL.   |
| URL                    | Absolute site URL.   |
| System master page URL | System master page URL, relative to the web application URL.   |
| Site master page URL   | Site master page URL, relative to the web application URL.   |
| Portal URL             | URL for a portal site that   |

| Properties | Description             |
|------------|-------------------------|
|            | this site is linked to. |

If the server declared in the URL can be resolved by DNS, you can open the site in the default browser.

### To open the site

1. Select the **SharePoint > Sites** category.
2. Select the site in the result list.
3. Select the **Open URL** task.

### Related topics

- [Setting up SharePoint site collections and sites](#) on page 84

## Site design properties

The following design information is displayed on **Design**.

**Table 18: Site design properties**

| Property              | Description  |
|-----------------------|--|
| Site template         | Unique identifier for the site template to be used when the site is created. A value is only shown if you add the site through One Identity Manager. |
| Title                 | Name for displaying the site.  |
| URL for logo          | URL for the site logo relative to the web application URL.   |
| Logo icon description | Description of the site's logo.  |

### Related topics

- [Setting up SharePoint site collections and sites](#) on page 84

## Additional tasks for managing sites

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

You can view all the roles and permission levels that are valid for this site on the overview form. Use the **Open URL** task to open the site in a standard web browser. Prerequisite for this is that the server in the URL can be resolved per DNS.

#### ***To obtain an overview of an site***

1. Select the **SharePoint > Sites** category.
2. Select the site in the result list.
3. Select the **SharePoint site overview** task.

#### **Related topics**

- [Address data for a site](#) on page 82

## **Passing on permissions to child sites**

SharePoint roles are defined at site level. There are always roles defined for the root site of a site collection. Child sites can inherit these role definitions. In the same way, roles on the root site of a site collection are also assigned to groups or user accounts. These assignments can inherit child sites. The **Unique role definition** option specifies whether a site inherits roles from the parent site. The **Unique role assignment** option specifies whether user accounts and groups are explicitly authorized for a site or whether the role assignments are inherited by the parent website.

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

- [SharePoint roles and groups](#) on page 108

#### **Related topics**

- [General main data of a site](#) on page 81

## **Setting up SharePoint site collections and sites**

Site collections and sites are simply loaded into the One Identity Manager database through synchronization in the default installation of One Identity Manager. You can add new site collections and site in the One Identity Manager and publish them in the SharePoint target system. To do this, the UID\_SPSPrefix and UID\_SPSTemplate columns are provided for the SPSWeb table as well as predefined scripts and processes.

**NOTE:** You can use the following scripts and processes to request site collections and sites from the IT Shop. Customize these scripts and processes as required!

| Script/Process                            | Description  |
|---|--|
| Script VI_<br>CreateSPSSite               | Creates a new site collection and the associate root site in the One Identity Manager database. Creates a user account that is entered as site collection administrator or root site author. |
| Script VI_<br>CreateSPSWeb                | Creates a new site within a site collection in the One Identity Manager database.  |
| Process SP0_<br>SPWeb_<br>(De-)Provision  | Creates a new site within a site collection. The process is triggered by the event PROVISION when the site in the One Identity Manager database is not labeled as the root site.             |
| Process SP0_<br>SPSite_<br>(De-)Provision | Creates a new site collection in a web application and the associated root site. The process is triggered by the event PROVISION.  |

The following step are required in additions:

- Define a requestable product through which the site collection/site is requested from the IT Shop.
- Define product properties that are mapped to the script parameter (for example web application, prefix, or site template). You must include these product properties when the site collection/site is requested.
- Create a process for the PersonWantsOrg table that is started when the request is approved (event OrderGranted). This process call the matching script and sets the parameter values with the defined product properties you have defined. Then the site collection/site is added to the One Identity Manager database.

## SharePoint user accounts

SharePoint user accounts provide the information necessary for user authentication, such as, the authentication mode and login names. In addition, permissions of users in a site collection are specified in the user accounts.

Each SharePoint user account represents an object from an authentication system trusted by the SharePoint installation. If this authentication system is managed as a target system in One Identity Manager, the SharePoint object used for authentication can be saved as the authentication object in the user policy. This means the SharePoint user account permissions are mapped to employees managed in One Identity Manager. One Identity Manager makes it possible for you to obtain an overview of all an employee's SharePoint access permissions. SharePoint permissions can be attested and checked for compliance. Employees can request or obtain the SharePoint permissions they requires through their memberships in hierarchical roles or through the Web Portal when appropriately configured.

### Example

Set up guest access to a site collection with read-only permissions. To do this, a SharePoint user account is added. The Active Directory group "Guests" is assigned as authentication object to the user account. Jo User1 owns an Active Directory user account, which is a member in this group. They can log in to the site collection with this and obtain all the SharePoint user account's permissions.

Jan User3 also obtain a guest login for the site collection. They own an Active Directory user account in the same domain. They request membership of the Web Portal group in Active Directory. Once the request is granted approval and assigned, they can log in on the site collection.

By default, the following objects can be assigned as authentication objects in One Identity Manager.

- Active Directory groups (ADSGroup)
- Active Directory user accounts (ADSAccount)

- LDAP groups (LDAPGroup)
- LDAP user accounts (LDAPAccount)

During synchronization, One Identity Manager tries to assign the matching authentication object using the login name.

SharePoint access permissions are supplied in different ways in the One Identity Manager, depending on the referenced authentication object.

### **Case 1: The associated authentication object is a group. The authentication system is managed in One Identity Manager. (Default case)**

- The user account represents an Active Directory or LDAP group. This group can be assigned in the One Identity Manager as authentication object.
- The user account cannot be assigned to an employee. This means, the user account can only become a member in SharePoint roles and groups through direct assignment.
- In order for an employee to log in on the SharePoint system, they require an Active Directory or LDAP user account. This user account must be member in the Active Directory or LDAP group.
- A new SharePoint user account can be created manually.
- The user account cannot be managed through an account definition.

### **Case 2: The authentication object is a user account. The authentication system is managed in One Identity Manager.**

- The user account represents an Active Directory or LDAP user account. The user account is not assigned as an authentication object in One Identity Manager.
- The SharePoint user account can be assigned to an employee. This means that the user account can become a member in SharePoint roles and groups through inheritance and direct assignment.

If an authentication object is assigned, the connected employee is found through the authentication object.

If there is no authentication object assigned, the employee can be assigned automatically or manually. Automatic employee assignment depends on the "TargetSystem | SharePoint | PersonAutoFullsync" and "TargetSystem | SharePoint | PersonAutoDefault" configuration parameters.

- A new SharePoint user account can be manually created or by using an account definition. The Active Directory or LDAP user account used as authentication object must belong to a domain trusted by the referenced authentication system.
- The user account can be managed through an account definition.

### Case 3: The authentication object is a user account. The authentication system is not managed in One Identity Manager.

- The user account cannot be assigned an authentication object.
- The user account can be manually or automatically assigned to an employee. This means that the user account can become a member in SharePoint roles and groups through inheritance and direct assignment. Automatic employee assignment depends on the "TargetSystem | SharePoint | PersonAutoFullsync" and "TargetSystem | SharePoint | PersonAutoDefault" configuration parameters.
- A new SharePoint user account can be manually created or by using an account definition. If an account definition is used, the column templates must be customized for the SPSUser.LoginName and SPSUser.DisplayName columns.
- The user account can be managed through an account definition.

The basics for managing employees and user account are described in the One Identity Manager Target System Base Module Administration Guide.

## Supported user account types

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

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

- Identity

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

**Table 19: 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                   |
| 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                        |



| Identity         | Description  | Value of the IdentityType column |
|------------------|--|----------------------------------|
| 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).

## 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. By default, the link between employee and SharePoint user account is set up through the authentication objects to which the user account is assigned. Alternatively, employees can also be directly linked to the user accounts. Such user accounts can be managed through account definitions. 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 settings are recommended for default user accounts:

- In the mapping rules for the `IsGroupAccount_SPSGroup` and `IsGroupAccount_SPSRLAsn` columns, use the default value **1** and set 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.

## **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.

You can label administrative user accounts as a **Personalized administrator identity** or as a **Shared identity**. Proceed as follows to provide the employees who use this user account with the required permissions.

- Personalized admin identity
  1. Use the `UID_Person` column to link the user account with an employee.  
Use an employee with the same identity or create a new employee.

2. Assign this employee to hierarchical roles.
- Shared identity
    1. Assign all employees with usage authorization to the user account.
    2. Link the user account to a pseudo employee using the UID\_Person column.  
Use an employee with the same identity or create a new employee.
    3. Assign this pseudo employee to hierarchical roles.
- The pseudo employee provides the user account with its permissions.

## 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\_SPSGroup and IsGroupAccount\_SPSRLAsgn columns 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.


## Entering main data of SharePoint user accounts

Each SharePoint user account represents an object from an authentication system. This object can be a group or a user. The group authentication and user authenticated user accounts are select separately in the navigation system.

### ***To edit the properties of a group authenticated user account***

1. Select the **SharePoint > User accounts (group authentication)** category.
2. Select the user account in the result list and run **Change main data**.  
- OR -  
Click  in the result list.
3. Edit the user account's resource data.
4. Save the changes.

### ***To edit the properties of a user authenticated user account.***

1. Select the **SharePoint > User accounts (user authentication)** category.
2. Select the user account in the result list and run **Change main data**.  
- OR -  
Click  in the result list.
3. Edit the user account's resource data.
4. Save the changes.

### ***To manually assign or create a user authenticated user account for an employee***

1. Select the **Employees > Employees** category.
2. Select the employee in the result list and run the **Assign SharePoint user accounts** task.

3. Assign a user account.
4. Save the changes.


### Detailed information about this topic

- [Group authenticated user account main data](#) on page 93
- [User authenticated user account main data](#) on page 95

## Group authenticated user account main data

Enter the following main data of a group authenticated user account.

**Table 20: Group authenticated user account main data**

| Property                        | Description   |
|---------------------------------|---|
| Employee                        | <p>Employee that uses this user account. The input field is only displayed if no authentication object is assigned. Select the employee from the menu.</p> <p>You can create a new employee for a user account with an identity of type <b>Organizational identity</b>, <b>Personalized administrator identity</b>, <b>Sponsored identity</b>, <b>Shared identity</b>, or <b>Service identity</b>. 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.</p> |
| No link to an employee required | <p>Specifies whether the user account is intentionally not assigned an employee. 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).</p> <p>If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an employee can be filtered according to various criteria.</p>   |
| Not linked to an employee       | <p>Indicates why the <b>No link to an employee required</b> option is enabled for this user account. The user account is not associated with an employee due to an exclusion criterion.</p>   |
| Site collection                 | <p>Site collection the user account is used in.</p>   |
| Group authenticated             | <p>Specifies whether the user account's authentication object is a group.</p>   |
| Authentication object           | <p>Authentication object referencing the user account. Each SharePoint user account represents an object from an authentication system trusted by the SharePoint installation. If this authentication system is</p>   |

| Property                | Description   |
|-------------------------|---|
|                         | <p>managed as a target system in One Identity Manager, the SharePoint object used for authentication can be saved as the authentication object in the user policy.</p> <p>The authentication object is assigned during automatic synchronization. You can assign an authentication object when setting up a new user account in the Manager. The authentication object cannot be changed after saving.</p> <p>The following authentication objects can be assigned to a group authenticated user account:</p> <ul style="list-style-type: none"> <li>• Active Directory groups with the type "Security group" from the domain assigned to the farm or a trusted domain</li> <li>• LDAP groups from the domain assigned to the farm</li> </ul> |
| Authentication mode     | <p>Authentication mode used for logging in on the SharePoint server with this user account.</p> <p>The login name of new user accounts depends on the authentication mode. The authentication mode is set by a template. The value depends on the <b>Claims-based authentication</b> option of the associated web application. If you have defined custom authentication modes, select your authentication mode in the menu.</p> <p><b>NOTE:</b> Modify the template for this column (SPSUser.UID_SPSAuthSystem) to assign a custom authentication mode to user accounts.</p>   |
| Display name            | <p>Any display name for the user account. By default, the display name is taken from the authentication object display name. Enter the display name by hand if no authentication object is assigned.</p>  |
| Login name              | <p>User account login name. It is found using a template. Enter the login name by hand if no authentication object is assigned.</p> <p><b>NOTE:</b> Modify the template for this column (SPSUser.LoginName) to assign a custom authentication mode to user accounts.</p>  |
| Email address           | <p>User account email address. It is formatted using templates from the authentication object's email address.</p>  |
| Risk index (calculated) | <p>Maximum risk index value of all assigned SharePoint roles and groups. The property is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>  |
| Category                | <p>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.</p>   |

| Property                 | Description   |
|--------------------------|---|
| Advice                   | Text field for additional explanation.  |
| Identity                 | <p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> <li>• <b>Primary identity:</b> Employee's default user account.</li> <li>• <b>Organizational identity:</b> Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</li> <li>• <b>Personalized administrator identity:</b> User account with administrative permissions, used by one employee.</li> <li>• <b>Sponsored identity:</b> User account to use for a specific purpose. Training, for example.</li> <li>• <b>Shared identity:</b> User account with administrative permissions, used by several employees. Assign all employees that use this user account.</li> <li>• <b>Service identity:</b> Service account.</li> </ul> |
| Privileged user account. | Specifies whether this is a privileged user account.  |
| Administrator            | Specifies whether the user account is a site collection administrator.  |
| Auditor                  | Specifies whether the user account is a site collection auditor.  |

### Detailed information about this topic


- [Authentication modes](#) on page 45
- [Specifying categories for inheriting SharePoint groups](#) on page 80
- [Supported user account types](#) on page 88
- One Identity Manager Identity Management Base Module Administration Guide

## User authenticated user account main data

Enter the following main data of a user authenticated user account.

**Table 21: User authenticated user account main data**

| Property | Description   |
|----------|---|
| 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 an authentication object is assigned, the connected employee |

| Property                        | Description  |
|---------------------------------|--|
|                                 | <p>is found through the authentication object by using a template. If there is no authentication object assigned, the employee can be assigned automatically or manually.</p> <p>You can create a new employee for a user account with an identity of type <b>Organizational identity</b>, <b>Personalized administrator identity</b>, <b>Sponsored identity</b>, <b>Shared identity</b>, or <b>Service identity</b>. 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.</p>                   |
| No link to an employee required | <p>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).</p> <p>If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an employee can be filtered according to various criteria.</p> |
| Not linked to an employee       | <p>Indicates why the <b>No link to an employee required</b> option is enabled for this user account. Possible values:</p> <ul style="list-style-type: none"> <li>• <b>By administrator:</b> The option was set manually by the administrator.</li> <li>• <b>By attestation:</b> The user account was attested.</li> <li>• <b>By exclusion criterion:</b> The user account is not associated with an employee due to an exclusion criterion. For example, the user account is included in the exclude list for automatic employee assignment (configuration parameter <b>PersonExcludeList</b>).</li> </ul>   |
| Manage level                    | <p>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.</p>  |
| Account definition              | <p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p><b>NOTE:</b> The account definition cannot be changed once the user account has been saved.</p>   |



| Property              | Description   |
|-----------------------|---|
|                       | <p><b>NOTE:</b> Use the user account's <b>Remove account definition</b> task to reset the user account to <b>Linked</b> status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (X0origin=1).</p> <p><b>NOTE:</b> If employees obtain their SharePoint user accounts through account definitions, the employees must own user accounts in the Active Directory domain or LDAP domain. This domain is stored in the SharePoint farm in which the SharePoint user accounts are to be created.</p>  |
| Site collection       | Site collection the user account is used in.  |
| Group authenticated   | Specifies whether the user account's authentication object is a group. This option is disabled for user authenticated user accounts.  |
| Authentication object | <p>Authentication object referencing the user account. Each SharePoint user account represents an object from an authentication system trusted by the SharePoint installation. If this authentication system is managed as a target system in One Identity Manager, the SharePoint object used for authentication can be saved as the authentication object in the user policy.</p> <p>The authentication object is assigned during automatic synchronization. You can assign an authentication object when setting up a new user account in the Manager. The authentication object cannot be changed after saving.</p> <p>The following authentication objects can be assigned to a user-authenticated user account:</p> <ul style="list-style-type: none"> <li>• Active Directory user accounts from the domain that is assigned to the farm or a trusted domain</li> <li>• LDAP user accounts from the domain assigned to the farm</li> </ul> <p>User accounts that refer to the default SIDs of an Active Directory environment cannot reference an authentication object in One Identity Manager.</p> <p><b>NOTE:</b> The SharePoint user account is also created if the user account that is used as the authentication object is disabled or locked.</p> |
| Authentication mode   | <p>Authentication mode used for logging in on the SharePoint server with this user account.</p> <p>The login name of new user accounts depends on the authentication mode. The authentication mode is set by a template. The value depends on the <b>Claims-based authentication</b> option of the</p>  |

| Property                 | Description   |
|--------------------------|---|
|                          | <p>associated web application. If you have defined custom authentication modes, select your authentication mode in the menu.</p> <p><b>NOTE:</b> Modify the template for this column (SPSUser.UID_SPSAuthSystem) to assign a custom authentication mode to user accounts.</p>   |
| Display name             | Any display name for the user account. By default, the display name is taken from the authentication object display name. Enter the display name by hand if no authentication object is assigned.   |
| Login name               | <p>User account login name. It is found using a template. Enter the login name by hand if no authentication object is assigned.</p> <p><b>NOTE:</b> Modify the template for this column (SPSUser.LoginName) to assign a custom authentication mode to user accounts.</p>  |
| Email address            | User account email address. It is formatted using templates from the authentication object's email address.   |
| Risk index (calculated)  | Maximum risk index value of all assigned SharePoint roles and groups. The property is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .  |
| Category                 | Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.  |
| Advice                   | Text field for additional explanation.  |
| Identity                 | <p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> <li>• <b>Primary identity:</b> Employee's default user account.</li> <li>• <b>Organizational identity:</b> Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</li> <li>• <b>Personalized administrator identity:</b> User account with administrative permissions, used by one employee.</li> <li>• <b>Sponsored identity:</b> User account to use for a specific purpose. Training, for example.</li> <li>• <b>Shared identity:</b> User account with administrative permissions, used by several employees. Assign all employees that use this user account.</li> <li>• <b>Service identity:</b> Service account.</li> </ul> |
| Privileged user account. | Specifies whether this is a privileged user account.  |

| Property                | Description   |
|-------------------------|---|
| Groups can be inherited | <p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> |
| Roles can be inherited  | <p>Specifies whether the user account can inherit SharePoint roles through the linked employee. If the option is set, the user account inherits the roles through hierarchical roles, in which the employee is a member, or through IT Shop requests.</p>   |
| Administrator           | <p>Specifies whether the user account is a site collection administrator.</p>   |
| Auditor                 | <p>Specifies whether the user account is a site collection auditor.</p>   |

### Detailed information about this topic

- [Setting up account definitions](#) on page 55
- [Authentication modes](#) on page 45
- [Specifying categories for inheriting SharePoint groups](#) on page 80
- [Assigning employees automatically to SharePoint user accounts](#) on page 102
- [Supported user account types](#) on page 88
- One Identity Manager Identity Management Base Module Administration Guide

## Additional tasks for managing SharePoint user accounts

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

# Displaying the SharePoint user account overview

## *To obtain an overview of a user account*

1. Select the **SharePoint > User accounts (group authenticated)** or the **SharePoint > User accounts (user authenticated)** category.
2. Select the user account in the result list.
3. Select the **SharePoint user account overview** task.

## Assigning SharePoint groups directly to a SharePoint user account

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


Only groups from the site collection to which the user account belongs can be assigned. You cannot directly assign groups that have the **Only use in IT Shop** option set.

## *To assign groups directly to user accounts*

1. Select the **SharePoint > User accounts (group authenticated)** or the **SharePoint > User accounts (user authenticated)** 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 SharePoint roles directly to user accounts](#) on page 101
- [Assigning SharePoint groups to SharePoint user accounts](#) on page 112

# Assigning SharePoint roles directly to user accounts

SharePoint roles can be assigned directly or indirectly to a user account. Indirect assignment is carried out by assigning the employee and SharePoint roles to hierarchical roles, like departments, cost centers, locations, or business roles. If the employee has a SharePoint user account, the SharePoint roles in the hierarchical roles are inherited by the user account. SharePoint roles can only be directly assigned to group authenticated user accounts.

Only SharePoint roles from the site collection to which the user account belongs can be assigned. You cannot directly assign SharePoint roles that have the **Only use in IT Shop** option set.

**NOTE:** SharePoint roles that reference permission levels set with **Hidden** cannot be assigned to user accounts.

## *To assign SharePoint roles directly to user accounts*

1. Select the **SharePoint > User accounts (group authenticated)** or the **SharePoint > User accounts (user authenticated)** category.
2. Select the user account in the result list.
3. Select the **Assign SharePoint roles** task.
4. In the **Add assignments** pane, assign roles.  
- OR -  
In the **Remove assignments** pane, remove the roles.
5. Save the changes.

## Related topics

- [Assigning SharePoint groups directly to a SharePoint user account](#) on page 100
- [Entering main data of SharePoint permission levels](#) on page 128

# Assigning extended properties

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

## *To specify extended properties for a user account*

1. Select the **SharePoint > User accounts (group authenticated)** or the **SharePoint > User accounts (user authenticated)** category.
2. Select the user account in the result list.
3. Select the **Assign extended properties** task.

4. Assign extended properties in **Add assignments**.  
- OR -  
Remove extended properties in **Remove assignments**.
5. Save the changes.

### Detailed information about this topic

- One Identity Manager Identity Management Base Module Administration Guide

## Using custom authentication modes

When user accounts are added, the values of various main data are determined using templates. One Identity Manager tries to identify and classify an authentication object using user account properties during synchronization. To use custom authentication modes, the templates of different columns must be modified if necessary. Create custom templates so that authentication modes can be assigned automatically to user accounts and the login names can be correctly formatted.

### To use custom authentication modes

1. In the Designer, adjust the templates for the `SPSUser.UID_SPSAuthSystem` column (authentication mode).
2. Test the template of `SPSUser.ObjectKeyNamespaceItem` (authentication modes) and `SPSUser.LoginName` columns (login name) and modify them if necessary.

### Detailed information about this topic

- [Authentication modes](#) on page 45
- One Identity Manager Configuration Guide

## Assigning employees automatically to SharePoint user accounts

**Table 22: Configuration parameters for automatic employee assignment**

| Configuration parameter                        | Meaning   |
|--|---|
| TargetSystem   SharePoint   PersonAutoFullSync | Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization. |

| Configuration parameter                       | Meaning   |
|---|---|
| TargetSystem   SharePoint   PersonAutoDefault | Mode for automatic employee assignment for user accounts added to the database outside synchronization. |

When you add a user authenticated user account, an existing employee can automatically be assigned to it. This mechanism can be triggered after a new user account is created either manually or through synchronization.

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

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

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

#### Prerequisites:

- **Group authenticated** is not set in the user accounts.
- The user accounts are not assigned an authentication object

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 | SharePoint | PersonAutoFullsync" configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the "TargetSystem | SharePoint | PersonAutoDefault" configuration parameter and select the required mode.
- Assign an account definition to the site collection. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employees assigned to the site collection.

#### 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.

## Related topics

- [Creating an account definition](#) on page 56
- [Assigning account definitions to a target system](#) on page 71
- [Editing search criteria for automatic employee assignment](#) on page 104

# 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 site collection. 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 SPSSite 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. Select the **SharePoint > Site collections** category.
2. Select the site collection 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 23: Standard search criteria for user accounts**

| Apply to                           | Column for employee                   | Column for user account |
|------------------------------------|---------------------------------------|-------------------------|
| User accounts (user authenticated) | Central user account (CentralAccount) | Login name (LoginName)  |



5. Save the changes.

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

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

**Table 24: Manual assignment view**

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

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

### To apply search criteria to user accounts

- Click **Reload**.

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

### To assign employees directly using a suggestion list

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

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

- c. Click **Assign selected**.
- d. Confirm the security prompt with **Yes**.

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

### **To remove assignments**


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

The assigned employees are removed from the selected user accounts.


## Deleting and restoring SharePoint 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.

### **To delete a user account**

1. Select the **SharePoint > User accounts (group authenticated)** or the **SharePoint > User accounts (user authenticated)** category.
2. Select the user account in the result list.
3. Click  to delete the user account.
4. Confirm the security prompt with **Yes**.

### **To restore a user account**

1. Select the **SharePoint > User accounts (group authenticated)** or the **SharePoint > User accounts (user authenticated)** category.
2. Select the user account in the result list.
3. Click  in the result list.

When an authentication object assigned to a SharePoint user account is deleted from the One Identity Manager database, the link to the authentication object is removed from the SharePoint user account. Define a custom process to delete these user accounts from the One Identity Manager database.

## Configuring deferred deletion

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 **SPSUser** 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 **SPSUser** table.

### Example:

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

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

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

**NOTE:** SharePoint user accounts cannot be locked. A user account marked for deletion remains enabled until deferred deletion has expired and the user account is finally deleted from the One Identity Manager database.

Lock the user account linked to the SharePoint user account as authentication object to prevent a user from logging into a site when the SharePoint user account is marked for deletion.

## SharePoint roles and groups

User accounts inherit SharePoint permissions through SharePoint roles and SharePoint groups. SharePoint groups are always defined for one site collection in this way. SharePoint roles are defined for sites. They are assigned to groups, and the user accounts that are members of these groups inherit SharePoint permissions through them. SharePoint roles can also be assigned directly to user accounts. User account permissions on individual sites in a site collection are restricted through the SharePoint roles that are assigned to it.

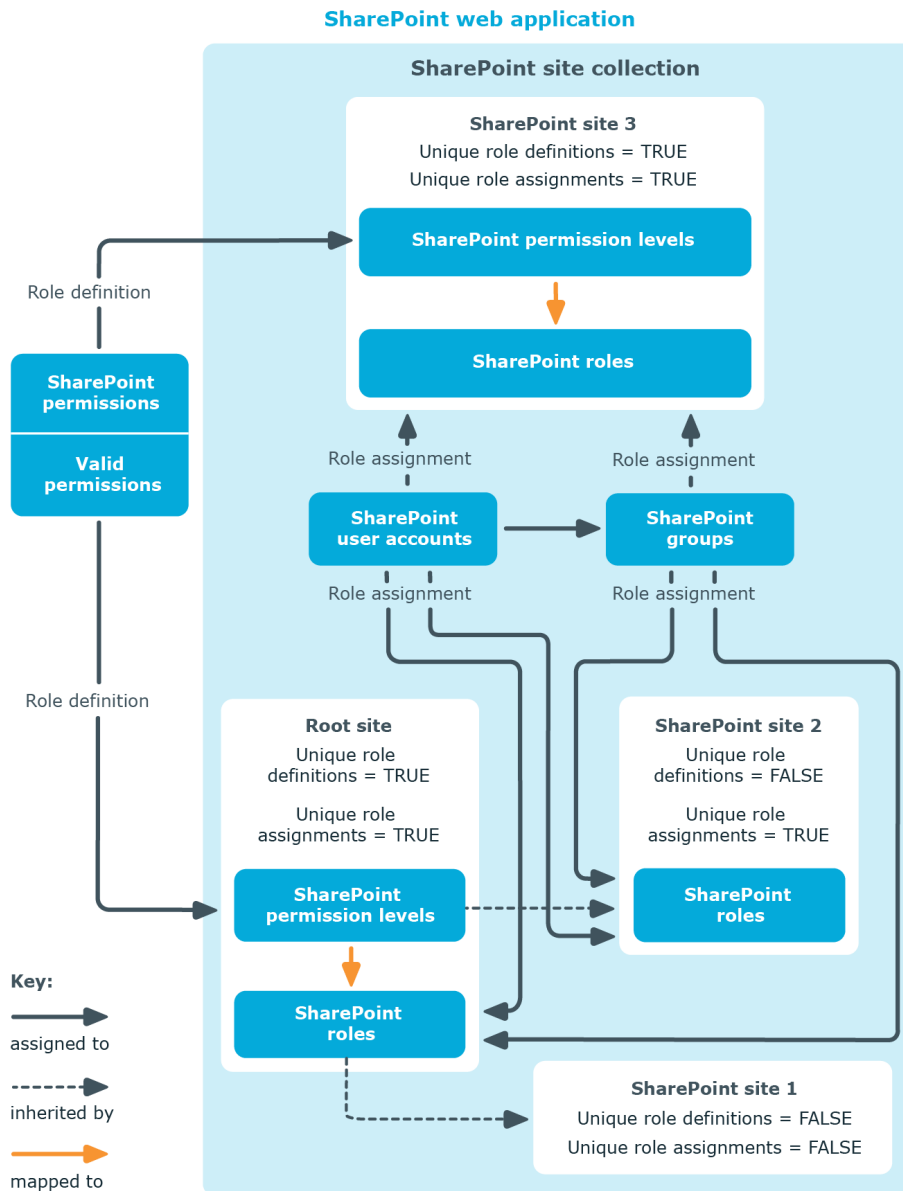
### Terms

- A SharePoint Role is the permission level linked to a fixed site.
- The assignment of SharePoint permissions to a permission level is called a role definition.
- The assignment of user account or groups to a SharePoint role is called a role assignment.

Child sites can inherit permissions from the sites that the user accounts have on those sites. Every root site of a site collection or every site that has a child site. This permits the following scenarios:

1. The child site inherits role definitions and role assignments.  
The permission levels and role definitions are valid as well as the role assignments from the parent (inheritance) site. User and groups cannot be explicitly authorized for the site. Only user accounts that have permissions for the parent (inheritance) site have access to the site.
2. The child site inherits the role definitions and role assignments.  
You cannot define unique permission levels for child site. The SharePoint roles for this site reference the permission levels of the parent (inheritance) site and its role definitions. User accounts and groups can be assigned to the SharePoint roles of the child site based on this. If there are unique permission levels defined for the child site the permissions are overwritten by the inherited permissions.
3. The child site does not inherit role definitions or role assignments.  
In this case unique permission levels with their role definitions can be added in the same way as the root site. The SharePoint roles based on the definitions are assigned to user accounts and groups.

**Figure 2: SharePoint user accounts inheriting SharePoint permissions in One Identity Manager**




## SharePoint groups

You can use groups in SharePoint to provide users with the same permissions. Groups that you add for site collections are valid for all sites in that site collection. SharePoint roles that you define for a site are assigned directly to groups. All user accounts that are members of these groups obtain the permissions defined in the SharePoint roles for this site.

You can edit the following group data in the One Identity Manager:

- Object properties like display name, owner, or visibility of memberships
- Assigned SharePoint role and user accounts
- Usage in the IT Shop
- Risk assessment
- Inheritance through roles and inheritance restrictions

### **To edit group main data**

1. Select the **SharePoint > Groups** category.
2. Select the group in the result list. Select the **Change main data** task.  
- OR -  
Click  in the result list.
3. Enter the required data on the main data form.
4. Save the changes.

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

- [Entering main data of SharePoint groups](#) on page 110

### **Related topics**

- [SharePoint roles and groups](#) on page 108

## **Entering main data of SharePoint groups**

**Table 25: Configuration parameters for setting up SharePoint groups**

| <b>Configuration parameter</b> | <b>Meaning</b>  |
|--------------------------------|---|
| QER   CalculateRiskIndex       | Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database.<br><br>If the parameter is enabled, values for the risk index can be entered and calculated. |

Enter the following main data of a group.

**Table 26: SharePoint group main data**

| <b>Property</b> | <b>Description</b>         |
|-----------------|----------------------------|
| Display name    | Display name of the group. |

| Property                            | Description  |
|-------------------------------------|--|
| Site collection                     | Site collection the group is used in.  |
| Owner                               | Owner of the group. A SharePoint user account or a SharePoint group can be selected.   |
| Service item                        | Service item data for requesting the group through the IT Shop.  |
| Distribution group alias            | Alias of the distribution group that the group is linked to.   |
| Distribution group email            | Email address of the distribution group that the group is linked to.   |
| Risk index                          | Value for evaluating the risk of assigning the group to user accounts. Set a value in the range <b>0</b> to <b>1</b> . This input field is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is activated.   |
| 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.   |
| Description                         | Text field for additional explanation.   |
| Description (HTML)                  | Additional information about the group in HTML format. (this is displayed in SharePoint in the description field "About me").  |
| Memberships only visible to members | Specifies whether only group members can see the list of members.  |
| Group members can edit memberships  | Specifies whether all group members can edit the group memberships.  |
| Request for membership permitted    | Specifies whether SharePoint users can request or end membership in these groups themselves.   |
| Automatic membership on request     | Specifies whether SharePoint users automatically become members in the group once they request membership. The same applies when user end their membership.  |
| Email address membership requested  | Email address that the group membership request or closure is sent to.   |
| 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. |

| Property                | Description   |
|-------------------------|---|
| 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. |

### Detailed information about this topic

- [Specifying categories for inheriting SharePoint groups](#) on page 80
- [SharePoint group inheritance based on categories](#) on page 123
- One Identity Manager IT Shop Administration Guide
- One Identity Manager Risk Assessment Administration Guide

## Assigning SharePoint groups to SharePoint user accounts

Groups can be assigned directly or indirectly to employees. In the case of indirect assignment, employees and groups are arranged in hierarchical roles. The number of groups assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance.

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

- Assignment of employees and groups is permitted for role classes (departments, cost centers, locations, or business roles).
- The **Group authenticated** option is not set in the user accounts.
- User accounts are marked with the **Groups can be inherited** option.
- User accounts and groups belong to the same site collection.

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

### Detailed information about this topic

- [Assigning SharePoint groups to departments, cost centers and locations](#) on page 113
- [Assigning SharePoint groups to business roles](#) on page 114
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 115
- [Assigning SharePoint roles to SharePoint groups](#) on page 116




- [Adding SharePoint groups to system roles](#) on page 116
- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Adding SharePoint groups automatically to the IT Shop](#) on page 119
- One Identity Manager Identity Management Base Module Administration Guide

## Assigning SharePoint groups to departments, cost centers and locations

Assign groups to departments, cost centers, and locations in order to assign user accounts to them through these organizations.

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

1. In the Manager, select the **SharePoint > 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 SharePoint groups** task.
4. In the **Add assignments** pane, assign groups.

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

**To remove an assignment**

- Select the group and double-click .

5. Save the changes.

## Related topics

- [Assigning SharePoint groups to business roles](#) on page 114
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 115
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint groups to system roles](#) on page 116
- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Adding SharePoint groups automatically to the IT Shop](#) on page 119
- [One Identity Manager users for managing SharePoint](#) on page 10

# Assigning SharePoint groups to business roles

Installed modules: Business Roles Module


You assign groups to business roles in order to assign them to user accounts through business roles.

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

1. In the Manager, select the **SharePoint > 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 SharePoint 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 SharePoint groups to departments, cost centers and locations](#) on page 113
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 115
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint groups to system roles](#) on page 116
- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Adding SharePoint groups automatically to the IT Shop](#) on page 119
- [One Identity Manager users for managing SharePoint](#) on page 10

## Assigning SharePoint user accounts directly to a SharePoint group

Groups can be assigned directly or indirectly to user accounts. Indirect assignment can only be used for user authenticated user accounts. Direct assignment can only be used for group and user authenticated user accounts.

User accounts and groups must belong to the same site collection.

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

1. Select the **SharePoint > Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign user accounts.  
- OR -  
In the **Remove assignments** pane, remove user accounts.
5. Save the changes.

## Related topics

- [Assigning SharePoint groups directly to a SharePoint user account](#) on page 100
- [Assigning SharePoint groups to departments, cost centers and locations](#) on page 113

- [Assigning SharePoint groups to business roles](#) on page 114
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint groups to system roles](#) on page 116
- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Adding SharePoint groups automatically to the IT Shop](#) on page 119

## Assigning SharePoint roles to SharePoint groups

In order for SharePoint user accounts to obtain permissions for individual websites, assign SharePoint roles to the groups. SharePoint roles and groups must belong to the same site collection.

**NOTE:** SharePoint roles with the **Hidden** option that reference permission levels, cannot be assigned to groups.

### *To assign SharePoint roles to a group*

1. Select the **SharePoint > Groups** category.
2. Select the group in the result list.
3. Select the **Assign SharePoint roles** task.
4. In the **Add assignments** pane, assign roles.  
- OR -  
In the **Remove assignments** pane, remove the roles.
5. Save the changes.

### Related topics

- [Entering main data of SharePoint permission levels](#) on page 128
- [Assigning SharePoint groups to SharePoint roles](#) on page 135
- [Assigning SharePoint groups to departments, cost centers and locations](#) on page 113
- [Assigning SharePoint groups to business roles](#) on page 114
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 115
- [Adding SharePoint groups to system roles](#) on page 116
- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Adding SharePoint groups automatically to the IT Shop](#) on page 119

## Adding SharePoint 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 user authenticated accounts owned by these employees inherit the group.


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

### **To assign a group to system roles**

1. In the Manager, select the **SharePoint > 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 the system role assignment.

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

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

### **Related topics**

- [Assigning SharePoint groups to departments, cost centers and locations](#) on page 113
- [Assigning SharePoint groups to business roles](#) on page 114
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 115
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Adding SharePoint groups automatically to the IT Shop](#) on page 119

## **Adding SharePoint groups to the IT Shop**

When you assign a group 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 a service item.

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

- If you only want the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

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

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

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

***To remove a group from individual shelves of the IT Shop***

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

***To remove a group from all shelves of the IT Shop***

1. In the Manager, select the **SharePoint > Groups** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > SharePoint groups** (role-based login) category.
2. In the result list, select the group.
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.

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

## Related topics

- [Entering main data of SharePoint groups on page 110](#)
- [Adding SharePoint groups automatically to the IT Shop on page 119](#)
- [Assigning SharePoint groups to departments, cost centers and locations on page 113](#)
- [Assigning SharePoint groups to business roles on page 114](#)
- [Assigning SharePoint user accounts directly to a SharePoint group on page 115](#)
- [Assigning SharePoint roles to SharePoint groups on page 116](#)
- [Adding SharePoint groups to system roles on page 116](#)

## Adding SharePoint groups automatically to the IT Shop

The following steps can be used to automatically add SharePoint groups to the IT Shop. Synchronization ensures that the SharePoint groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor. New SharePoint groups created in One Identity Manager also are added automatically to the IT Shop.

### *To add SharePoint groups automatically to the IT Shop*

1. In the Designer, set the **QER | ITShop | AutoPublish | SPSGroup** configuration parameter.
2. In order not to add SharePoint groups to the IT Shop automatically, in the Designer, set the **QER | ITShop | AutoPublish | SPSGroup | ExcludeList** configuration parameter.

This configuration parameter contains a listing of all SharePoint groups that should not be allocated to the IT Shop automatically. You can extend this list if required. To do this, enter the name of the groups in the configuration parameter. Names are listed in a pipe (|) delimited list. Regular expressions are supported.

3. Compile the database.

The SharePoint groups are added automatically to the IT Shop from now on.

The following steps are run to add a SharePoint group to the IT Shop.

1. A service item is determined for the SharePoint group.

The service item is tested for each SharePoint group and modified if necessary. The name of the service item corresponds to the name of the SharePoint group.

  - The service item is modified for SharePoint groups with service items.
  - SharePoint groups without service items are allocated new service items.
2. The service item is assigned to the **SharePoint groups** default service category.

3. An application role for product owners is determined and assigned to the service item.

Product owners can approve requests for membership in these SharePoint groups. The default product owner is the SharePoint group's owner.

**NOTE:** The application role for the product owner must be added under the **Request & Fulfillment | IT Shop | Product owner** application role.

- If the owner of the SharePoint group is already a member of an application role for product owners, this application role is assigned to the service item. Therefore, all members of this application role become product owners of the SharePoint group.
  - If the owner of the SharePoint group is not yet a member of an application role for product owners, a new application role is created. The name of the application corresponds to the name of the owner.
    - If the owner is a user account, the user account's employee is added to the application role.
    - If it is a group of owners, the employees of all this group's user accounts are added to the application role.
  - If the SharePoint group does not have an owner, the **Request & Fulfillment | IT Shop | Product owner | Without owner in SharePoint** default application role is used.
4. The SharePoint group is labeled with the **IT Shop** option and assigned to the **IT Shop groups** SharePoint shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can use the Web Portal to request memberships in SharePoint groups.

**NOTE:** If a SharePoint group is irrevocably deleted from the One Identity Manager database, the associated service item is also deleted.

For more information about configuring the IT Shop, see the *One Identity Manager IT Shop Administration Guide*. For more information about requesting access requests in the Web Portal, see the *One Identity Manager Web Portal User Guide*.

## Related topics

- [Adding SharePoint groups to the IT Shop](#) on page 117
- [Assigning SharePoint groups to departments, cost centers and locations](#) on page 113
- [Assigning SharePoint groups to business roles](#) on page 114
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 115
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint groups to system roles](#) on page 116
- [Default solutions for requesting SharePoint groups](#) on page 126



# Additional tasks for managing SharePoint groups

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

## Displaying an overview of SharePoint groups

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

### *To obtain an overview of a group*

1. Select the **SharePoint > Groups** category.
2. Select the group in the result list.
3. Select the **SharePoint group overview** task.

## Effectiveness of group memberships

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.

The effectiveness of the assignments is mapped in the `SPSUserInSPSGroup` and `BaseTreeHasSPSGroup` tables by the `XIsInEffect` column.

### Example: The effect of group memberships

- The groups A, B, and C are defined in a site collection.
- Group A is assigned through the "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

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

By using suitable controls, you want to prevent an employee from obtaining authorizations of groups A and group B at the same time. That means, groups A, B, and C are mutually exclusive. A user, who is a member of group C cannot be a member of group B at the same time. That means, groups B and C are mutually exclusive.

**Table 27: Specifying excluded groups (SPSGroupExclusion table)**

| Effective group | Excluded group |
|-----------------|----------------|
| Group A         |                |
| Group B         | Group A        |
| Group C         | Group B        |

**Table 28: Effective assignments**

| Employee      | Member in role                    | Effective group  |
|---------------|-----------------------------------|------------------|
| Pat Identity1 | Marketing                         | Group A          |
| Jan User3     | Marketing, finance                | Group B          |
| Jo User1      | Marketing, finance, control group | Group C          |
| Chris User2   | Marketing, control group          | Group A, Group C |

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

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

**Table 29: Excluded groups and effective assignments**

| Employee    | Member in role | Assigned group | Excluded group     | Effective group |
|-------------|----------------|----------------|--------------------|-----------------|
| Chris User2 | Marketing      | Group A        |                    | Group C         |
|             | Control group  | Group C        | Group B<br>Group A |                 |

## Prerequisites

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

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

**NOTE:** If you disable the configuration parameter at a later date, model components and scripts that are 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 site collection.

### To exclude a group

1. In the Manager, select the **SharePoint > 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.

## SharePoint 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**.

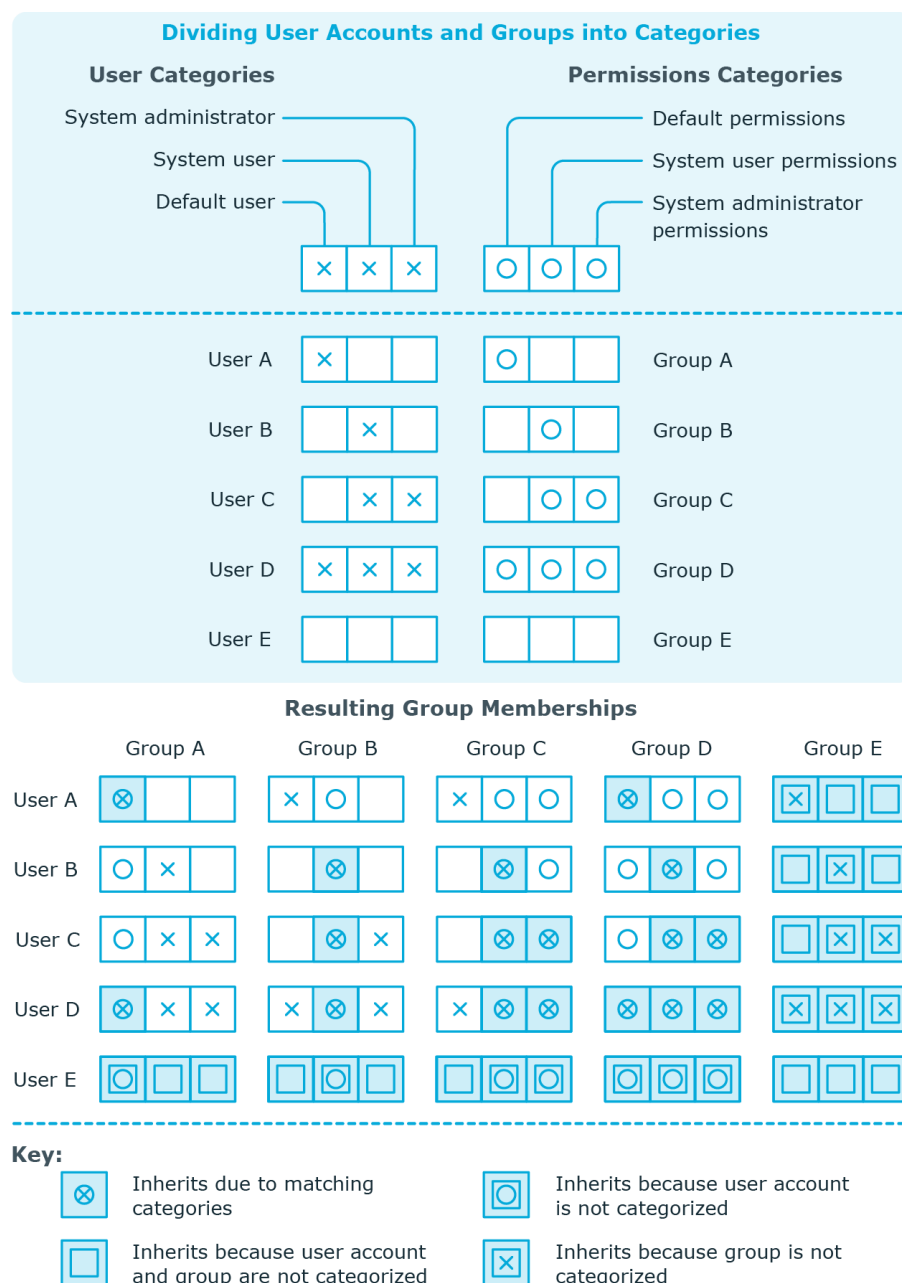
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or 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 30: 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 3: Example of inheriting through categories.**



### ***To use inheritance through categories***

1. Define the categories in the site collection.
2. Assign categories to user accounts through their main data.
3. Assign categories to groups through their main data.

### **Related topics**

- [Specifying categories for inheriting SharePoint groups](#) on page 80
- [User authenticated user account main data](#) on page 95
- [Group authenticated user account main data](#) on page 93
- [Entering main data of SharePoint groups](#) on page 110

## **Assigning extended properties to SharePoint groups**

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


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

### ***To specify extended properties for a group***

1. In the Manager, select the **SharePoint > 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 SharePoint groups**

### ***To delete a group***

1. Select the **SharePoint > Groups** category.
2. Select the group in the result list.

3. Click  to delete the group.
4. Confirm the security prompt with **Yes**.

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

## Default solutions for requesting SharePoint groups

In One Identity Manager, standard products and default approval workflows are provided for requesting SharePoint groups and membership in these groups through the IT Shop. Permissions in this target system are therefore issued by defined approval processes.

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

### Detailed information about this topic

- [Adding SharePoint groups](#) on page 126
- [SharePointRequesting Groups Memberships](#) on page 127

## Adding SharePoint groups

New SharePoint groups can be created in the SharePoint environment by a request for this standard product. The requester provides information about the name and site collection, if known, of the request. Based on this information, the target system manager specifies the container, in which the group will be added and grants approval for the request. The group is created in One Identity Manager and published to the target system.

### Prerequisite

- Employees are assigned to the **Target systems | SharePoint** application role.

If the **QER | ITShop | AutoPublish | SPSGroup** configuration parameter is set, the group is added to the IT Shop and the assigned to the **Identity & Access Lifecycle | SharePoint groups** shelf. The group is assigned to the existing service category.

**Table 31: Standard product for requesting a SharePoint group**

|                                      |   |
|--------------------------------------|---|
| Product                              | Adding a SharePoint group                     |
| Service category                     | SharePoint groups                             |
| Shelf                                | Identity & Access Lifecycle   Group Lifecycle |
| Approval policies/approval workflows | Approval of SharePoint group create requests  |

## Related topics

- [Adding SharePoint groups automatically to the IT Shop](#) on page 119

## SharePointRequesting Groups Memberships

Product owners and target system managers can request members for groups in these shelves in the Web Portal. The respective product owner or target system manager must grant approval for this modification. The changes are published in the target system.

**Table 32: Default objects for requesting group memberships**

|                                       |   |
|---------------------------------------|---|
| Shelves:                              | Identity & Access Lifecycle > SharePoint groups |
| Approval policies/approval workflows: | Approval of group membership requests           |

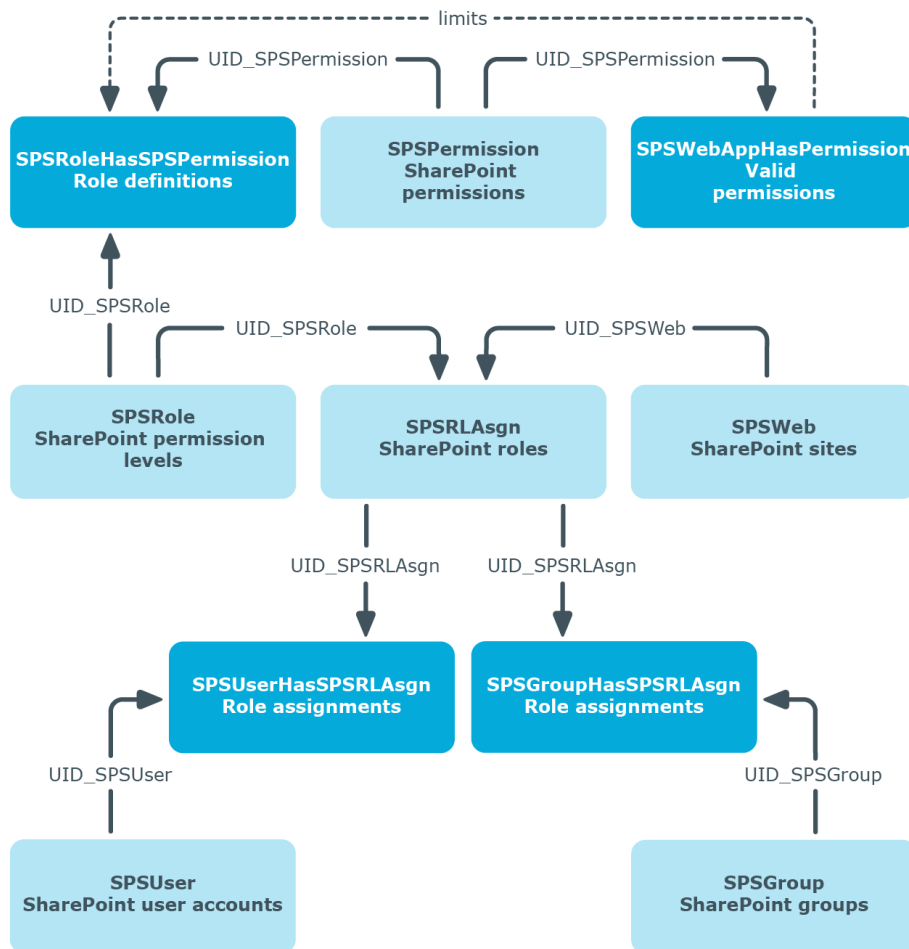
## Related topics

- [Adding SharePoint groups automatically to the IT Shop](#) on page 119
- [Adding SharePoint groups](#) on page 126

## SharePoint roles and permission levels


You can define so-called permission levels in SharePoint to grant permissions to objects in a site. These permission levels group together different SharePoint permissions. Permission levels with a unique reference to a site are mapped in the One Identity Manager database as SharePoint roles. You can assign SharePoint roles through groups, or directly to user accounts. SharePoint users obtain their permissions for site objects in this way.

**Figure 4: SharePoint roles and permission levels in One Identity Manager**



## Entering main data of SharePoint permission levels

### *To edit main data of a permission level*

1. Select the **SharePoint > Permission levels** category.
2. Select the permission level in the result list. Select the **Change main data** task.  
- OR -  
Click  in the result list.
3. Enter the required data on the main data form.
4. Save the changes.

Enter the following properties for a permission level on the main data form:



**Table 33: Properties of a permission level**

| Property         | Description   |
|------------------|---|
| Permission level | Name of the permission level.   |
| Site             | Unique identifier for the site the permission level is added to.  |
| Description      | Text field for additional explanation.  |
| Hidden           | Specifies whether a SharePoint role with the permission level can be assigned to user accounts or groups. |

## Additional tasks for managing SharePoint permission levels

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

### Displaying the SharePoint permission level overview

#### *To obtain an overview of a permission level*

1. Select the **SharePoint > Permission levels** category.
2. Select the permission level in the result list.
3. Select the **SharePoint permission level overview** task.

## Assigning permissions

You can assign One Identity Manager permission levels in SharePoint. Only valid permissions for web applications can be assigned. User account obtain these site permissions through a SharePoint internal inheritance procedure.

Permissions may depend on other permissions. SharePoint assigns these dependent permissions automatically. For example, the permissions "view pages", "browse user information", and "open" are always passed down with the permission "create groups".

**NOTE:** Dependent permissions cannot be automatically assigned in the One Identity Manager.

### **To assign permissions to permission levels**

1. Select the **SharePoint > Permission levels** category.
2. Select the permission level in the result list.
3. Select the **Assign permission** task.
4. In the **Add assignments** pane, assign permission.  
- OR -  
In the **Remove assignments** pane, remove permission.
5. Save the changes.

### **Related topics**

- [SharePoint roles and groups](#) on page 108

## **Special synchronization cases for valid permissions**

If you remove permissions from the list of valid permissions for a web application in SharePoint, the permissions cannot be assigned to permission levels within the web application from this point on. Assignments to permission levels that already exist for these permissions remain intact but are not active. These permissions are deleted from the SPSWebAppHasPermission table during synchronization. Assignments to permission levels that already exist for these permissions are not changed. Inactive permissions are displayed in the permission levels' overview.

## **Entering main data of SharePoint roles**

**Table 34: Configuration parameters for setting up SharePoint roles**

| <b>Configuration parameter</b> | <b>Meaning</b>   |
|--------------------------------|--|
| QER   CalculateRiskIndex       | <p>Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database.</p> <p>If the parameter is enabled, values for the risk index can be entered and calculated.</p> |

### **To edit SharePoint role main data**

1. Select the **SharePoint > Roles** category.
2. Select the SharePoint role in the result list. Select the **Change main data** task.

3. Enter the required data on the main data form.
4. Save the changes.

The following properties are displayed for SharePoint roles.

**Table 35: SharePoint role properties**

| Property                | Description   |
|-------------------------|---|
| Display name            | SharePoint role display name.   |
| Permission level        | Unique identifier for the permission level on which the SharePoint role is based.   |
| Site                    | Unique identifier for the site that inherits its permissions from the SharePoint role.  |
| Risk index              | Value for evaluating the risk of assigning the SharePoint role to user accounts. Enter a value between 0 and 1. The field is only visible if the "QER   CalculateRiskIndex" configuration parameter is set.   |
| Description             | Text field for additional explanation.  |
| Service item            | Service item data for requesting the group through the IT Shop.   |
| IT Shop                 | Specifies whether the SharePoint role can be requested through the IT Shop. This SharePoint role can be requested by staff through the Web Portal and granted through a defined approval procedure. The SharePoint role can still be assigned directly to employees and hierarchical roles. |
| Only for use in IT Shop | Specifies whether the SharePoint role can only be requested through the IT Shop. This SharePoint role can be requested by staff through the Web Portal and granted through a defined approval procedure. The SharePoint role may not be assigned directly to hierarchical roles.            |

**NOTE:** If the SharePoint role references a permission level for which the **Hidden** option is set, the options **IT Shop** and **Only use in IT Shop** cannot be set. You cannot assign these SharePoint roles to user accounts or groups.

### Detailed information about this topic

- [Entering main data of SharePoint permission levels](#) on page 128
- One Identity Manager IT Shop Administration Guide
- One Identity Manager Risk Assessment Administration Guide

# Assigning SharePoint roles to SharePoint user accounts

SharePoint roles can be assigned directly or indirectly to user accounts. In the case of indirect assignment, employees and SharePoint roles are arranged in hierarchical roles. The number of SharePoint roles assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If you add an employee to hierarchical roles and the employee owns a user authenticated user account, the user account is added to the SharePoint role. Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and groups is permitted for role classes (departments, cost centers, locations, or business roles).
- The **Group authenticated** option is not set in the user accounts.
- User accounts are labeled with the **Roles can be inherited** option.
- User accounts and SharePoint groups belong to the same site collection.

Furthermore, SharePoint roles can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that SharePoint roles can be assigned through IT Shop requests. All SharePoint roles, which are assigned to this shop as products, can be requested by the customers. Requested SharePoint roles are assigned to the employees after approval is granted.

**NOTE:** SharePoint roles that reference permission levels with have **Hidden** set, cannot be assigned to business roles and organizations. These SharePoint roles can be neither directly nor indirectly assigned to user accounts or groups.

## Detailed information about this topic

- [Entering main data of SharePoint permission levels](#) on page 128
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 132
- [Assigning SharePoint roles to business roles](#) on page 134
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 135
- [Assigning SharePoint groups to SharePoint roles](#) on page 135
- [Adding SharePoint roles to system roles](#) on page 136
- [Adding SharePoint roles to the IT Shop](#) on page 137
- One Identity Manager Identity Management Base Module Administration Guide

## Assigning SharePoint roles to departments, cost centers and locations


Assign SharePoint roles to departments, cost centers and locations in order to assign user accounts to them through these organizations.

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

1. Select the **SharePoint > Roles** category.
2. Select the role 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 SharePoint roles to departments, cost centers, or locations (role-based login)***

1. Select the **Organizations > Departments** category.
  - OR -
  - Select the **Organizations > Cost centers** category.
  - OR -
  - Select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign SharePoint roles** task.
4. In the **Add assignments** pane, assign SharePoint roles.
  - OR -
  - In the **Remove assignments** pane, remove SharePoint roles.
5. Save the changes.

### **Related topics**

- [Assigning SharePoint roles to business roles](#) on page 134
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 135
- [Assigning SharePoint groups to SharePoint roles](#) on page 135
- [Adding SharePoint roles to system roles](#) on page 136
- [Adding SharePoint roles to the IT Shop](#) on page 137
- [One Identity Manager users for managing SharePoint](#) on page 10

# Assigning SharePoint roles to business roles

Installed modules: Business Roles Module

You assign SharePoint roles to business roles in order to assign them to user accounts over business roles.

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

1. Select the **SharePoint > Roles** category.
2. Select the role in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.  
- OR -  
In the **Remove assignments** pane, remove business roles.
5. Save the changes.

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

1. Select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign SharePoint roles** task.
4. In the **Add assignments** pane, assign SharePoint roles.  
- OR -  
In the **Remove assignments** pane, remove SharePoint roles.
5. Save the changes.

## **Related topics**

- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 132
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 135
- [Assigning SharePoint groups to SharePoint roles](#) on page 135
- [Adding SharePoint roles to system roles](#) on page 136
- [Adding SharePoint roles to the IT Shop](#) on page 137
- [One Identity Manager users for managing SharePoint](#) on page 10

# Assigning SharePoint user accounts directly to a SharePoint role

SharePoint roles can be assigned directly or indirectly to user accounts. Indirect assignment can only be used for user authenticated user accounts. Direct assignment can only be used for group and user authenticated user accounts.

User accounts and SharePoint roles must belong to the same site collection.

**NOTE:** SharePoint roles that reference permission levels and have the option **hidden** set, cannot be assigned to user accounts.

## *To assign a SharePoint role directly to user accounts*

1. Select the **SharePoint > Roles** category.
2. Select the role in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign user accounts.  
- OR -  
In the **Remove assignments** pane, remove user accounts.
5. Save the changes.

## Related topics

- [Entering main data of SharePoint permission levels on page 128](#)
- [Assigning SharePoint roles directly to user accounts on page 101](#)
- [Assigning SharePoint roles to departments, cost centers and locations on page 132](#)
- [Assigning SharePoint roles to business roles on page 134](#)
- [Assigning SharePoint groups to SharePoint roles on page 135](#)
- [Adding SharePoint roles to system roles on page 136](#)
- [Adding SharePoint roles to the IT Shop on page 137](#)

# Assigning SharePoint groups to SharePoint roles

In order for SharePoint user accounts to obtain permissions for individual websites, assign SharePoint roles to the groups. SharePoint roles and groups must belong to the same site collection.

**NOTE:** SharePoint roles with the **Hidden** option that reference permission levels, cannot be assigned to groups.

### ***To assign groups to a SharePoint role***

1. Select the **SharePoint > Roles** category.
2. Select the role in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign groups.  
- OR -  
In the **Remove assignments** pane, remove groups.
5. Save the changes.

### **Related topics**

- [Entering main data of SharePoint permission levels](#) on page 128
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 132
- [Assigning SharePoint roles to business roles](#) on page 134
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 135
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint roles to system roles](#) on page 136
- [Adding SharePoint roles to the IT Shop](#) on page 137

## **Adding SharePoint roles to system roles**

Installed modules: System Roles Module

Use this task to add a SharePoint role to system roles. If you assign a system role to employees, all authenticated user accounts owned by these employees inherit the SharePoint role.

**NOTE:** If the SharePoint role references a permission level for which the **Hidden** option is enabled, system roles cannot be assigned. These SharePoint roles cannot be assigned to user accounts or groups, either directly or indirectly. For more information, see [Entering main data of SharePoint permission levels](#) on page 128.

**NOTE:** SharePoint roles with the **Only use in IT Shop** option 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 SharePoint role to system roles***

1. Select the **SharePoint > Roles** category.
2. Select the role 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 the system role assignment.

**To remove an assignment**

- Select the system role and double-click .

5. Save the changes.

## Related topics

- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 132
- [Assigning SharePoint roles to business roles](#) on page 134
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 135
- [Assigning SharePoint roles to SharePoint groups](#) on page 116
- [Adding SharePoint roles to the IT Shop](#) on page 137

## Adding SharePoint roles to the IT Shop

Once a SharePoint role 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 SharePoint role must be labeled with the **IT Shop** option.
- The SharePoint role must be assigned to a service item.
- The SharePoint role must be also labeled with the **Only use in IT Shop** option if the SharePoint role can only be assigned to employees using IT Shop requests. Direct assignment to hierarchical roles may not be possible.

**NOTE:** IT Shop administrators can assign SharePoint roles to IT Shop shelves in the case of role-based login. Target system administrators are not authorized to add SharePoint roles in the IT Shop.

### **To add a SharePoint role to the IT Shop**

1. Select the **SharePoint > Roles** category.
2. Select the role in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the IT Shop shelves.
5. Save the changes.

### **To remove a SharePoint role from individual IT Shop shelves**

1. Select the **SharePoint > Roles** category.
2. Select the role 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.

#### ***To remove a SharePoint roles from all IT Shop shelves***

1. Select the **SharePoint > Roles** category.
2. Select the role 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 SharePoint role is removed from all shelves by the One Identity Manager Service. All requests and assignment requests are canceled along with the SharePoint role as a result.

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

- One Identity Manager IT Shop Administration Guide

#### **Related topics**

- [Entering main data of SharePoint roles](#) on page 130
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 132
- [Assigning SharePoint roles to business roles](#) on page 134
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 135
- [Assigning SharePoint groups to SharePoint roles](#) on page 135
- [Adding SharePoint roles to system roles](#) on page 136

## **Additional tasks for managing SharePoint roles**

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

### **Displaying the SharePoint rules overview**

#### ***To obtain an overview of a SharePoint role***

1. Select the **SharePoint > Roles** category.
2. Select the role in the result list.

3. Select the **SharePoint role overview** task.

## Effectiveness of SharePoint roles

The behavior described under [Effectiveness of group memberships](#) on page 121 can also be used for SharePoint roles.

The effect of the assignments is mapped in the `SPSUserHasSPSRLAssign` and `BaseTreeHasSPSRLAssign` tables through the column `XIsInEffect`.

### Prerequisites

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

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

**NOTE:** If you disable the configuration parameter at a later date, model components and scripts that are 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 SharePoint roles belong to the same site collection.

### To exclude SharePoint roles

1. Select the **SharePoint > Roles** category.
2. Select the role in the result list.
3. Select the **Exclude SharePoint roles** task.
4. In the **Add assignments** pane, assign the roles that are mutually exclusive to the selected role.

- OR -

In the **Remove assignments** pane, remove the roles that no longer exclude each other.

5. Save the changes.

### Detailed information about this topic

- [Effectiveness of group memberships](#) on page 121

## Assigning extended properties to SharePoint roles


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

### **To specify extended properties for a SharePoint role**

1. In the Manager, select the **SharePoint > Roles** category.
2. Select the role in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

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


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

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

## **Deleting SharePoint roles and permission levels**


You cannot delete SharePoint roles in the Manager. They are deleted by the DBQueue Processor when the associated permission level is deleted.

### **To delete a permission level**

1. Select the **SharePoint > Permission levels** category.
2. Select the permission level in the result list.
3. Click  to delete the permission level.
4. Confirm the security prompt with **Yes**.

If deferred deletion is configured, the permission level is marked for deletion and finally deleted after the deferred deletion period has expired. During this period, the permission level can be restored. Permission levels with deferred deletion of 0 days are deleted immediately.

### **To restore a permission level**

1. Select the **SharePoint > Permission levels** category.
2. Select the permission level marked for deletion in the result list.
3. Click  in the result list.

### **Related topics**

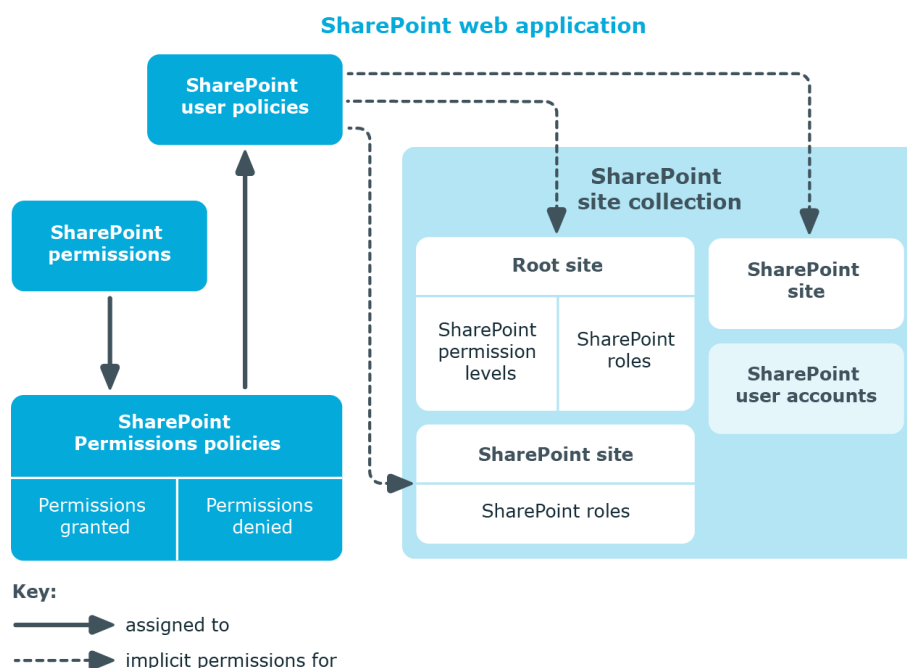
- One Identity Manager Configuration Guide

## Permissions for SharePoint web applications

You can define user policies in SharePoint that guarantee permissions across all sites in a site collection. These user policies overlay all the permissions that are specially defined for the sites. User policies are based on authentication objects from which SharePoint user accounts are created. These authentication objects can be saved as authentication objects in user policies.

User policies obtain their permissions through permission policies. SharePoint permissions are explicitly granted or denied in permission policies.

**Figure 5: Permissions for SharePoint web applications through policies**



You define user policies and permission policies for a web application. User policies are therefore implicitly authorized for all web application sites. You can limit them to single zones or be allow them for the entire web application.

# SharePoint permission policies

On the permission policy overview form, you can view the web application and the user policies to which the permission policy is assigned. All permissions are listed that have been explicitly granted or denied.

## *To obtain an overview of a permission policy*

1. Select the **SharePoint > Permission policies** category.
2. Select the permission policy from the result list.
3. Select the **SharePoint permission policy overview** task.

The denied SharePoint permission "Deny write" is displayed. SharePoint groups internally several single permissions together that are only found as single permissions in the SharePoint interface. One Identity Manager maps the SharePoint internal permission. That is why only the permission "Deny write" appears in the One Identity Manager interface. Single permissions are therefore not known to One Identity Manager.

# SharePoint user policies

User policies have a dynamic foreign key (column **AuthenticationObject**) that references the appropriate authentication object. An additional employee can be assigned if the dynamic foreign key references an Active Directory or an LDAP user account.

Each user policy represents an object from an authentication system. This object can be a group or a user.

## *To edit user policy main data*

1. Select the **SharePoint > User accounts** category.
2. Select the SharePoint role in the result list. Select the **Change main data** task.
3. Enter the required data on the main data form.
4. Save the changes.

The following properties are displayed for user policies.

**Table 36: Main data for a user policy**

| Property     | Description  |
|--------------|--|
| Display name | Display name for the user policy.  |
| User account | Specifies whether the user policy's authentication object is a user account. |

| Property              | Description  |
|-----------------------|--|
| Login name            | Login name for the user policy. It is found using a template.  |
| System account        | Specified whether the user policies in the SharePoint environment operates as a system account.  |
| Employee              | <p>Employee using the user policy. If an authentication object is assigned, the connected employee is found through the authentication object by using a template. If there is no authentication object assigned, the employee can be assigned manually.</p> <p>An employee can only be assigned if the <b>User account</b> option is set.</p>   |
| Web application       | Unique identifier for the web application for which the user policy is setup.  |
| Zone                  | Unique identifier of the SharePoint zone for which the user policy is valid.   |
| Authentication object | <p>Authentication object referencing the user policy. Each user policy represents an object from an authentication system trusted by the SharePoint installation. If this authentication system is managed as a target system in One Identity Manager, the object used for authentication can be saved as the authentication object in the user policy.</p> <p>The authentication object is assigned during automatic synchronization. If the <b>User account</b> option is set, the following authentication objects can be assigned:</p> <ul style="list-style-type: none"> <li>• Active Directory user accounts</li> <li>• LDAP user accounts</li> </ul> <p>If the <b>User account</b> option is disabled, the following authentication objects can be assigned:</p> <ul style="list-style-type: none"> <li>• Active Directory groups</li> <li>• LDAP groups</li> </ul> |

**NOTE:** When an authentication object assigned to a SharePoint user policy is deleted from the One Identity Manager database, the link to the authentication object is removed from the user policy. Employees assigned to it remain assigned if necessary.

## Global user policies

Global user policies are user policies that are valid for all zones. They are mapped in the **SharePoint > Hierarchical view > <farm> > Web applications > <web application> > Global user policies** category.

## Zone-specific user policies

Zone specific user policies are user policies that are valid for a single zone in a web application. They are displayed in the **SharePoint > Hierarchical view > <farm> >**

**Web applications > <web application> > Zone specific user policies > <zone> category.**



## Reports about SharePoint 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 SharePoint farms.

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

**Table 37: 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.<br><br>Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report. |
| Overview of all assignments     | group<br>Role | This report finds all roles containing employees who have the selected system entitlement.   |
| Show overview                   | group<br>Role | This report shows an overview of the system entitlement and its assignments.   |
| Show overview including origin  | group<br>Role | This report shows an overview of the system entitlement and origin of the assigned user accounts.  |
| Show overview including history | group<br>Role | This report shows an overview of the system entitlement and including its history.<br><br>Select the end date for displaying the history   |

| Report   | Published for                       | Description   |
|--|-------------------------------------|---|
|  |                                     | ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.  |
| Show entitlement drifts  | Site collection                     | 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)                            | Site<br>Site collection             | This report returns all the user accounts with their permissions including a history.<br>Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.          |
| Show user accounts with an above average number of system entitlements | Site collection                     | This report contains all user accounts with an above average number of system entitlements.   |
| Show employees with multiple user accounts                             | Site collection                     | This report shows all the employees that have multiple user accounts. The report contains a risk assessment.  |
| Show system entitlements overview (incl. history)                      | Site<br>Site collection             | This report shows the system entitlements with the assigned user accounts including a history.<br>Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report. |
| Overview of all assignments  | Web applications<br>Site collection | This report finds all roles containing employees with at least one user account in the selected target system.  |
| Show unused user accounts  | Site collection                     | This report contains all user accounts, which have not been used in the last few months.  |
| Show orphaned user accounts  | Site collection                     | This report shows all user accounts to which no employee is assigned.   |

## Related topics

- [Overview of all assignments](#) on page 147


# Overview of all assignments


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



## Examples:

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

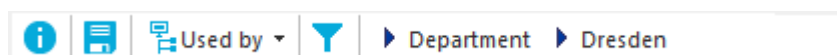
## To display detailed information about assignments

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





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

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

**Figure 6: Toolbar of the Overview of all assignments report.**



**Table 38: Meaning of icons in the report toolbar**

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

## Configuration parameters for managing a SharePoint environment

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

**Table 39: Configuration parameter**

| Configuration parameters   | Description  |
|--|--|
| TargetSystem   SharePoint  | SharePoint is supported. The parameter is a precompiler dependent configuration parameter. The database needs to be recompiled after the configuration parameter has been changed.<br><br>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 <i>One Identity Manager Configuration Guide</i> . |
| TargetSystem   SharePoint   Accounts                             | Parameter for configuring SharePoint user accounts. If this parameter is set, settings for SharePoint user accounts can be configured.   |
| TargetSystem   SharePoint   Accounts   MailTemplateDefaultValues | This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account.   |
| TargetSystem   SharePoint   DBDeleteOnError                      | If a error occurs adding a user account in a target system, the object is deleted from the database afterward.   |
| TargetSystem   SharePoint   DefaultAddress                       | This configuration parameter contains the default email address for messages when actions in the target system fail.   |

| Configuration parameters                            | Description  |
|---|--|
| TargetSystem   SharePoint   MaxFullsyncDuration     | Specifies the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time.   |
| TargetSystem   SharePoint   PersonAutoDefault       | Automatic employee assignment for user accounts added to the database outside synchronization based on the given mode.   |
| TargetSystem   SharePoint   PersonAutoFullsync      | Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.  |
| QER   ITShop   AutoPublish   SPSGroup               | <p>Preprocessor relevant configuration parameter for automatically adding SharePoint groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are 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 <i>One Identity Manager Configuration Guide</i>.</p> |
| QER   ITShop   AutoPublish   SPSGroup   ExcludeList | <p>List of all SharePoint groups that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.</p> <p>Example:</p> <pre>.*Administrator.* Exchange.* .*Admins . *Operators II S_IUSRS</pre>   |

# Default project template for SharePoint

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 40: Mapping SharePoint schema types to tables in the One Identity Manager schema**

| Schema type in SharePoint | Table in the One Identity Manager Schema |
|---------------------------|--|
| SPAlternateUrl            | SPSAlternateURL                          |
| SPClaimProvider           | SPSClaimProvider                         |
| SPFarm                    | SPSFarm                                  |
| SPGroup                   | SPSGroup                                 |
| SPLanguage                | SPSLanguage                              |
| SPPolicy                  | SPSPolicyUser                            |
| SPPolicyRole              | SPSPolicyRole                            |
| SPPrefix                  | SPSPrefix                                |
| SPQuotaTemplate           | SPSQuota                                 |
| SPRoleDefinition          | SPSRole                                  |
| RoleAssignment            | SPSRIAsgn                                |
| SPSite                    | SPSSite                                  |

| Schema type in SharePoint | Table in the One Identity Manager Schema |
|---------------------------|--|
| SPUser                    | SPSUser                                  |
| SPWeb                     | SPSWeb                                   |
| SPWebApplication          | SPSWebApplication                        |
| SPWebTemplate             | SPSWebTemplate                           |



# 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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## A

- account definition 55
  - add to IT Shop 68
  - assign to system roles 68
- Active Directory domain
  - SharePoint authentication object 86
  - SharePoint synchronization 74
- Active Directory group
  - SharePoint authentication object 86
- Active Directory user account
  - SharePoint authentication object 86
- alternative URL 47
- application role
  - target system managers 53
- architecture 9
- authentication
  - authentication mode 45
  - claims based 12
- authentication mode 45
- authentication object 86

## B

- base object 29, 36
  - create 28

## C

- calculation schedule
  - deactivate 39
- category 80
- configuration parameter 149
- connection parameter 18, 26, 28

- connector 9
- convert connection parameter 29

## D

- direction of synchronization
  - direction target system 27

## E

- employee
  - number user accounts (report) 145
- employee assignment
  - automatic 102
  - manual 105
  - remove 105
  - search criteria 104
- exclusion definition 121, 139
- extended property
  - assign group 125
  - assign SharePoint role 139
  - user account 101
- extended schema 28

## F

- farm
  - domain 74
  - set up 74
  - target system managers 74

## G

### group

- about IT Shop requests 110
- add to IT Shop 117
- add to IT Shop (automatic) 119
- add to system role 116
- assign category 110
- assign extended properties 125
- assign SharePoint role 116
- assign to business role 114
- assign to cost center 113
- assign to department 113
- assign to location 113
- assign user account 112, 115
- category 123
- delete 125
- drifted (report) 145
- effective 121
- exclusion 121
- group membership 115
- inheriting through categories 80
- inheriting through system roles 116
- overview form 121
- owner 110
- request 126-127
- risk index 110
- role assignment 84
- set up 109

group prefix 45

## I

### IT operating data

- change 64

### IT Shop shelf

- assign account definition 68
- assign group 117
- assign SharePoint roles 137

## J

### Job server

- load balancing 37
- properties 50

## L

### language 47-48

### LDAP domain

- SharePoint authentication object 86
- SharePoint synchronization 74

### LDAP group

- SharePoint authentication object 86

### LDAP user account

- SharePoint authentication object 86

### load balancing 37

### login 10

## M

### manage level 59

### membership

- modify provisioning 35

## O

### object

- delete immediately 32
- outstanding 32
- publish 32

### offline mode 41

orphaned user accounts (report) 145  
outstanding object 32

## P

permission 47  
    assign permissions level 47  
    permitted permissions 47, 77  
    synchronizing 25  
permissions level 47, 127-128  
    assign permissions 129  
    assign to group 128  
    assign to user account 128  
    delete 140  
    overview form 129  
    permitted permissions  
        synchronizing 130  
    role definition 108, 129  
    site 128  
permissions policy 47, 142  
    denied permissions 142  
    granted permissions 142  
    synchronization object type 142  
prefix 12, 45-46  
    create site 82  
product owners 119  
    request group 126  
project template 151  
provider 12, 77  
provisioning  
    accelerate 37  
    members list 35

## Q

quota 48

## R

relative URL 46  
report  
    overview of all assignments 147  
    site collection 145  
request  
    authorizations 126  
    group membership 127  
    groups 126  
revision filter 32  
role  
    about IT Shop requests 130  
    add to IT Shop 137  
    add to system role 136  
    assign group 135  
    assign to business role 134  
    assign to cost center 132  
    assign to department 132  
    assign to location 132  
    assign user account 132, 135  
    delete 140  
    effective 139  
    exclusion 139  
    hierarchical role inheritance 132  
    inheriting through system roles 136  
    map in One Identity Manager 127  
    overview form 138  
    permissions inheritance 108  
    permissions level 108, 130  
    risk index 130  
    role assignment 108, 135  
    role definition 84, 108  
    site 130

- root site 81
  - site 80
  - site collection 79

## S

- schema
  - changes 31
  - shrink 31
  - update 31
- scope 26
- server farm account 14
- server function 52
- SharePoint role
  - assign extended properties 139
- single object synchronization 36, 40
  - accelerate 37
- site 80
  - anonymous access 81
  - author 81
  - create 84
  - prefix 82
  - request through IT Shop 84
  - role assignment 81, 84
  - role definition 81, 84
  - root site 80-81
    - permissions inheritance 84, 108
  - site template 83
  - subordinate 108
  - URL 82-83
    - open 82
- site collection 78
  - account definition 79
  - administrator 79
  - category 123
  - create 84

- employee assignment 104
- quota 48
- request through IT Shop 84
- root site 79
  - permissions inheritance 84, 108
- server 79
- specify category 80
- URL 79
- site template 47
  - create site 83
- start up configuration 29
- synchronization
  - accelerate 32
  - configure 18
  - configure synchronization 15
  - connection data 18
  - different farms 28
  - Microsoft.SharePoint.dll 15
  - permissions 14
  - prerequisites 13
  - prevent 39
  - provider 12
  - start 18
- synchronization analysis report 38
- synchronization configuration
  - customize 26-28
  - remote connection 27-28
- synchronization log 25
- synchronization project
  - deactivate 39
  - edit 75
  - project template 151
  - set up 18
- synchronization server
  - edit 49

- server function 52
- synchronization workflow
  - create 27
- synchronize single object 40
- system connection
  - change 29
  - enabled variable set 30

## T

- target system
  - not available 41
- target system manager 53
  - assign 74
- target system schema 28
- target system synchronization 32
- template
  - IT operating data, modify 64

## U

- unused user accounts (report) 145
- URL
  - prefix 46
  - site 82-83
  - site collection 79
- user 10
  - synchronization 14
- user account 86
  - administrative user account 88
  - administrator 93, 95
  - apply template 64
  - assign category 93, 95
  - assign employee 95, 102
  - assign extended properties 101
  - assign group 100, 115

- assign role 101
- assign SharePoint role 135
- auditor 93, 95
- authentication mode 102
- authentication object 86, 93, 95, 102
- authentication system 93, 95
- category 123
- create automatically 55
- custom template 102
- default user accounts 88
- deferred deletion 106
- delete 106
- identity 88, 93, 95
- lock 106
- login name 93, 95, 102
- more than 1 per employee 86
- number of group memberships (report) 145
- overview 100
- permissions for synchronization 14
- privileged user account 88, 93, 95
- retrieve 106
- risk index 93, 95
- role assignment 84
- set up 92
- type 88
- user definition 142
  - Active Directory user account 142
  - assign employee 142
  - authentication object 142
  - global 143
  - system account 142
  - Web application 142
  - zone 142
  - zone specific 143



user prefix 45

## **V**

variable 26

variable set 28-29

active 30

## **W**

Web application 77

alternative URL 47

claims authentication 77

cross permissions 141

permissions policy 77, 141

permitted conditions 77

user definition 77, 141

valid permissions 47, 77

workflow 27

## **Z**

zone 47

user definition 142