



One Identity Manager 8.1.5

Administration Guide for Connecting to SharePoint

Copyright 2021 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

One Identity Manager Administration Guide for Connecting to SharePoint
Updated - 09 July 2021, 13:06
Version - 8.1.5

Contents

Managing SharePoint environments	7
Architecture overview	8
One Identity Manager users for managing SharePoint	9
Claims-based authentication	11
Setting up SharePoint farm synchronization	12
Users and permissions for synchronizing with a SharePoint farm	13
Setting up the synchronization server	14
Creating a synchronization project for initial synchronization of a SharePoint farm	17
Special synchronization cases for valid permissions	24
Displaying synchronization results	24
Customizing the synchronization configuration	25
How to configure SharePoint synchronization	26
Configuring synchronization of several SharePoint farms	27
Updating schemas	28
Speeding up synchronization with revision filtering	29
Post-processing outstanding objects	29
Configuring the provisioning of memberships	31
Accelerating provisioning and single object synchronization	33
Help for the analysis of synchronization issues	34
Disabling synchronization	34
Basic data for managing a SharePoint environment	36
Authentication modes	37
Prefixes	38
Zones and alternative URLs	39
SharePoint site templates	39
SharePoint permissions	39
SharePoint quotas	40
SharePoint languages	40
Editing a server	41
Master data for a Job server	42
Specifying server functions	44

Target system managers	45
Setting up account definitions	48
Creating an account definition	48
Master data for an account definition	49
Creating manage levels	51
Master data for manage levels	52
Creating a formatting rule for IT operating data	53
Collecting IT operating data	55
Modify IT operating data	57
Assigning account definitions to employees	58
Assigning account definitions to departments, cost centers, and locations	59
Assigning an account definition to business roles	59
Assigning account definitions to all employees	60
Assigning account definitions directly to employees	60
Assigning account definitions to system roles	61
Adding account definitions to the IT Shop	61
Assigning account definitions to a target system	63
Deleting an account definition	63
SharePoint farms	66
General master data for a SharePoint farm	66
How to edit a synchronization project	67
SharePoint web applications	69
SharePoint site collections and sites	70
SharePoint site collections	70
General master data for a site collection	71
Specifying categories for inheriting SharePoint groups	72
SharePoint sites	72
General master data for a site	73
Address data for a site	74
Site design properties	74
Additional tasks for managing sites	75
Passing on permissions to child sites	75
Setting up SharePoint site collections and sites	76
SharePoint user accounts	78

Supported user account types	80
Entering master data for SharePoint user accounts	84
Group authenticated user account master data	85
User authenticated user account master data	87
Additional tasks for managing SharePoint user accounts	91
Displaying the SharePoint user account overview	91
Assigning SharePoint groups directly to a SharePoint user account	91
Assigning SharePoint roles directly to user accounts	92
Assigning extended properties	92
Using custom authentication modes	93
Automatic assignment of employees to SharePoint user accounts	94
Editing search criteria for automatic employee assignment	95
Deleting and restoring SharePoint user accounts	97
SharePoint roles and groups	99
SharePoint groups	100
Entering master data for SharePoint groups	101
Assigning SharePoint groups to SharePoint user accounts	103
Assigning SharePoint groups to departments, cost centers and locations	104
Assigning SharePoint groups to business roles	105
Assigning SharePoint user accounts directly to a SharePoint group	106
Assigning SharePoint roles to SharePoint groups	107
Adding SharePoint groups to system roles	108
Adding SharePoint groups to the IT Shop	108
Adding SharePoint groups automatically to the IT Shop	110
Additional tasks for managing SharePoint groups	112
Displaying an overview of SharePoint groups	112
Effectiveness of group memberships	112
SharePoint group inheritance based on categories	114
Assigning extended properties to SharePoint groups	117
Deleting SharePoint groups	117
Default solutions for requesting SharePoint groups	118
Adding SharePoint groups	118
SharePointRequesting Groups Memberships	119
SharePoint roles and permission levels	119
Entering master data for SharePoint permission levels	120

Additional tasks for managing SharePoint permission levels	121
Displaying the SharePoint permission level overview	121
Assigning permissions	121
Special synchronization cases for valid permissions	122
Entering master data for SharePoint roles	122
Assigning SharePoint roles to SharePoint user accounts	124
Assigning SharePoint roles to departments, cost centers and locations	124
Assigning SharePoint roles to business roles	126
Assigning SharePoint user accounts directly to a SharePoint role	127
Assigning SharePoint groups to SharePoint roles	127
Adding SharePoint roles to system roles	128
Adding SharePoint roles to the IT Shop	129
Additional tasks for managing SharePoint roles	130
Displaying the SharePoint rules overview	131
Effectiveness of SharePoint roles	131
Deleting SharePoint roles and permission levels	132
Permissions for SharePoint web applications	133
SharePoint permission policies	134
SharePoint user policies	134
Reports about SharePoint site collections	137
Overview of all assignments	138
Appendix: Configuration parameters for managing a SharePoint environment	140
Appendix: Default project template for SharePoint	142
About us	144
Contacting us	144
Technical support resources	144
Index	145

Managing SharePoint environments

In One Identity Manager, components and access rights from SharePoint 2010, SharePoint 2013, SharePoint 2016 and SharePoint 2019 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

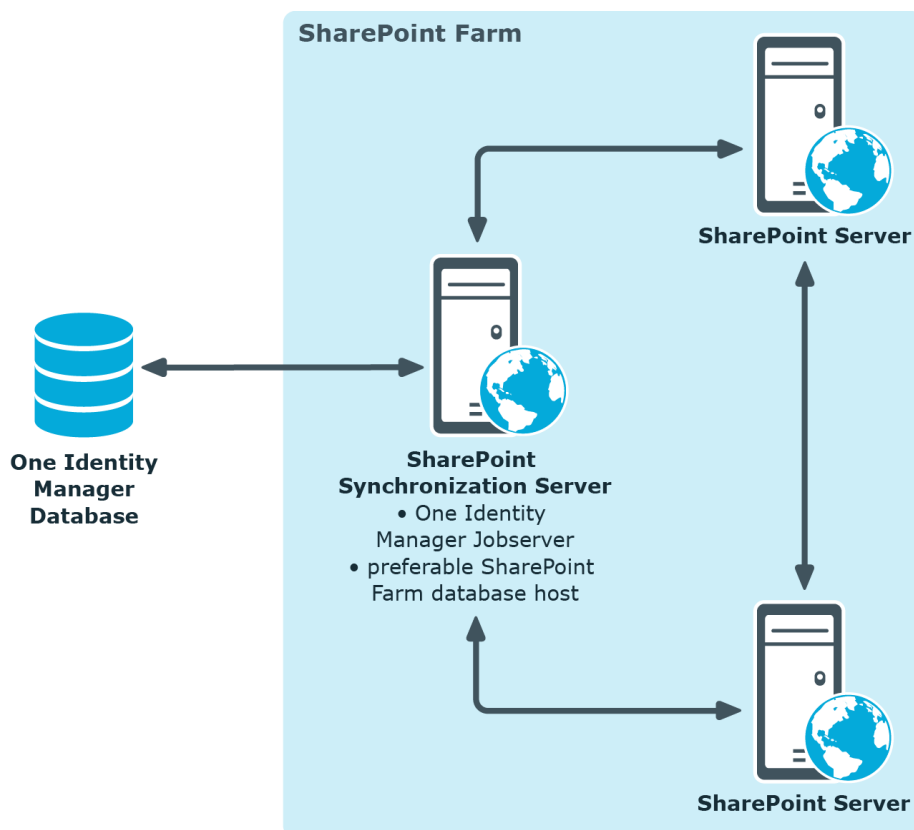
and groups to the organizational units. It is also possible to request permissions through the IT Shop. Permissions assigned to an employee can be monitored over compliance rules.

The SharePoint Module module is based on the SharePoint Foundation 2010, 2013, 2016 and 2019 class libraries respectively.

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

Detailed information about this topic

- [Setting up the synchronization server](#) on page 14

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

User	Tasks
Target system administrators	<p>Target system administrators must be assigned to the Target systems Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Administer application roles for individual target system types.• Specify the target system manager.• Set up other application roles for target system managers if required.• Specify which application roles for target system managers are mutually exclusive.• Authorize other employees to be target system administrators.• Do not assume any administrative tasks within the target system.
Target system managers	<p>Target system managers must be assigned to the Target systems SharePoint application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects like user accounts or groups.• Edit password policies for the target system.• Prepare system entitlements to add to the IT Shop.• Can add employees who have an other identity than the Primary identity.

User	Tasks
	<ul style="list-style-type: none"> • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	<ul style="list-style-type: none"> • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	<p>Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign system entitlements to IT Shop structures.
Product owner for the IT Shop	<p>Product owners must be assigned to the Request & Fulfillment IT Shop Product owners application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Approve through requests. • Edit service items and service categories under their management.
Administrators for organizations	<p>Administrators must be assigned to the Identity Management Organizations Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign system entitlements to departments, cost centers, and locations.
Business roles admin-	<p>Administrators must be assigned to the Identity Management</p>

User	Tasks
istrators	 Business roles Administrators application role. Users with this application role: <ul style="list-style-type: none"> 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 37

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. One Identity Manager parts for managing SharePoint systems are available if the "TargetSystem | SharePoint" configuration parameter is set.

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

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

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

For more detailed information about synchronizing with Active Directory, see the One Identity Manager Administration Guide for Connecting to Active Directory. For more detailed 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 detailed 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 13
- [Setting up the synchronization server](#) on page 14
- [Creating a synchronization project for initial synchronization of a SharePoint farm](#) on page 17
- [Configuration parameters for managing a SharePoint environment](#) on page 140

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 not 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 One Identity Manager Service requires additional permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files.</p> <p>The user account must belong to the Domain users group.</p> <p>The user account must have the Login as a service extended user permissions.</p> <p>The user account requires access permissions to the internal web service.</p> <p>NOTE: If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/user="NT AUTHORITY\NETWORKSERVICE"</pre>

User	Permissions
	<p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (on 32-bit operating systems) • %ProgramFiles%\One Identity (on 64-bit operating systems)
User for accessing the One Identity Manager database	The Synchronization default system user is provided to execute synchronization with 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 be installed on the synchronization server.

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 detailed 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 25.

To synchronize a SharePoint 2010 environment

- Windows Server 2008 R2 (prerequisite for SharePoint Server 2010)
 - Microsoft SharePoint Server 2010
 - Microsoft .NET Framework Version 4.7.2 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.

To synchronize SharePoint 2013, 2016, or 2019 environments

- Windows Server 2008 R2 or Windows Server 2012
 - Microsoft SharePoint Server 2013, 2016 or 2019 respectively
 - Microsoft .NET Framework Version 4.7.2 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 executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

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

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

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

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

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

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

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

- OR -

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

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

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

Syntax:

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

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

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

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

detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files.
10. On the **Select private key file** page, select the file with the private key.
| NOTE: This page is only displayed when the database is encrypted.
11. On the **Service access** page, enter the service's installation data.
 - **Computer:** Name or IP address of the server that the service is installed and started on.
 - **Service account:** User account data for the One Identity Manager Service.
 - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.

The One Identity Manager Service farm's server farm account must be used as user account for SharePoint.
 - **Installation account:** Data for the administrative user account to install the service.
 - To use the current user's account, set the **Current user** option.
 - To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.
 - To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.
12. Click **Next** to start installing the service.
Installation of the service occurs automatically and may take some time.
13. Click **Finish** on the last page of the Server Installer.
| NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Creating a synchronization project for initial synchronization of a 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 2010, 2013, 2016 and 2019.
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 Users and permissions for synchronizing with a SharePoint farm on page 13.
Domain	Server farm account domain.
synchronization server	<p>All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>Installed components:</p> <ul style="list-style-type: none"> • SharePoint server • One Identity Manager Service (started) • Synchronization Editor • SharePoint connector <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 Setting up the synchronization server on page 14.</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>To use a remote connection</p>

Data	Explanation
	<ol style="list-style-type: none"> 1. Provide a workstation on which the Synchronization Editor is installed. 2. Install the RemoteConnectPlugin on the synchronization server. Thus the synchronization server simultaneously assumes the function of the remote connection server. <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • SharePoint connector is installed • Target system specific components are installed <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>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"> • Database server • Database • SQL Server login and password • Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

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:

- Executed in default mode
- Started from the Launchpad

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

To set up an initial synchronization project for a SharePoint farm

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

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

2. Select the **Target system type 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.
Domain	Server farm account domain.
User account and password	User name and password for the server farm account. 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
Read-only access to target system.	<p>Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none">• Synchronization is in the direction of One Identity Manager.• Processing methods in the synchronization steps are only defined for synchronization in the direction of One Identity Manager.
Read/write access to target system. Provisioning available.	<p>Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none">• Synchronization is in the direction of the Target system.• Processing methods are only defined in the synchronization steps for synchronization in the direction of the Target system.• Synchronization steps are only created for such schema classes whose schema types have write access.

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

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

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

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

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

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

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

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

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

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

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

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

To configure the content of the synchronization log

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

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

7. Click **OK**.

To synchronize on a regular basis

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Start up configurations** category.
3. Select a start up configuration in the document view and click **Edit schedule**.
4. Edit the schedule properties.

5. To enable the schedule, click **Activate**.
6. Click **OK**.

To start initial synchronization manually

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

NOTE:

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

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

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the 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 14
- [Users and permissions for synchronizing with a SharePoint farm](#) on page 13

- [Default project template for SharePoint](#) on page 142
- [Setting up account definitions](#) on page 48
- [Automatic assignment of employees to SharePoint user accounts](#) on page 94

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 SPSRoleHasSPSPermission 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 119


Displaying synchronization results

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

To display a synchronization log

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

To display a provisioning log

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.
3. Click  in the navigation view toolbar.

Logs for all completed provisioning processes are displayed in the navigation view.

4. Select a log by double-clicking it.

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

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

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

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 master system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing methods, for example.
- Use variables to set up a synchronization project for synchronizing different 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 26
- [Configuring synchronization of several SharePoint farms](#) on page 27
- [Updating schemas](#) on page 28
- 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 master system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing SharePoint farms

1. Open the synchronization project in the Synchronization Editor.

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

Detailed information about this topic

- [Configuring synchronization of several SharePoint farms](#) on page 27

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 and declare the connection parameters. The connection parameters are saved in a special variable set.
A start up configuration is created that uses the newly created variable set.
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 14
- [Users and permissions for synchronizing with a SharePoint farm](#) on page 13
- [How to configure SharePoint synchronization](#) on page 26

Updating schemas

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

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

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

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

To update a system connection schema

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

To edit a mapping

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

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

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

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.
All the synchronization tables assigned to the **SharePoint** target system type are displayed in the navigation view.
2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.
All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the

synchronization log and which processing method was executed. The **No log available** entry can mean the following:




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

TIP:

To display object properties of an outstanding object

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

Table 6: Methods for handling outstanding objects

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

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

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

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

To disable bulk processing

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

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

To add custom tables to target system synchronization

1. In the Manager, select the **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 in the target system as an object property in list form (Example: List of user accounts in the Users property of an 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.
 - This option can only be enabled for assignment tables that have a base table with an `XDateSubItem` column.
 - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically (for example, `SPSGroupHasSPSRLAsgn` and `SPSUserHasSPSRLAsgn`).
5. Click **Merge mode**.
6. Save the changes.

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

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

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

To restore the default condition

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

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

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

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

Detailed information about this topic

- [Editing a server](#) on page 41

Help for the analysis of synchronization issues

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

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

To generate a synchronization analysis report

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Help | Generate synchronization analysis report** menu item and click **Yes** in the security prompt.

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

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

Disabling synchronization

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

To prevent regular synchronization

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

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Detailed information about this topic

- [Creating a synchronization project for initial synchronization of a SharePoint farm](#) on page 17

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 140.

- Account definitions

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

For more information, see [Setting up account definitions](#) on page 48.

- 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 37.

- Prefixes

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

For more information, see [Prefixes](#) on page 38.

- 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 39.

- Site templates

Use site templates to add sites.

For more information, see [SharePoint site templates](#) on page 39.

- 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 39.

- Target system types

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

For more information, see [Post-processing outstanding objects](#) on page 29.

- Server

In order to handle SharePoint -specific processes in One Identity Manager, the synchronization server and its server functions must be declared.

For more information, see [Editing a server](#) on page 41.

- Target system managers

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

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


For more information, see [Target system managers](#) on page 45.

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 master 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 Group 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 Group 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_SPSSAuthSystem 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 permission 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 119

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 SharePoint -specific processes in One Identity Manager, the synchronization server and its server functions 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 detailed information, see *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 master 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 master data** task.
4. Edit the Job server's master data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- [Master data for a Job server](#) on page 42
- [Specifying server functions](#) on page 44

Related topics

- [Setting up the synchronization server](#) on page 14

Master data for a Job server

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

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

Table 8: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: <Name of server>.<Fully qualified domain name>
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The Server is cluster and Server belongs to cluster properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process

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

Related topics

- [Specifying server functions](#) on page 44

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.
Native 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.

Server function	Remark
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for running synchronization with an SMB-based target system.
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

- [Master data for a Job server](#) on page 42

Target system managers

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

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

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

Implementing application roles for target system managers

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

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

To initially specify employees to be target system administrators

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

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

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration | Target systems | 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 master data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

- OR -

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

- a. Enter the application role name and assign the **Target systems | 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 9
- [General master data for a SharePoint farm](#) on page 66

Setting up account definitions

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

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

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


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 78.

The following steps are required to implement an account definition:

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

Creating an account definition

To create a new account definition

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

Master data for an account definition

Enter the following data for an account definition:

Table 11: Master 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>Required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it.</p> <p>TIP: 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.</p> <p>Customize <code>TSB_PersonHasAccountDef_AutoCreate_SPSUser</code> 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 account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.</p> <p>For more detailed 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 in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition 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

Property	Description
	IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	<p>Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.</p> <p>IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.</p> <p>Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</p>
Retain account definition if permanently disabled	<p>Specifies the account definition assignment to permanently disabled employees.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition if temporarily disabled	<p>Specifies the account definition assignment to temporarily disabled employees.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on deferred deletion	<p>Specifies the account definition assignment on deferred deletion of employees.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>
Retain account definition on security risk	<p>Specifies the account definition assignment to employees posing a security risk.</p> <p>Option set: the account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: the account definition assignment is not in effect. The associated user account is deleted.</p>

Property	Description
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

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

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

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

- Employee user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the employee is reinstated at a later date, the user accounts are also reactivated.
- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee's user accounts are disabled and

therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted.

To assign manage levels to an account definition


1. In the Manager, select the **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 levels.
- OR -

In the **Remove assignments** pane, remove the manage levels.

5. Save the changes.

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

To edit a manage level

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

Master data for manage levels

Enter the following data for a manage level.

Table 12: Master data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <ul style="list-style-type: none">• Never: Data is not updated.• Always: Data is always updated.• Only initially: Data is only determined at the start.

Property	Description
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled *)	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled *)	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred*)	Specifies whether user accounts of employees marked for deletion are locked.
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 (with delay) 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
- 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 and enter the following data.

Table 13: Mapping rule for IT operating data

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

4. 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

Normally, each employee in department A obtains a default user account in the A. In addition, certain employees in department A obtain administrative user accounts in the A.

Create an account definition A for the default user account of the A and an account definition B for the administrative user account of A. Specify the "Department" property in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.

3. Click **Add** and enter the following data.

Table 14: IT operating data

Property	Description
Effects on	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 <ol style="list-style-type: none">a. Click ➔ next to the field.b. Under Table, select the table that maps the target system for select the TSBAccountDef table or an account definition.c. Select the specific target system or account definition under Effects on.d. Click OK.
Column	User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the <i>One Identity Manager Target System Base Module Administration Guide</i> .
Value	Concrete value which is assigned to the user account 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, business role or to a primary location changes, the templates are automatically executed.

To execute 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 **Execute templates** task.

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

Old value: Current value of the object property.

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

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

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

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

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


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 an account definition to business roles

Installed modules: Business Roles Module


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, 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

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

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

5. Save the changes.

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

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


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

Installed modules: System Roles Module


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

To add account definitions to a system role

1. In the Manager, select the **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 assigned system roles.

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

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

To remove an account definition from individual IT Shop shelves

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

To remove an account definition from all IT Shop shelves

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

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

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

Related topics

- [Master data for an account definition on page 49](#)
- [Assigning account definitions to departments, cost centers, and locations on page 59](#)
- [Assigning an account definition to business roles on page 59](#)
- [Assigning account definitions directly to employees on page 60](#)
- [Assigning account definitions to system roles on page 61](#)

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 master 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 master data** task.
 - d. On the **General** tab, disable the **Automatic assignment to employees** option.
 - e. Save the changes.
- 2. Remove direct assignments of the account definition to employees.
 - a. In the Manager, select the **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 the employees.
 - e. Save the changes.
- 3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **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.
 - In the **Remove assignments** pane, remove the business roles.
 - d. Save the changes.
- 5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.


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

To remove an account definition from all IT Shop shelves

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

- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

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

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. In the Manager, select the **SharePoint | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change master data** task.
 - d. From the **Required account definition** menu, remove the account definition.
 - e. Save the changes.
7. Remove the account definition's assignments to target systems.
 - a. In the Manager, select the site collection in the **SharePoint | Site collections** category.
 - b. Select the **Change master data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
8. Delete the account definition.
 - a. In the Manager, select the **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 master data of a farm


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

General master data for a SharePoint farm

Enter the following master data for a farm.

Table 15: General master data for 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	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.

Property	Description									
	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.									
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>When you create a farm with the Synchronization Editor, One Identity Manager is used.</p> <p>Table 16: Permitted values</p> <table><tr><th>Value</th><th>Synchronization by</th><th>Provisioned by</th></tr><tr><td>One Identity Manager</td><td>SharePoint connector</td><td>SharePoint connector</td></tr><tr><td>No synchronization</td><td>none</td><td>none</td></tr></table> <p>NOTE: If you select No synchronization, you can define custom processes to exchange data between One Identity Manager and the target system.</p>	Value	Synchronization by	Provisioned by	One Identity Manager	SharePoint connector	SharePoint connector	No synchronization	none	none
Value	Synchronization by	Provisioned by								
One Identity Manager	SharePoint connector	SharePoint connector								
No synchronization	none	none								
Build version	The build version for SharePoint services for this farm are read in during synchronization.									

Related topics

- [Target system managers](#) on page 45

How to edit a synchronization project

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 master 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 25

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 119

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 99
- [SharePoint user accounts](#) on page 78

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 master data** task.
3. Enter the required data on the master data form.
4. Save the changes.

Detailed information about this topic

- [General master data for a site collection](#) on page 71
- [Specifying categories for inheriting SharePoint groups](#) on page 72

General master data for a site collection

The following properties are displayed for site collections.

Table 17: General master data for a site collection

Property	Description
Account definition	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 (Linked configured). The account definition's default manage level is applied. 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.
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 root site .
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 48

Specifying categories for inheriting SharePoint groups

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

To define a category

1. In the Manager, select the site collection in the **SharePoint | Site collections** category.
2. Select the **Change master data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- [SharePoint group inheritance based on categories](#) on page 114
- 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 master data** task.

Detailed information about this topic

- [General master data for a site](#) on page 73
- [Address data for a site](#) on page 74

- [Site design properties](#) on page 74

General master data for a site

The following master data is displayed for sites.

Table 18: General master data for 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 99
- [SharePoint roles and permission levels](#) on page 119

Address data for a site

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

Table 19: 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.
Master page URL	URL of the master page used for the site.
Alternative master URL	URL to an alternative master page referenced by the site.
Portal URL	URL for a portal site that 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 76

Site design properties

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

Table 20: Site design properties

Property	Description
Site	Unique identifier for the site template to be used when the site is created. A

Property	Description
template	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 76

Additional tasks for managing sites

After you have entered the master 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 74

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 99

Related topics

- [General master data for a site](#) on page 73

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 SPSTemplate 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_ 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_ CreateSPSTemplate	Creates a new site within a site collection in the One Identity Manager database.
Process SP0_ SPSTemplate_ (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_ SPSTemplate_ (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. Clara Harris owns an Active Directory user account, which is a member in this group. She can log in to the site collection with this and obtain all the SharePoint user account's permissions.

Jan Bloggs is also requires guest access to the site collection. He owns an Active Directory user account in the same domain. He request membership of the Web Portal group in Active Directory. Once the request is granted approval and assigned, he 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 "TargetSystem | SharePoint | PersonAutoFullsync" and "TargetSystem | SharePoint | PersonAutoDefault".

- 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 "TargetSystem | SharePoint | PersonAutoFullsync" and "TargetSystem | SharePoint | PersonAutoDefault".
- 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 21: 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	User account that is used for a specific purpose,	Sponsored

Identity	Description	Value of the IdentityType column
identity	such as training.	
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

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

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

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

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

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

- Privileged user account

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

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

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

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

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

5. Assign the account definition to employees.

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

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 dummy employee using the UID_Person column.
Use an employee with the same identity or create a new employee.
 3. Assign this dummy employee to hierarchical roles.
- The dummy 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 the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined through a person's primary roles.

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

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

5. Enter the effective IT operating data for the target system.
Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
6. Assign the account definition directly to employees who work with privileged user accounts.


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

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


Entering master data for 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 master 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 the **Change master data** task.
- 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 master data](#) on page 85
- [User authenticated user account master data](#) on page 87

Group authenticated user account master data

Table 22: Configuration parameters for risk assessment of user accounts

Configuration parameter	Effect when set
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>

Enter the following master data for a group authenticated user account.

Table 23: Group authenticated user account master data

Property	Description
Site collection	Site collection the user account is used in.
Group authenticated	Specifies whether the user account's authentication object is a group.
Authentication object	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.

Property	Description
	<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"> • Active Directory groups with the type "Security group" from the domain assigned to the farm or a trusted domain • LDAP groups from the domain assigned to the farm
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 Claims-based authentication option of the associated web application. If you have defined custom authentication modes, select your authentication mode in the menu.</p> <p>NOTE: 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>NOTE: 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 QER CalculateRiskIndex configuration parameter is set. For detailed 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>
Advice	<p>Text field for additional explanation.</p>
Identity	<p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> • Primary identity: Employee's default user account.

Property	Description
	<ul style="list-style-type: none"> • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account that is used for a specific purpose, such as training. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • Service identity: Service account.
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 37
- [Specifying categories for inheriting SharePoint groups](#) on page 72
- [Supported user account types](#) on page 80
- One Identity Manager Identity Management Base Module Administration Guide


User authenticated user account master data

Table 24: Configuration parameters for risk assessment of user accounts

Configuration parameter	Effect when set
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>

Enter the following master data for a user authenticated user account.

Table 25: User authenticated user account master data

Property	Description
Employee	<p>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If 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 automatically or manually.</p> <p>You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.</p>
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 master data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p>NOTE: The account definition cannot be changed once the user account has been saved.</p> <p>NOTE: 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	<p>Site collection the user account is used in.</p>
Group authenticated	<p>Specifies whether the user account's authentication object is a group. This option is disabled for user authenticated user accounts.</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 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.</p>

Property	Description
	<p>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"> • Active Directory user accounts from the domain that is assigned to the farm or a trusted domain • LDAP user accounts from the domain assigned to the farm <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>NOTE: 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 Claims-based authentication option of the associated web application. If you have defined custom authentication modes, select your authentication mode in the menu.</p> <p>NOTE: 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>NOTE: 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 QER CalculateRiskIndex configuration parameter is set. For detailed 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"> • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account that is used for a specific purpose, such as training. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • Service identity: Service account.
Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	<p>Specifies whether the user account can inherit SharePoint roles and groups through the employee. If this option is set, the user account inherits SharePoint roles and groups through hierarchical roles or IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
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

- [Setting up account definitions](#) on page 48
- [Authentication modes](#) on page 37
- [Specifying categories for inheriting SharePoint groups](#) on page 72
- [Automatic assignment of employees to SharePoint user accounts](#) on page 94
- [Supported user account types](#) on page 80
- One Identity Manager Identity Management Base Module Administration Guide

Additional tasks for managing SharePoint user accounts

After you have entered the master 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.

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 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 92
- [Assigning SharePoint groups to SharePoint user accounts](#) on page 103

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.

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 91
- [Entering master data for SharePoint permission levels](#) on page 120

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. In the **Add assignments** pane, assign extended properties.
- OR -
In the **Remove assignments** pane, remove extended properties.
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 master 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_SPSEAuthSystem` 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 37
- One Identity Manager Configuration Guide

Automatic assignment of employees to SharePoint user accounts

Table 26: Configuration parameters for automatic employee assignment

Configuration parameter	Meaning
TargetSystem SharePoint PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem SharePoint PersonAutoDefault	This configuration parameter specifies the 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 be assigned automatically. This mechanism can be triggered after a new user account is created either manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

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.

Detailed information about this topic

- For more information, see the One Identity Manager Target System Base Module Administration Guide.

Related topics

- [Creating an account definition](#) on page 48
- [Assigning account definitions to a target system](#) on page 63
- [Editing search criteria for automatic employee assignment](#) on page 95

Editing search criteria for automatic employee assignment

The criteria for employee assignments are defined for the site collection. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (AccountToPersonMatchingRule) in the 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: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

To specify criteria for employee assignment

1. Select the **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 27: Default 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 28: Manual assignment view

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

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

To apply search criteria to user accounts

- Click **Reload**.

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

To assign employees directly using a suggestion list

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

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

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

To remove assignments

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


The assigned employees are removed from the selected user accounts.

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

To delete a user account

1. Select the **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

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

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

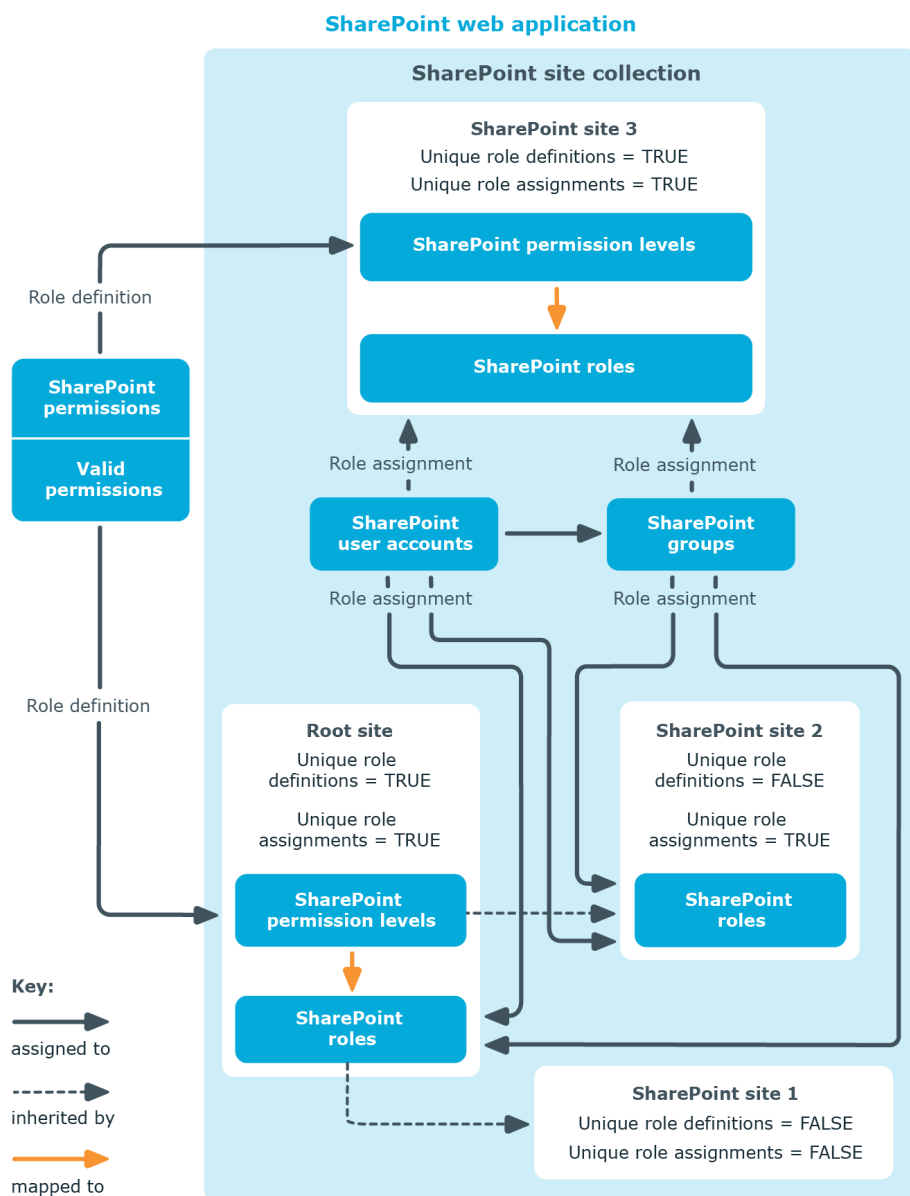
- A SharePoint Role is the permission level linked to a fixed site.
- The assignment of SharePoint permissions to a permission level is called a role definition.
- The assignment of user account or groups to a SharePoint role is called a role assignment.

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 master data

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

Detailed information about this topic

- [Entering master data for SharePoint groups](#) on page 101

Related topics

- [SharePoint roles and groups](#) on page 99

Entering master data for SharePoint groups

Table 29: Configuration parameters for setting up SharePoint groups

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

Enter the following master data for a group.

Table 30: SharePoint group master data

Property	Description
Display name	Display name of the group.
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. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex 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.

Property	Description
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.

Detailed information about this topic

- [Specifying categories for inheriting SharePoint groups](#) on page 72
- [SharePoint group inheritance based on categories](#) on page 114
- 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).
- **Group authenticated** 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 are 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 104
- [Assigning SharePoint groups to business roles](#) on page 105
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 106
- [Assigning SharePoint roles to SharePoint groups](#) on page 107
- [Adding SharePoint groups to system roles](#) on page 108
- [Adding SharePoint groups to the IT Shop](#) on page 108
- [Adding SharePoint groups automatically to the IT Shop](#) on page 110
- 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, cost center, or location (role-based login)

1. In the Manager, select the **Organizations | Departments** category.
 - OR -In the Manager, select the **Organizations | Cost centers** category.
 - OR -

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

2. Select the department, cost center, or location in the result list.
3. Select the **Assign 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 105
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 106
- [Assigning SharePoint roles to SharePoint groups](#) on page 107
- [Adding SharePoint groups to system roles](#) on page 108
- [Adding SharePoint groups to the IT Shop](#) on page 108
- [Adding SharePoint groups automatically to the IT Shop](#) on page 110
- [One Identity Manager users for managing SharePoint](#) on page 9

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

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

1. In the Manager, select the **Business roles | <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign 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 departments, cost centers and locations on page 104](#)
- [Assigning SharePoint user accounts directly to a SharePoint group on page 106](#)
- [Assigning SharePoint roles to SharePoint groups on page 107](#)
- [Adding SharePoint groups to system roles on page 108](#)
- [Adding SharePoint groups to the IT Shop on page 108](#)
- [Adding SharePoint groups automatically to the IT Shop on page 110](#)
- [One Identity Manager users for managing SharePoint on page 9](#)

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 91](#)
- [Assigning SharePoint groups to departments, cost centers and locations on page 104](#)
- [Assigning SharePoint groups to business roles on page 105](#)
- [Assigning SharePoint roles to SharePoint groups on page 107](#)
- [Adding SharePoint groups to system roles on page 108](#)
- [Adding SharePoint groups to the IT Shop on page 108](#)
- [Adding SharePoint groups automatically to the IT Shop on page 110](#)

Assigning SharePoint roles to SharePoint groups

In order for SharePoint user groups 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 enabled 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 master data for SharePoint permission levels on page 120](#)
- [Assigning SharePoint groups to SharePoint roles on page 127](#)
- [Assigning SharePoint groups to departments, cost centers and locations on page 104](#)
- [Assigning SharePoint groups to business roles on page 105](#)
- [Assigning SharePoint user accounts directly to a SharePoint group on page 106](#)
- [Adding SharePoint groups to system roles on page 108](#)
- [Adding SharePoint groups to the IT Shop on page 108](#)
- [Adding SharePoint groups automatically to the IT Shop on page 110](#)

Adding SharePoint groups to system roles

Installed modules: System Roles Module

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


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

To assign a group to system roles

1. In the Manager, select the **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 assigned system roles.

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 104
- [Assigning SharePoint groups to business roles](#) on page 105
- [Assigning SharePoint user accounts directly to a SharePoint group](#) on page 106
- [Assigning SharePoint roles to SharePoint groups](#) on page 107
- [Adding SharePoint groups to the IT Shop](#) on page 108
- [Adding SharePoint groups automatically to the IT Shop](#) on page 110

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** category (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. In the **Add assignments** pane, assign the group to the IT Shop shelves.
5. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager select the **SharePoint | Groups** category (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. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
5. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **SharePoint | Groups** category (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 detailed information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- [Entering master data for SharePoint groups on page 101](#)
- [Adding SharePoint groups automatically to the IT Shop on page 110](#)
- [Assigning SharePoint groups to departments, cost centers and locations on page 104](#)
- [Assigning SharePoint groups to business roles on page 105](#)
- [Assigning SharePoint user accounts directly to a SharePoint group on page 106](#)
- [Assigning SharePoint roles to SharePoint groups on page 107](#)
- [Adding SharePoint groups to system roles on page 108](#)

Adding SharePoint groups automatically to the IT Shop

Table 31: Configuration parameter for automatically adding groups to the IT Shop

Configuration parameter	Description
QER ITShop GroupAutoPublish	Preprocessor relevant configuration parameter for automatically adding groups to the IT Shop. This configuration parameter specifies whether all Active Directory and SharePoint target system groups are automatically added to the IT Shop. Changes to this parameter require the database to be recompiled.

To add groups automatically to the IT Shop

1. In the Designer, set the **QER | ITShop | GroupAutoPublish** configuration parameter.
2. Compile the database.

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

- Synchronization ensures that the groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor.
- New groups created in One Identity Manager are added to the IT Shop.

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

1. A service item is determined for the group.

The service item is tested and modified for each group as required. The service item name corresponds to the name of the group. The service item is assigned to one of the default service categories.

- The service item is modified for groups with service items.
- Groups without service items are allocated new service items.

2. An application role for product owners is determined and the service item is assigned. Product owners can approve requests for membership in these groups. By default, the group's owner is established as product 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 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 group.
- If the owner of the 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 group does not have an owner, the **Request & Fulfillment | IT Shop | Product owner | Without owner in SharePoint** default application role is used.

3. The group is labeled with the **IT Shop** option and assigned to the **SharePoint Groups** IT Shop shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can request group memberships through the Web Portal.

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

Related topics

- [Adding SharePoint groups to the IT Shop on page 108](#)
- [Assigning SharePoint groups to departments, cost centers and locations on page 104](#)
- [Assigning SharePoint groups to business roles on page 105](#)
- [Assigning SharePoint user accounts directly to a SharePoint group on page 106](#)
- [Assigning SharePoint roles to SharePoint groups on page 107](#)
- [Adding SharePoint groups to system roles on page 108](#)
- [Default solutions for requesting SharePoint groups on page 118](#)
- One Identity Manager IT Shop Administration Guide

Additional tasks for managing SharePoint groups

After you have entered the master 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

Table 32: Configuration parameters for conditional inheritance

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

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

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

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.

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

Example of 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.

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

By using suitable controls, you want to prevent an employee from 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 33: Specifying excluded groups (SPSGroupExclusion table)

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

Table 34: Effective assignments

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

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

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

Table 35: Excluded groups and effective assignments

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

Prerequisites

- The **QER | Structures | Inherit | GroupExclusion** configuration parameter is set.
- Mutually exclusive groups belong to the same 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 not longer mutually exclusive.
5. Save the changes.

SharePoint group inheritance based on categories

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

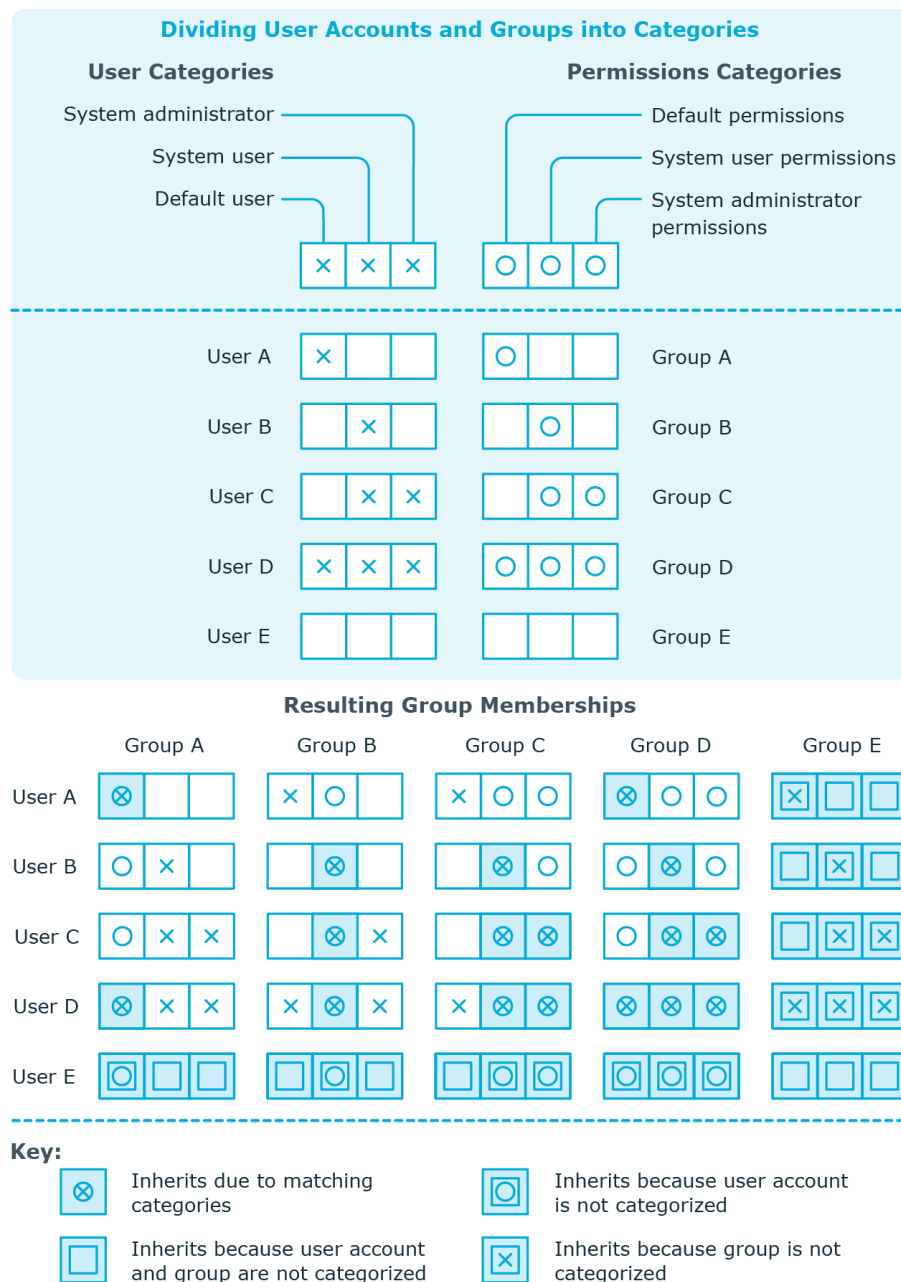
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or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

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

Table 36: 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

- Define the categories in the site collection.
- Assign categories to user accounts through their master data.
- Assign categories to groups through their master data.

Related topics

- [Specifying categories for inheriting SharePoint groups](#) on page 72
- [User authenticated user account master data](#) on page 87
- [Group authenticated user account master data](#) on page 85
- [Entering master data for SharePoint groups](#) on page 101

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.

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

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


To remove an assignment

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

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

Deleting 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, default 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 detailed information, see the *One Identity Manager Web Portal User Guide*.

Detailed information about this topic

- [Adding SharePoint groups](#) on page 118
- [SharePointRequesting Groups Memberships](#) on page 119

Adding SharePoint groups

New SharePoint groups can be created in the SharePoint environment by a request for this default 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 | GroupAutoPublish** 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 37: Default 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 110

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 38: Default objects for requesting group memberships

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

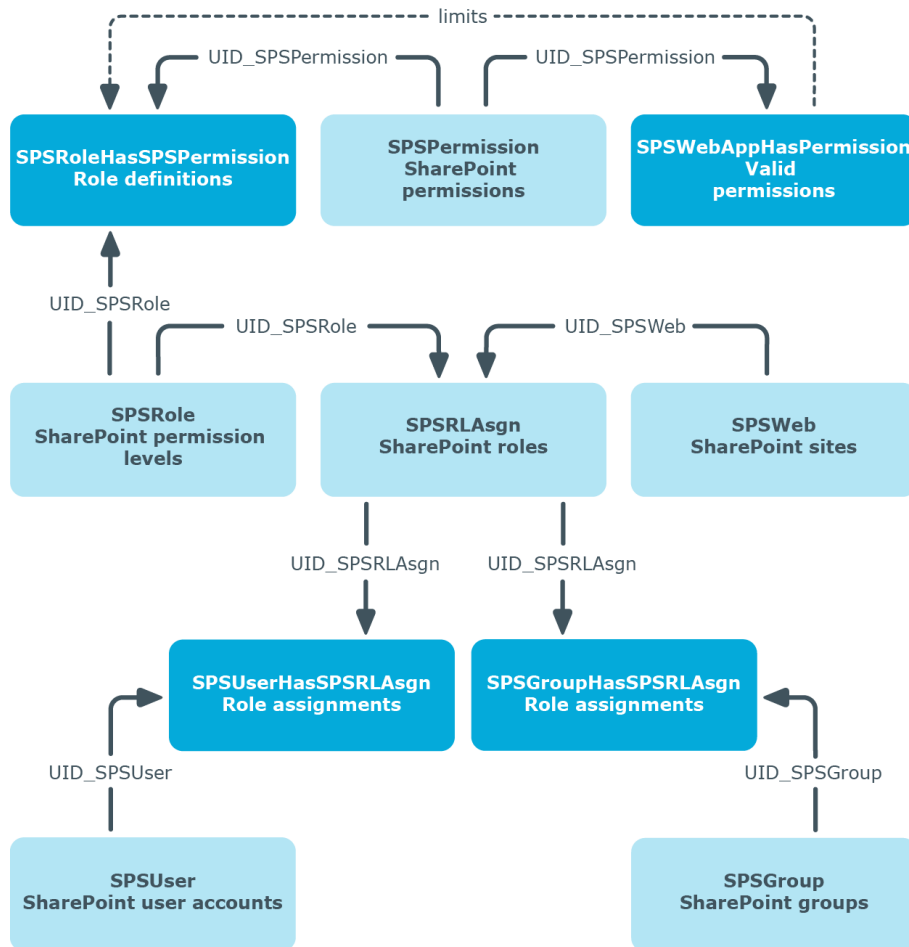
Related topics

- [Adding SharePoint groups automatically to the IT Shop](#) on page 110
- [Adding SharePoint groups](#) on page 118

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 master data for SharePoint permission levels

To edit master data for a permission level

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

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

Table 39: Properties of a permission level

Property	Description
Permission level	Name of the permissions 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 master 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 99

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 master data for SharePoint roles

Table 40: Configuration parameters for setting up SharePoint roles

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

To edit SharePoint role master data

1. Select the **SharePoint | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | Roles** category.
2. Select the SharePoint role in the result list. Select the **Change master data** task.
3. Enter the required data on the master data form.
4. Save the changes.

The following properties are displayed for SharePoint roles.

Table 41: 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 master data for SharePoint permission levels](#) on page 120
- 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 marked with the **Groups 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 master data for SharePoint permission levels](#) on page 120
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 124
- [Assigning SharePoint roles to business roles](#) on page 126
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 127
- [Assigning SharePoint groups to SharePoint roles](#) on page 127
- [Adding SharePoint roles to system roles](#) on page 128
- [Adding SharePoint roles to the IT Shop](#) on page 129
- 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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 126
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 127
- [Assigning SharePoint groups to SharePoint roles](#) on page 127
- [Adding SharePoint roles to system roles](#) on page 128
- [Adding SharePoint roles to the IT Shop](#) on page 129
- [One Identity Manager users for managing SharePoint](#) on page 9

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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 124
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 127
- [Assigning SharePoint groups to SharePoint roles](#) on page 127
- [Adding SharePoint roles to system roles](#) on page 128
- [Adding SharePoint roles to the IT Shop](#) on page 129
- [One Identity Manager users for managing SharePoint](#) on page 9

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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 master data for SharePoint permission levels](#) on page 120
- [Assigning SharePoint roles directly to user accounts](#) on page 92
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 124
- [Assigning SharePoint roles to business roles](#) on page 126
- [Assigning SharePoint groups to SharePoint roles](#) on page 127
- [Adding SharePoint roles to system roles](#) on page 128
- [Adding SharePoint roles to the IT Shop](#) on page 129

Assigning SharePoint groups to SharePoint roles

In order for SharePoint user groups 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 enabled that reference permission levels, cannot be assigned to groups.

To assign groups to a SharePoint role

1. Select the **SharePoint | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 master data for SharePoint permission levels](#) on page 120
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 124
- [Assigning SharePoint roles to business roles](#) on page 126
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 127
- [Assigning SharePoint roles to SharePoint groups](#) on page 107
- [Adding SharePoint roles to system roles](#) on page 128
- [Adding SharePoint roles to the IT Shop](#) on page 129

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 the employees' user authenticated user accounts 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 master data for SharePoint permission levels](#) on page 120.

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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 assigned system roles.

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 124
- [Assigning SharePoint roles to business roles](#) on page 126
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 127
- [Assigning SharePoint roles to SharePoint groups](#) on page 107
- [Adding SharePoint roles to the IT Shop](#) on page 129

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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 master data for SharePoint roles](#) on page 122
- [Assigning SharePoint roles to departments, cost centers and locations](#) on page 124
- [Assigning SharePoint roles to business roles](#) on page 126
- [Assigning SharePoint user accounts directly to a SharePoint role](#) on page 127
- [Assigning SharePoint groups to SharePoint roles](#) on page 127
- [Adding SharePoint roles to system roles](#) on page 128

Additional tasks for managing SharePoint roles

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

Displaying the SharePoint rules overview

To obtain an overview of a SharePoint role

1. Select the **SharePoint | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 112 can also be used for SharePoint roles.

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

Prerequisites

- The "QER | Structures | Inherit | GroupExclusion" configuration parameter is set.
- Mutually exclusive SharePoint roles belong to the same site collection.

To exclude SharePoint roles

1. Select the **SharePoint | Hierarchical view | <Farm> | Web applications | <web application> | <site collection> | <site> | 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 112

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

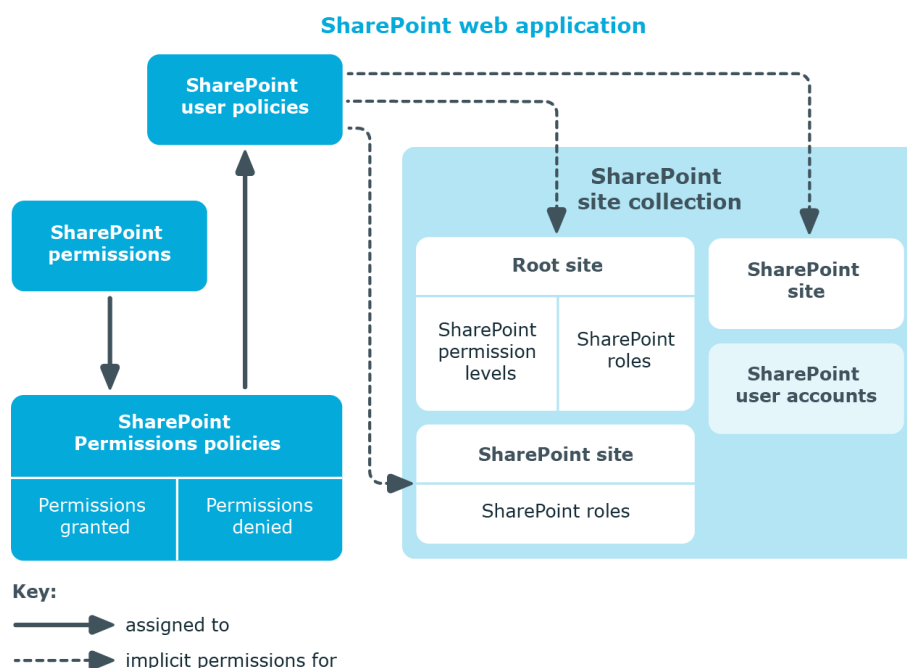
- One Identity Manager Configuration Guide

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 master data

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

The following properties are displayed for user policies.

Table 42: Master 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 User account 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 User account option is set, the following authentication objects can be assigned:</p> <ul style="list-style-type: none"> • Active Directory user accounts • LDAP user accounts <p>If the User account option is disabled, the following authentication objects can be assigned:</p> <ul style="list-style-type: none"> • Active Directory groups • LDAP groups

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 site collections

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 43: Reports for the target system

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


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 44: 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 additionally available in One Identity Manager after the module has been installed.

Table 45: Configuration parameters

Configuration parameter	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.
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.
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.

Configuration parameter	Description
TargetSystem SharePoint PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.

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 template uses mappings for the following schema types.

Table 46: 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

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

Contacting us

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

Technical support resources

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

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

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

A

- account definition 48
 - add to IT Shop 61
 - assign to system roles 61
- Active Directory domain
 - SharePoint authentication object 78
 - SharePoint synchronization 66
- Active Directory group
 - SharePoint authentication object 78
- Active Directory user account
 - SharePoint authentication object 78
- alternative URL 39
- application role
 - target system managers 45
- architecture 8
- authentication
 - authentication mode 37
 - claims based 11
- authentication mode 37
- authentication object 78

B

- base object
 - create 27

C

- calculation schedule
 - disable 34
- category 72
- configuration parameter 140
- connection parameter 17, 25, 27

- connector 8

D

- direction of synchronization
 - direction target system 26

E

- employee
 - number user accounts (report) 137
- employee assignment
 - automatic 94
 - manual 96
 - remove 96
 - search criteria 95
- exclusion definition 112, 131
- extended property
 - assign group 117
 - user account 92
- extended schema 27

F

- farm
 - domain 66
 - set up 66
 - target system managers 66

G

- group
 - about IT Shop requests 101

- add to IT Shop 108
- add to IT Shop (automatic) 110
- add to system role 108
- assign category 101
- assign extended properties 117
- assign SharePoint role 107
- assign to business role 105
- assign to cost center 104
- assign to department 104
- assign to location 104
- assign user account 103, 106
- category 114
- delete 117
- drifted (report) 137
- effective 112
- exclusion 112
- group membership 106
- inheriting through categories 72
- inheriting through system roles 108
- overview form 112
- owner 101
- request 118-119
- risk index 101
- role assignment 75
- set up 100
- group prefix 37

I

- IT operating data
 - change 57
- IT Shop shelf
 - assign account definition 61
 - assign group 108
 - assign SharePoint roles 129

J

- Job server
 - load balancing 33
 - properties 42

L

- language 39-40
- LDAP domain
 - SharePoint authentication object 78
 - SharePoint synchronization 66
- LDAP group
 - SharePoint authentication object 78
- LDAP user account
 - SharePoint authentication object 78
- load balancing 33
- login 9

M

- manage level 51
- membership
 - modify provisioning 31

O

- object
 - delete immediately 29
 - outstanding 29
 - publish 29
- orphaned user accounts (report) 137
- outstanding object 29

P

- permission 39
 - assign permissions level 39
 - permitted permissions 39, 69
 - synchronizing 24
- permissions level 39, 119-120
 - assign permissions 121
 - assign to group 120
 - assign to user account 120
 - delete 132
 - overview form 121
 - permitted permissions
 - synchronizing 122
 - role definition 99, 121
 - site 120
- permissions policy 39, 134
 - denied permissions 134
 - granted permissions 134
 - synchronization object type 134
- prefix 11, 37-38
 - create site 74
- product owners 110
 - request group 118
- project template 142
- provider 11, 69
- provisioning
 - accelerate 33
 - members list 31

Q

- quota 40

R

- relative URL 38
- report
 - overview of all assignments 138
 - site collection 137
- request
 - authorizations 118
 - group membership 119
 - groups 118
- revision filter 29
- role
 - about IT Shop requests 122
 - add to IT Shop 129
 - add to system role 128
 - assign group 127
 - assign to business role 126
 - assign to cost center 124
 - assign to department 124
 - assign to location 124
 - assign user account 124, 127
 - delete 132
 - effective 131
 - exclusion 131
 - hierarchical role inheritance 124
 - inheriting through system roles 128
 - map in One Identity Manager 119
 - overview form 131
 - permissions inheritance 99
 - permissions level 99, 122
 - risk index 122
 - role assignment 99, 127
 - role definition 75, 99
 - site 122

- root site 73
 - site 72
 - site collection 71

S

- schema
 - changes 28
 - shrink 28
 - update 28
- scope 25
- server farm account 13
- server function 44
- single object synchronization
 - accelerate 33
- site 72
 - anonymous access 73
 - author 73
 - create 76
 - prefix 74
 - request through IT Shop 76
 - role assignment 73, 75
 - role definition 73, 75
 - root site 72-73
 - permissions inheritance 75, 99
 - site template 74
 - subordinate 99
 - URL 74
 - open 74
- site collection 70
 - account definition 71
 - administrator 71
 - category 114
 - create 76
 - employee assignment 95
 - quota 40

- request through IT Shop 76
- root site 71
 - permissions inheritance 75, 99
- server 71
- specify category 72
- URL 71
- site template 39
 - create site 74
- synchronization
 - accelerate 29
 - configure 17
 - configure synchronization 14
 - connection data 17
 - different farms 27
 - Microsoft.SharePoint.dll 14
 - permissions 13
 - prerequisites 12
 - prevent 34
 - provider 11
 - start 17
- synchronization analysis report 34
- synchronization configuration
 - customize 25-27
 - remote connection 26-27
- synchronization log 24
- synchronization project
 - disable 34
 - edit 67
 - project template 142
 - set up 17
- synchronization server
 - edit 41
 - server function 44
- synchronization workflow
 - create 26

T

- target system manager 45
 - assign 66
- target system schema 27
- target system synchronization 29
- template
 - IT operating data, modify 57

U

- unused user accounts (report) 137
- URL
 - prefix 38
 - site 74
 - site collection 71
- user 9
 - synchronization 13
- user account 78
 - administrative user account 80
 - administrator 85, 87
 - apply template 57
 - assign category 85, 87
 - assign employee 87, 94
 - assign extended properties 92
 - assign group 91, 106
 - assign role 92
 - assign SharePoint role 127
 - auditor 85, 87
 - authentication mode 93
 - authentication object 78, 85, 87, 93
 - authentication system 85, 87
 - category 114
 - create automatically 48
 - custom template 93

- default user accounts 80
- deferred deletion 97
- delete 97
- identity 80, 85, 87
- lock 97
- login name 85, 87, 93
- more than 1 per employee 78
- number of group memberships (report) 137
- overview 91
- permissions for synchronization 13
- privileged user account 80, 85, 87
- retrieve 97
- risk index 85, 87
- role assignment 75
- set up 84
- type 80

- user definition 134
 - Active Directory user account 134
 - assign employee 134
 - authentication object 134
 - global 135
 - system account 134
 - Web application 134
 - zone 134
 - zone specific 135
- user prefix 37

V

- variable 25
- variable set 27

W

Web application 69

- alternative URL 39

- claims authentication 69

- cross permissions 133

- permissions policy 69, 133

- permitted conditions 69

- user definition 69, 133

- valid permissions 39, 69

workflow 26

Z

zone 39

- user definition 134