



One Identity Manager 9.0

One Identity Manager Connector User Guide

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

-  **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**
-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

Contents

Setting up synchronization with the One Identity Manager connector	5
Architecture overview	6
Synchronization set up method	6
Prerequisites and guidance for connecting a One Identity Manager database	8
Setting up the synchronization server	9
Setting up system synchronization	12
Users and permissions for system synchronization	13
Setting up custom application roles for system synchronization	13
Preparing work database for setting up system synchronization	14
Selecting tables and columns for system synchronization	16
Information required for creating a synchronization project for system synchron- ization	18
Creating a synchronization project for the system synchronization	20
Starting system synchronization	23
Displaying the synchronization log	23
Modifying the synchronization configuration	24
Transferring synchronization configuration into another database	24
Disabling system synchronization	25
Setting up synchronization using custom configuration	26
Users and permissions for synchronizing	26
Setting up custom application roles for custom configuration	31
Information required for creating a synchronization project for custom synchron- ization	32
Creating custom configurations	35
Updating schemas	38
Configuring the provisioning of memberships	39
Configuring single object synchronization	41
Starting synchronization	42
Analyzing synchronization	43
Post-processing outstanding objects	43
Configuring target system synchronization	44

Post-processing outstanding objects	46
Troubleshooting	48
Ignoring data error in synchronization	48
Help for analyzing synchronization issues	49
About us	50
Contacting us	50
Technical support resources	50
Index	51

Setting up synchronization with the One Identity Manager connector

The One Identity Manager connector allows One Identity Manager databases to synchronize with each other. For example, in this way, you can transfer application data from a production database to a test database or have time-consuming tasks, such as attestations or the report generation, run in a separate environment. You can optimize use of One Identity Manager functionality by synchronizing with a central database, containing all the data, on a regular basis.

As of One Identity Manager version 8.2, there is support for synchronizing databases with different product versions or a different number of modules.

One Identity Manager offers two ways to set up a synchronization project:

1. Generate a synchronization project based on predefined criteria
The synchronization configuration is created completely automatically and cannot be edited. Three schedules can be selected to start synchronization.
2. Individual, manual configuration of the synchronization
The synchronization configuration is created completely manually and can be adapted at any time if requirements change. The synchronization can be scheduled as well as started manually.

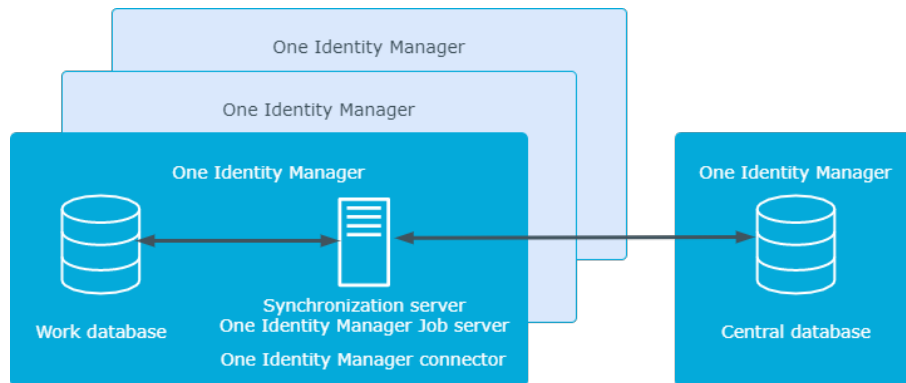
Detailed information about this topic

- [Architecture overview](#) on page 6
- [Synchronization set up method](#) on page 6
- [Prerequisites and guidance for connecting a One Identity Manager database](#) on page 8
- [Setting up the synchronization server](#) on page 9
- [Setting up synchronization using custom configuration](#) on page 26
- [Setting up system synchronization](#) on page 12

Architecture overview

As of One Identity Manager version 8.2, there is support for synchronizing databases with different product versions or a different number of modules. The central database must be connected over an application server for this. To be able to use the latest features and bug fixes, the database on which the synchronization project is set up must always have the latest product version.

Figure 1: The synchronization architecture



The **work database** is the database on which the synchronization project is set up. After synchronization, the work database contains an image of the application data from the central database. The **central database** is the database in the connected system (target system).

If both databases have the same product version and the same modules installed, you do not have to connect the central database through an application server.

Synchronization set up method

Method 1 (system synchronization): The synchronization project is created automatically

To allow a synchronization project to be created automatically, first select the tables and columns from all the tables that contain application data. On basis of this, the Synchronization Editor generates a complete synchronization configuration. If the selection of tables to synchronize changes, the synchronization project updates automatically.

Use the system synchronization to map selected One Identity Manager database application data. The same schema types (tables) and schema properties (columns) are synchronized with each other in the connected databases. For example, if you have selected the BaseTree table for synchronization, the objects of the BaseTree table in the central database will be synchronized with the BaseTree table in the work database.

Only one synchronization project can be created automatically for the work database.

Only the connection credentials for the connected systems may be changed manually in a generated synchronization project.

Method 2 (custom configuration): You create the synchronization project manually

This allows you to create all the components of the synchronization configuration manually with the Synchronization Editor. The One Identity Manager connector does not provide a project template for setting up synchronization. The synchronization project can be adjusted at any time as needed.

Since the synchronization configuration is fully customized, the schema types and schema properties of the central database can be mapped to any schema types and properties in the work database.

Selecting a method

Use the system synchronization if the following criteria apply:

- You want to map selected application data from the central database. The application data are mapped in both databases in the same tables.
- Numerous tables are to be synchronized.
- Different startup behavior is to be defined for different tables.
- One Identity Manager creates the system configuration automatically. The synchronization configuration does not require manual adjustments.

Use individual synchronization if the following criteria apply:

- Only individual tables are to be synchronized.
- You want to be able to create mappings and workflows yourself and customize the synchronization configuration.
- You want to use custom processing methods in synchronization steps.
- Objects that have been deleted in the central database should be marked as outstanding during synchronization and can then be post-processed in the work database.
- Single object synchronization is to be used.

Connect the central database over an application server if the following criteria apply:

- A different number of modules is installed in the work than in the central database.
- Work and central databases have different product versions, but at least One Identity Manager version 8.2.

Related topics

- [Setting up synchronization with the One Identity Manager connector on page 5](#)
- [Prerequisites and guidance for connecting a One Identity Manager database on page 8](#)

- [Setting up system synchronization](#) on page 12
- [Setting up synchronization using custom configuration](#) on page 26

Prerequisites and guidance for connecting a One Identity Manager database

Requirements for the central database

To synchronize One Identity Manager databases with different modules or different product versions:

- The central database is connected over an application server.
- The **System user** authentication module is enabled and assigned to the application server.

To synchronize One Identity Manager databases with different product versions:

- The following plugins are enabled on the application server:
 - API (restapi)
 - Meta Data (metadata)
 - One Identity Manager Sync Access (sync)
- The HTTP request methods POST, GET, PUT, and DELETE must be permitted by the application server's web server.
- The central database has at least version 8.2.

Notes about the application server's REST API

The REST API is not as powerful as the primary interface because it is designed for backward compatibility, among other things. This enables communication with older One Identity Manager systems. Some secondary functions are not available when using this interface. One Identity Manager versions from 8.2 are supported, but possibly not to the full extent.

- Customized processing methods in synchronization steps cannot be used.
- Data errors cannot be ignored during synchronization.
- No detailed error messages are output.

Notes about the work database

- If both databases have different One Identity Manager versions, the work database should have the latest product version to take advantage of the latest features and bug fixes of the One Identity Manager connector.
- The work database has at least version 8.2.

Related topics

- [Setting up synchronization with the One Identity Manager connector](#) on page 5

Setting up the synchronization server

A server with the following software must be available for setting up synchronization:

- One Identity Manager Service
 - Install One Identity Manager components with the installation wizard.
 1. Select **Select installation modules with existing database**.
 2. Select the **Server | Job Server** machine role.

For more information about system requirements for installing the One Identity Manager Service, see the *One Identity Manager Installation Guide*.

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

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

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

NOTE: The program performs a remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

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

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For more information about setting

up Job servers, see the *One Identity Manager Configuration Guide*.

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.
3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.
 - a. Select a Job server from the **Server** menu.
- OR -
To create a new Job server, click **Add**.
 - b. Enter the following data for the Job server.
 - **Server:** Name of the Job server.
 - **Queue:** Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
 - **Full server name:** Full server name in accordance with DNS syntax.
Syntax:
`<Name of servers>.<Fully qualified domain name>`

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

4. On the **Machine roles** page, select **Job server**.
5. (For system synchronization) On the **Server functions** page, select **One Identity Manager synchronization**.
(For custom synchronization) On the **Server functions** page, select **One Identity Manager connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

- For a direct connection to the database:
 1. Select **Process collection > sqlprovider**.
 2. Click the **Connection parameter** entry, then click the **Edit** button.
 3. Enter the connection data for the One Identity Manager database.

- For a connection to the application server:
 1. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
 2. Click the **Connection parameter** entry, then click the **Edit** button.
 3. Enter the connection data for the application server.
 4. Click the **Authentication data** entry and click the **Edit** button.
 5. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
- 7. To configure remote installations, click **Next**.
- 8. Confirm the security prompt with **Yes**.
- 9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
- 10. If the database is encrypted, on the **Select private key file** page, select the file with the private key.
- 11. On the **Service access** page, enter the service's installation data.
 - **Computer:** Enter the name or IP address of the server that the service is installed and started on.
 - **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

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

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

Setting up system synchronization

System synchronization allows you to map selected application data from one One Identity Manager database into a second One Identity Manager database. The synchronization configuration is generated completely automatically based on selected criteria.

To generate a synchronization project

1. Provide One Identity Manager users with the necessary permissions to set up synchronization.

NOTE:

- You can only use non role-based credentials to log in to the Designer.
 - Role-based login is only possible for the Launchpad and the Synchronization Editor.
2. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
 3. To be able to successfully run system synchronization, you need to set some properties on the work database.
 4. In the Designer, mark the tables and columns whose contents you want synchronized.
 5. Generate a synchronization project with the Synchronization Editor.

Only the connection credentials for the connected systems may be changed manually in a generated synchronization project.

Detailed information about this topic

- [Users and permissions for system synchronization](#) on page 13
- [Setting up the synchronization server](#) on page 9
- [Preparing work database for setting up system synchronization](#) on page 14
- [Selecting tables and columns for system synchronization](#) on page 16
- [Information required for creating a synchronization project for system synchronization](#) on page 18
- [Creating a synchronization project for the system synchronization](#) on page 20

Related topics

- [Synchronization set up method](#) on page 6

Users and permissions for system synchronization

For non role-based login to the One Identity Manager tools you need:

- To select tables and columns to synchronize: An administrative system user working with the Designer
- To set up synchronization: A system user with **DPR_EditRights_Methods** and **QBM_LaunchPad** permissions groups.

For the role-based login you need:

- To select tables and columns to synchronize: An administrative system user working with the Designer
You can only use non role-based credentials to log in to the Designer.
- To set up synchronization: a custom application role
The application role gets its permissions through a custom permissions group and the **vi_4_SYNCPROJECT_ADMIN** permissions group.

For more information about system users and permissions groups, see the *One Identity Manager Authorization and Authentication Guide*.

Detailed information about this topic

- [Setting up custom application roles for system synchronization](#) on page 13

Setting up custom application roles for system synchronization

To grant One Identity Manager users the necessary permissions to set up synchronization when using role-based login, create a custom application role. This application role obtains the required permissions by using a custom permissions group.

To set up an application role for synchronization

1. In the Designer, create a new permissions group .
 - Set the **Only use for role based authentication** option.

2. Make the new permissions group dependent on the **vi_4_SYNCPROJECT_ADMIN** permissions group.
 - Select the **Inherit permissions from** context menu item and select the **vi_4_SYNCPROJECT_ADMIN** permissions group.
3. Save the changes.
4. In the Manager, create a new application role.
 - a. Assign the **Custom | Managers** application role as the parent application role.
 - b. Assign the newly created permissions group.
5. Assign employees to this application role.
6. Save the changes.

For more information about setting up application roles and permissions groups, see the *One Identity Manager Authorization and Authentication Guide*.

Related topics

- [Users and permissions for system synchronization](#) on page 13

Preparing work database for setting up system synchronization

To be able to successfully run system synchronization, some properties must be set on the work database. You can run the SQL queries listed here with a suitable program.

TIP: Depending on the purpose of the work database, it may be useful to adjust further settings. For example, check whether to disable templates on the synchronized columns in the work database.

Using the GUID module

The **Module GUID permitted** table property (`DialogTable.IsModuleGUIDAllowed`) table property must be set on all the tables you want to synchronize. To enable this option, run the following query on the central database first and then on the work database.

```
-- transfer customized configuration DialogTable.IsModuleGUIDAllowed from your central
database
-- => manual process required
select UID_DialogTable, 'Update DialogTable set IsModuleGUIDAllowed = 1
  where IsModuleGUIDAllowed = 0 and UID_DialogTable = ''' + UID_DialogTable + ''' ' as
ChangeStatement
  from DialogTable where IsModuleGUIDAllowed = 1
--if you got an result, copy the commands and execute them in your work database
```

Disabling all provisioning processes

Since there are no target systems associated with the work database, the standard provisioning processes should not be run here. Run the queries for this on the work database.

The following query disables all processes for the tables:

- PersonHasTSBAccountDef
- PersonHasQERResource
- TSBAccountDef (TSB_TSBAccountDef_AutoAssignToPerson and TSB_TSBAccountDef_AutoRemoveFromPerson)

```
-- deactivate all predefined provisioning processes
update JobChain set NoGenerate = 1, XDateUpdated = GETUTCDATE(), XUserUpdated = 'SysSyn-
cInitialConfig' from JobChain JC
    join JobEventGen JEG on JEG.UID_JobChain = JC.UID_JobChain
    join QBMEvent JE on JE.UID_QBMEvent = JEG.UID_QBMEvent where
    (
        JE.EventName in ('Insert', 'Update', 'Delete', 'Assign', 'Remove')
    or JC.UID_DialogTable in ('TSB-T-PersonHasTSBAccountDef', 'QER-T-PersonHasQERRe-
source')
    or UID_JobChain in ('TSB-F9E8F1B2DA86E847A254E70A572A3832', 'TSB-
EB76885961C6404FB7BB73FC1AC83153')
    )
    and dbo.QBM_FCVIDToModuleOwner(JC.UID_JobChain) <> 'CCC'
    and NoGenerate = 0
```

The following query disables the merge mode of single membership provisioning for all assignment tables.

```
-- deactivate merge for provisioning (DPRMemberShipAction) for all synchronized tables
update DPRNameSpaceHasDialogTable set IsAdHocSingleMembership = 0, WhereClause = Null
```

The following query prevents dependencies' modification dates from updating on assignment base tables.

```
-- deactivate XDateSubItem behavior for all synchronized tables
update QBMRelation set IsForUpdateXDateSubItem = 0 where UID_QBMRelation in
(
    select UID_QBMRelation from QBM_VQBMRelation r
        join DialogTable t on r.UID_DialogTableChild=t.UID_DialogTable or r.UID_Dialo-
gTableParent=t.UID_DialogTable
            where t.SystemSyncMode > 0 and r.IsForUpdateXDateSubItem = 1
    )
```

Disabling schedules

The following query disables all schedules except for custom schedules and system schedules. Modify this query for the purposes of the work database. Run the query on the

work database.

```
-- deactivate all not required schedules
-- allow only system and custom schedules as well as such ones belonging to reports and
attestation
-- but disable all synchronization schedules except the system synchronization
update DialogSchedule
  set Enabled = 0, XDateUpdated = GETUTCDATE(), XUserUpdated = 'SysSyncInitialConfig'
  where Enabled = 1 and
    (
      dbo.QBM_FCVGUIDToModuleOwner(UID_DialogSchedule) not in
('CCC', 'QBM', 'QER', 'RPS', 'ATT')
      or (Name like '%execution of Initial Synchronization%' and Name
not like 'System Synchronization%')
    )
```

Disabling DBQueue Processor tasks for SAP objects

Since there are no target systems associated with the work database, DBQueue Processor tasks for processing SAP objects can be disabled. Run the query on the work database.

```
-- disable SAP/SBW DBQueueTask for generation SAPUserMandant and SAPBWUser
update QBMDBQueueTask
  set ProcedureName = 'QBM_ZDBQueueVoidTask', CountParameter = 0, MaxInstance = 1,
IsBulkEnabled = 0, QueryForRecalculate = Null
  where UID_Task in ('SAP-K-SAPUserMandant', 'SBW-K-SAPBWUser')
```

Related topics

- [Setting up system synchronization](#) on page 12

Selecting tables and columns for system synchronization

Before you create a synchronization project for system synchronization, flag all the table and column content to synchronize.

Notes on selecting tables and columns

- For each table selected, specify the mapping direction for all primary key columns and mandatory columns.
- For each table selected, specify the mapping direction for the XOrigin and XIsInEffect columns.
- For each table selected with multi-column uniqueness definitions, specify the mapping direction for all columns that make up the unique group and are not

populated automatically.

- If a base table and its derivatives are selected (for example, BaseTree and Department), then set the same synchronization configuration for both tables.
 - Same synchronization mode for the base table and its derivatives
 - Same columns to be mapped
 - Same mapping direction for these columns

To select a table for system synchronization

1. In the Designer, select the **One Identity Manager schema** category.
2. Select the table and start the Schema Editor with the **Show table definition** task.
3. In the **Table properties** view, select the **System synchronization** tab.
4. Edit the following table properties:
 - **Synchronization mode:** Permitted synchronization directions and processing methods for this table. Set all the bit positions that apply to this table.
Set:
 - The direction of synchronization
 - Whether to provision changes to the central database,
 - Which processing methods to use for application data
 - Whether to update system data
 - Which schedule to use for synchronizing this table (start frequency)
If neither the **Start synchronization frequently** or the **Start synchronization very frequently** bit positions is set, synchronization is started once a day (default).
 - **Columns for alternative rules:** Comma delimited list of columns to be used for creating alternative object matching rules.
If the One Identity Manager connector cannot identify a system object through the primary object matching rule, it applies the alternative rules to determine a matching system object. Enter the technical names of all the columns for which you want to generate alternative rules.
 - **Columns for alternative rules:** .NET class used to consider special cases when generating a synchronization project between two One Identity Manager databases.
5. Set the permitted mapping direction for all columns to be mapped.
 - a. Select the column in the Schema Editor and edit the column properties.
 - b. On the **More** tab, in the **Mapping direction** menu, select all permitted mapping directions.
6. Perform steps 2 to 5 for all the tables that are going to be synchronized.
7. Select the **Database > Save to database** and click **Save**.

IMPORTANT: If an assignment table is selected for synchronization and the **Provisioning the central database** synchronization mode is selected, the table's **Assign by event** property must be enabled for this table to generate the provisioning processes.

If this table property is enabled after a synchronization project has been generated, then the synchronization project must be regenerated.

To set the mapping direction for a column

1. In the Designer, select the **One Identity Manager schema** category.
2. Select the table and start the Schema Editor with the **Show table definition** task.
3. Select the column in the Schema Editor and edit the column properties.
4. On the **More** tab, in the **Mapping direction** menu, select all permitted mapping directions.
5. Select the **Database > Save to database** and click **Save**.

If you change the tables or columns to be synchronized after the synchronization project has been generated, the synchronization project will be updated automatically.

Related topics

- [Setting up system synchronization](#) on page 12

Information required for creating a synchronization project for system synchronization

To set up a synchronization project for system synchronization, have the following information ready.

Table 1: Information required to set up a synchronization project

Data	Explanation
Connection credentials for the central database	<p>For direct database connection:</p> <ul style="list-style-type: none">• Database server• Database name• SQL Server login and password• Specifies whether integrated Windows authentication is used <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that</p>

Data	Explanation
	<p>your environment supports Windows authentication.</p> <p>For connecting through an application server:</p> <ul style="list-style-type: none"> • Application server URL • Synchronization user's password
<p>Connection credentials for the work database</p>	<ul style="list-style-type: none"> • Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p>
<p>Synchronization server</p>	<p>All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>Installed components:</p> <ul style="list-style-type: none"> • One Identity Manager Service (started) <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 9.</p>
<p>Remote connection server</p>	<p>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed

Data	Explanation
	<p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>

Detailed information about this topic

- [Creating a synchronization project for the system synchronization](#) on page 20

Creating a synchronization project for the system synchronization

NOTE: Exactly one synchronization project for system synchronization can be created for a work database.

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

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

- Run in default mode
- Started from the Launchpad

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

To set up a synchronization project

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

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

2. Select the **One Identity Manager connector** entry and click **Start**.

This starts the Synchronization Editor's project wizard.

3. On the **System access** page, specify how One Identity Manager can access the target system.
 - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
 - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
 - Click **Next** to start the system connection wizard to create a connection to a One Identity Manager database.
4. Select the database system to which you want to connect on the **Select database system** page.
 - **Direct database connection:** Specifies whether to connect directly to the central database.
 - **Application server:** Specifies whether the central database should be connected through an application server.

Set this option if modules other than in the work database are installed in the central database, or if the central database is running with an older version of One Identity Manager.
 - **Use application server REST API:** Specifies whether to use the application server's REST API for communicating with the central database.

IMPORTANT: Enable this option if the central database is operated with an older version of One Identity Manager.
5. On the **Connection parameters** page, enter the database credentials for the central database.
 - Enter the following data connecting directly to the database:
 - **Server:** Database server.
 - (Optional) **Windows Authentication:** Specifies whether the 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.
 - **User:** The user's SQL Server login name.
 - **Password:** Password for the user's SQL Server login.
 - **Database:** Select the database.
 - To connect through an application server, enter the **URL** and **Synchronization user password**.
 - To enter additional information about the database connection, click **Advanced options**.
 - Click **Test**.
6. Enter the private key for encrypting the database on the **Encryption** page.

7. On the **Additional settings** page, you define additional settings to customize the behavior of the connector.

- **Try to ignore data errors:** Specifies whether objects with erroneous data should be synchronized with the central database.

By default, objects with incorrect data are not synchronized. For example, a user account is not loaded in the One Identity Manager database if, in the user account table, the formatting script of a column contains an email address detects invalid data. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors.

IMPORTANT: If data errors are ignored, performance will be affected. Synchronization can also lead to data loss. Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

NOTE:

- The option cannot be enabled if the REST API of the application server is used.
- Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.

8. On the last page of the system connection wizard, you can save the connection data.

- Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
- Click **Finish**, to end the system connection wizard and return to the project wizard.

9. 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.

10. 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.

11. On the **Select project template** page, select a project template to use for setting up the synchronization configuration.

- Select **AutomaticOne Identity Manager synchronization**.

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

13. Save the synchronization project in the database.

Only the connection credentials for the connected systems may be changed manually in a generated synchronization project.

Related topics

- [Information required for creating a synchronization project for system synchronization](#) on page 18
- [Ignoring data error in synchronization](#) on page 48
- [Creating custom configurations](#) on page 35

Starting system synchronization

Three schedules are generated for starting system synchronization. By default, synchronization is started once a day. If you want synchronization to start more frequently for certain tables, adjust the synchronization mode for these tables.

To change how frequently a table is synchronized

1. In Designer, edit the table properties of the table you want to synchronize.
2. On the **System synchronization** tab, select the **Synchronization mode** menu.
3. Select the synchronization frequency.
 - If you want to start synchronization several times a day, activate **Start synchronization frequently**.
 - If you want to start synchronization several times per hour, activate **Start synchronization very frequently**.

If none of these options is enabled, this table will be synchronized once a day.

4. Save the changes.

NOTE: Synchronization can only be started if the synchronization project is activated.


Related topics

- [Disabling system synchronization](#) on page 25

Displaying the synchronization log

Synchronization results are summarized in the synchronization log.

To display a synchronization log

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

Logs for all completed synchronization runs are displayed in the navigation view.

4. Select a log by double-clicking it.

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

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.

Modifying the synchronization configuration

A generated synchronization project can only be edited to a limited extent. The following changes are possible:

- Connection credentials for the central database
- Connection credentials for the work database
- Selection of the tables to be synchronized and the mapped columns

If the selection of the tables to be synchronized or the mapped columns is changed, the synchronization project will be updated automatically after a short delay.

Other manual changes to the synchronization configuration will be overwritten when the synchronization project is updated.

Related topics

- [Selecting tables and columns for system synchronization](#) on page 16

Transferring synchronization configuration into another database

If you want to transfer the system synchronization configuration to another database, it is not enough to simply transport the synchronization project. Instead, you need to transport the selected tables and mapped columns that are going to be synchronized and regenerate the synchronization configuration in the target database with this data.

To transfer a system synchronization configuration to another database

1. Use the Database Transporter to create a transport package for your changes to DialogTable and DialogColumn.
2. Import the transport package into the target database with the Database Transporter.
3. Set up the system synchronization in the target database.

For more information about creating and importing transport packages, see the *One Identity Manager Operational Guide*.

Related topics

- [Creating a synchronization project for the system synchronization](#) on page 20

Disabling system synchronization

Regular synchronization can only be started if schedules are enabled.

To prevent regular synchronization

- In the Designer, disable the **Daily database synchronization**, **Frequent database synchronization**, and **Most frequent database synchronization** schedules.

If you do not want synchronization to be started manually, deactivate the synchronization project as well.

To deactivate the synchronization project

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

Related topics

- [Starting system synchronization](#) on page 23

Setting up synchronization using custom configuration

To manually set up synchronization with a One Identity Manager database, follow the steps described here.

To set up synchronization manually

1. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
2. Provide One Identity Manager users with the required permissions for setting up synchronization and post-processing synchronization objects.
3. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Setting up the synchronization server](#) on page 9
- [Users and permissions for synchronizing](#) on page 26
- [Information required for creating a synchronization project for custom synchronization](#) on page 32
- [Synchronization set up method](#) on page 6

Users and permissions for synchronizing

In the synchronization with the database connectors, there are three use cases for mapping synchronization objects in the One Identity Manager data model.

1. Mapping custom target systems
2. Mapping default tables (for example Person or Department)
3. Mapping custom tables

In the case of One Identity Manager tools non role-based login, it is sufficient to add a system user in the **DPR_EditRights_Methods** and **QBM_LaunchPad** permissions groups. For more information about system users and permissions groups, see the *One Identity Manager Authorization and Authentication Guide*.

Table 2: Users and permissions groups for non role-based login

User	Tasks
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> • 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.
System users in the DPR_EditRights_Methods permissions group	<ul style="list-style-type: none"> • Configure and start synchronization in the Synchronization Editor. • Edit the synchronization's target system types as well as outstanding objects in the Manager.
System users in the QBM_LaunchPad permissions group	<ul style="list-style-type: none"> • Working with the Launchpad.

There are different steps required for role-based login, in order to equip One Identity Manager users with the required permissions for setting up synchronization and post-processing of synchronization objects.

Table 3: User and permissions groups for role-based login: Mapped as custom target system

User	Tasks
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p>

User	Tasks
Target system 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. <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 Custom target systems 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. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have another identity than the Primary identity. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.

User	Tasks
	<ul style="list-style-type: none"> • 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.

Table 4: User and permissions groups for role-based login: Default table mapping

User	Tasks
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> • 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.
Custom application role	<p>Users with this application role:</p> <ul style="list-style-type: none"> • Configure and start synchronization in the Synchronization Editor. • Edit the synchronization's target system types as well as outstanding objects in the Manager. <p>The application role gets its permissions through a custom permissions group and the vi_4_SYNCPROJECT_ADMIN permissions group.</p>

Table 5: Users and permissions groups for role-based login: Custom table mapping (only custom configuration)

User	Tasks
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.

User	Tasks
Application roles for custom tasks	<p>One Identity Manager administrators:</p> <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. <p>Administrators must be assigned to the Custom Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Administrate custom application roles. • Set up other application roles for managers if required.
Manager for custom tasks	<p>Managers must be assigned to the Custom Managers application role or a child role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Add custom task in One Identity Manager. • Configure and start synchronization in the Synchronization Editor. • Edit the synchronization's target system types as well as outstanding objects in the Manager. <p>You can use these application roles, for example, to guarantee One Identity Manager user permissions on custom tables or columns. All application roles that you define here must obtain their permissions through custom permissions groups.</p> <p>The application role gets its permissions through a custom permissions group and the vi_4_SYNCPROJECT_ADMIN permissions group.</p>

To configure synchronization projects and target system synchronization (in the use cases 2 and 3)

1. Set up a custom permissions group with all permissions for configuring synchronization and editing synchronization objects.
2. Assign a custom application role to this permissions group.

Detailed information about this topic

- [Setting up custom application roles for custom configuration](#) on page 31

Setting up custom application roles for custom configuration

For role-based login, create a custom application role to guarantee One Identity Manager users the necessary permissions for configuring synchronization and handling outstanding objects. This application role obtains the required permissions by using a custom permissions group.

To set up an application role for synchronization (use case 2):

1. In the Manager, select the default application role to use to edit the objects you want to synchronize.

- Establish the application role's default permissions group.

If you want to import employee data, for example, select the **Identity Management | Employees | Administrators** application role. The default permissions group of this application role is **vi_4_PERSONADMIN**.

2. In the Designer, create a new permissions group .

- Set the **Only use for role based authentication** option.

3. Make the new permissions group dependent on the **vi_4_SYNCPROJECT_ADMIN** permissions group.

Then the **vi_4_SYNCPROJECT_ADMIN** permissions groups must be assigned as the parent permissions group. This means that the new permissions group inherits the properties.

4. Make the new permissions group dependent on the default permissions group of the selected default application role.

Then the default permissions groups must be assigned as the parent permissions group. This means that the new permissions group inherits the properties.

5. Save the changes.

6. In the Manager, create a new application role.

- a. Assign the selected application role to be the parent application role.
- b. Assign the newly created permissions group.

7. Assign employees to this application role.

8. Save the changes.

To set up an application role for synchronization (use case 3):

1. In the Designer, create a new permissions group for custom tables that are populated by synchronization.
 - Set the **Only use for role based authentication** option.
2. Guarantee this permissions group all the required permissions to the custom tables.
3. Create another permissions group for synchronization.
 - Set the **Only use for role based authentication** option.
4. Make the permissions group for synchronization dependent on the permissions group for custom tables.

Then the permissions group for custom tables must be assigned as the parent permissions group. This means the permissions groups for synchronization inherits its properties.
5. Make the permissions group for synchronization dependent on the **vi_4_SYNCPROJECT_ADMIN** permissions group.

Then the **vi_4_SYNCPROJECT_ADMIN** permissions groups must be assigned as the parent permissions group. This means the permissions groups for synchronization inherits its properties.
6. Save the changes.
7. In the Manager, create a new application role.
 - a. Assign the **Custom | Managers** application role as the parent application role.
 - b. Assign the permissions group for the synchronization.
8. Assign employees to this application role.
9. Save the changes.

For more information about setting up application roles and permissions groups, see the *One Identity Manager Authorization and Authentication Guide*.

Information required for creating a synchronization project for custom synchronization

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.

Make the following information available for setting up a custom synchronization project for synchronizing with the One Identity Manager connector.

Table 6: Information required to set up a synchronization project

Data	Explanation
Synchronization server	<p>All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>Installed components:</p> <ul style="list-style-type: none">• One Identity Manager Service (started) <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 9.</p>
Remote connection server	<p>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none">• One Identity Manager Service is started• RemoteConnectPlugin is installed <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>
Synchronization workflow	<p>Set the Data import option in the synchronization step if synchronization data is imported from a secondary system. You cannot select the MarkAsOutstanding processing method for</p>

Data	Explanation
	<p>these synchronization steps. This option takes effect in both directions, meaning also for synchronization to the target system.</p> <p>For more detailed information about synchronizing user data with different systems, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>
Base object	<p>You cannot normally specify a base object for synchronizing with database connectors. In this case, assignment of one base table and the synchronization server is sufficient.</p> <ul style="list-style-type: none"> • Select the table from the Base table menu in which to load the objects. The base table can be used to defined downstream processes for synchronization. For more information about downstream processes, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>. • The Synchronization servers menu displays all Job servers with an enabled One Identity Manager connector server function.
Variable set	<p>If you implement specialized variable sets, ensure that the start up configuration and the base object use the same variable set.</p>

To configure synchronization with the One Identity Manager connector

1. Use the Synchronization Editor to create a new synchronization project.
2. Add mappings. Define property mapping rules and object matching rules.
3. Create synchronization workflows.
4. Create a start up configuration.
5. Define the synchronization scope.
6. Specify the base object of the synchronization.
7. Specify the extent of the synchronization log.
8. Run a consistency check.
9. Activate the synchronization project.
10. Save the new synchronization project in the database.

Detailed information about this topic

- [Creating custom configurations](#) on page 35

Creating custom configurations

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

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

- Run in default mode
- Started from the Launchpad

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

To set up a synchronization project

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

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

2. Select the **One Identity Manager connector** entry and click **Start**.

This starts the Synchronization Editor's project wizard.

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

- If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
- If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.
Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
- Click **Next** to start the system connection wizard to create a connection to a One Identity Manager database.

4. Select the database system to which you want to connect on the **Select database system** page.

- **Direct database connection:** Specifies whether to connect directly to the central database.
- **Application server:** Specifies whether the central database should be connected through an application server.

Set this option if modules other than in the work database are installed in the central database, or if the central database is running with an older version of One Identity Manager.

- **Use application server REST API:** Specifies whether to use the application server's REST API for communicating with the central database.

IMPORTANT: Enable this option if the central database is operated with an older version of One Identity Manager.

5. On the **Connection parameters** page, enter the database credentials for the central database.

- Enter the following data connecting directly to the database:
 - **Server:** Database server.
 - (Optional) **Windows Authentication:** Specifies whether the 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.
 - **User:** The user's SQL Server login name.
 - **Password:** Password for the user's SQL Server login.
 - **Database:** Select the database.
- To connect through an application server, enter the **URL** and **Synchronization user password**.
- To enter additional information about the database connection, click **Advanced options**.
- Click **Test**.

6. Enter the private key for encrypting the database on the **Encryption** page.

7. On the **Additional settings** page, you define additional settings to customize the behavior of the connector.

- **Try to ignore data errors:** Specifies whether objects with erroneous data should be synchronized with the central database.

By default, objects with incorrect data are not synchronized. For example, a user account is not loaded in the One Identity Manager database if, in the user account table, the formatting script of a column contains an email address detects invalid data. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors.

IMPORTANT: If data errors are ignored, performance will be affected. Synchronization can also lead to data loss. Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

NOTE:

- The option cannot be enabled if the REST API of the application server is used.

- This option is only effective if **Continue on error** is set in the synchronization workflow.
 - Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.
8. On the last page of the system connection wizard, you can save the connection data.
 - Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
 - Click **Finish**, to end the system connection wizard and return to the project wizard.
 9. 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.
10. 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.
 11. On the **Select project template** page, select a project template to use for setting up the synchronization configuration.

NOTE: The One Identity Manager connector does not provide a default project template for setting up synchronization. If you have created your own project template, you can select it to configure the synchronization project. Otherwise, select **Create blank project**.

12. Enter the general setting for the synchronization project under **General**.

Table 7: General properties of the synchronization project

Property	Description
Display name	Display name for the synchronization project.
Script language	<p>Language in which the scripts for this synchronization project are written.</p> <p>Scripts are implemented at various points in the synchronization configuration. Specify the script language when you set up an empty project.</p> <p>IMPORTANT: You cannot change the script language once the synchronization project has been saved.</p> <p>If you use a project template, the template's script language is used.</p>
Description	Text field for additional explanation.

13. To close the project wizard, click **Finish**.
14. Save the synchronization project in the database.

Related topics

- [Information required for creating a synchronization project for custom synchronization on page 32](#)
- [Ignoring data error in synchronization on page 48](#)
- [Creating a synchronization project for the system synchronization on page 20](#)

Updating schemas

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

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

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

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

To update a system connection schema

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

To edit a mapping

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

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

Configuring the provisioning of memberships

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

- Memberships are saved as an object property in list form in the target system.
Examples: List of user accounts in the Member property of a group - OR - List of profiles in the MemberOf property of a user account
- 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 **Data Synchronization > Basic configuration data > Target system types** category.
2. In the result list, select the target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.

NOTE:


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

Example: ADSAccountInADSGroup, ADSGroupInADSGroup, and ADSMachineInADSGroup

6. Save the changes.

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

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

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

To restore the original condition

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

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

Example of a condition on the UNSAccountBInUNSGroupB assignment table:

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

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

Configuring single object synchronization

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

Prerequisites

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

Specify the tables that you want to synchronize using single object synchronization and configure single object synchronization for these tables. For more information, see the *One Identity Manager Target System Synchronization Reference Guide*, section *Include custom tables in the synchronization*.

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

1. In the Manager, select the **Data Synchronization > Basic configuration data > Target system types** category.
2. In the result list, select the target system type.

3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the table and enter the **Root object path**.
 - If a concrete base object is defined for the target system, enter the path to the base object in the ObjectWalker notation of the VI.DB.
Example: `FK(UID_GAPCustomer).XObjectKey`
 - If no concrete base object is defined for the target system, enter the XObjectKey of the base table.
Example: `<Key><T>DialogTable</T><P>RMB-T-Org</P></Key>`
8. Save the changes.

Starting synchronization

Synchronization is started using scheduled process plans. A scheduled process plan is added once a start up configuration is assigned to a schedule. Use schedules to define running times for synchronization.

NOTE: Synchronization can only be started if the synchronization project is enabled.

To run synchronization regularly, configure, and activate the a schedule. You can also start synchronization manually if there is no active schedule.

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.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up

configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Analyzing synchronization

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

To display a synchronization log

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

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.

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 allow post-processing of outstanding objects

- Configure target system synchronization.
For more information, see [Configuring target system synchronization](#) on page 44.


Related topics

- [Post-processing outstanding objects](#) on page 46
- [Users and permissions for synchronizing](#) on page 26

Configuring target system synchronization

Create a target system for post-processing outstanding objects. Assign tables you want to be populated by synchronization, to this target system type. Specify the tables for which outstanding objects can be published in the target system during post-processing. Define a process for publishing the objects.

To create a target system type

1. In the Manager, select the **Data Synchronization > Basic configuration data > Target system types** category.
2. Click  in the result list.
3. Edit the target system type main data.
4. Save the changes.

Enter the following data for a target system type.

Table 8: main data for a target system type

Property	Description
Target system type	Target system type description.
Description	Text field for additional explanation.
Display name	Name of the target system type as displayed in One Identity Manager tools.
Cross-boundary inheritance	<p>Specifies how user accounts are assigned to or inherit groups and system entitlements if they belong to different custom target systems.</p> <ul style="list-style-type: none">• If the option is set, groups and system entitlements can be assigned to user accounts that belong to the same target system or to different target systems. The target systems must have the same target system type. <p>For all target systems of a target system type, the settings for the</p>

Property	Description
	<p>User Account Contains Memberships column (UNSRootB.UserContainsGroupList) must be identical.</p> <ul style="list-style-type: none"> If the option is not set, groups and system entitlements can only be assigned to the same target system. <p>NOTE: If the option is not set, the target system type is used to simplify grouping of the target systems.</p>
Show in compliance rule wizard	Specifies whether the target system type for compliance rule wizard can be selected when rule conditions are being set up.
Text snippet	Text snippets used for linking text in the compliance rule wizard.
Alternative connectors	List of connector that can process this type of target system.

To add tables to target system synchronization

- In the Manager, select the **Data Synchronization > Basic configuration data > Target system types** category.
- In the result list, select the target system type.
- Select the **Assign synchronization tables** task.
- In the pane, assign **custom** tables to the outstanding objects you want to handle.
- Save the changes.
- Select the **Configure tables for publishing** task.
- Select the tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
- Save the changes.

NOTE: The 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.

To publish outstanding objects

- For each table for which you want to publish outstanding objects, create a process, which is triggered by the event `HandleOutstanding` and which runs the provisioning of the objects. Use the `AdHocProjection` process task of the `ProjectorComponent` process component.

For more information about defining processes, see the *One Identity Manager Configuration Guide*.

Post-processing outstanding objects

To post-process outstanding objects




1. In the Manager, select the **Data synchronization > Target system synchronization: <target system type>** category.
All tables assigned to the target system type are displayed in the navigation view.
2. Select the table whose outstanding objects you want to edit in the navigation view.
All objects marked as outstanding are shown on the form.

TIP:

To display object properties of an outstanding object

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

Table 9: Methods for handling outstanding objects


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

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

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

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

To disable bulk processing

- Disable the  icon in the form's toolbar.

Related topics

- [Configuring target system synchronization](#) on page 44
- [Users and permissions for synchronizing](#) on page 26

Troubleshooting

For more information about correcting errors during synchronization of object hierarchies, see the *One Identity Manager Target System Synchronization Reference Guide*.

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. For example, a user account is not loaded in the One Identity Manager database if, in the user account table, the formatting script of a column contains an email address detects invalid data. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

The setting does not take effect if the application server's REST API is used to connect to the central database.

To ignoring data errors during synchronization in One Identity Manager

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

This starts the system connection wizard.

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

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

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

5. Save the changes.

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

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

Help for analyzing synchronization issues

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

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

To generate a synchronization analysis report

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

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

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

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

application role 13, 26
 custom synchronization 31
 system synchronization 13
application server 8

B

base object 32, 41

D

direction of synchronization
 system synchronization 16

I

individual configuration 6

J

Job server
 edit 9

M

mapping direction
 system synchronization 16
membership
 modify provisioning 39

O

object
 delete immediately 46

outstanding 43, 46
 publish 46

One Identity Manager connector 5

One Identity Manager version 8

outstanding object 43

P

permission 13
processing method
 system synchronization 16
provisioning
 members list 39

R

remote connection server 18, 32
request method 8
REST API 8

S

schema
 changes 38
 shrink 38
 update 38
single object synchronization 41
synchronization
 deactivate 25
 start 42
synchronization analysis report 49
synchronization configuration 32, 35

- synchronization log 43
 - system synchronization 23
- synchronization server 18, 32
 - configure 9
 - install 9
 - Job server 9
- system synchronization 6
 - calculation schedule 14
 - configure 20
 - connection parameter 20
 - customize 24
 - DBQueue Processor 14
 - direction of synchronization 16
 - GUID module 14
 - mapping direction 16
 - merge mode 14
 - processing method 16
 - provisioning 16
 - provisioning process 14
 - select column 16
 - select table 16
 - set start frequency 16
 - set up 12
 - start 23
 - synchronization project
 - create 20
 - transport 24
 - template 14
 - XDateSubItem 14

T

- target system synchronization
 - table to assign 44
- target system type 44

V

- variable set 32

W

- workflow 32