One Identity Manager 8.1.2

User Guide for the Windows PowerShell Connector

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

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

Patents

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

Trademarks

Legend

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

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

One Identity Manager User Guide for the Windows PowerShell Connector
Updated - January 2020
Version - 8.1.2

Contents

Connecting a target system using the Windows PowerShell connector

You can use the Windows PowerShell connector to connect target systems to One Identity Manager that do not have native support in One Identity Manager. Windows PowerShell cmdlets are used to execute read/write operations in the target system.

The Windows PowerShell connector does not provide a project template for setting up synchronization. You must create synchronization configuration components (mappings, workflows, start up configurations ...) manually after the synchronization project has been saved.

NOTE: You need strong knowledge of Windows PowerShell to set up synchronization with the Windows PowerShell connector.

To set up synchronization with the Windows PowerShell connection

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

Detailed information about this topic

- Setting up the synchronization server on page 10
- Users and permissions for synchronizing on page 4
- Creating a synchronization project on page 13

Users and permissions for synchronizing

In the synchronization process with the Windows PowerShell connector, 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`, `Department`)
3. Mapping custom tables

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

Table 1: Users and permissions groups for non role-based login

User	Tasks
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
System users in the **DPR_EditRights_Methods** permissions group	• Configure and start synchronization in the Synchronization Editor. • Edit the synchronization's target system types as well as outstanding objects in the Manager.

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

User	Tasks
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in

User	Tasks
	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.
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administrate application roles for individual target systems 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 employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Custom target systems** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Can add employees, who have an other identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and defines 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.

Table 3: User and permissions groups for role-based login: Mapped as default tables

User	Tasks
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Custom application role	Users with this application role: • Configure and start synchronization in the Synchronization Editor. • Edit the synchronization's target system types as well as outstanding objects in the Manager. This application role gets its write access through a custom permissions group and the **vi_4_SYNCPROJECT_ADMIN** permissions group.

Table 4: Users and permissions groups for role-based login: Mapped in custom tables

User	Tasks
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Application roles for custom tasks	Administrators must be assigned to the **Custom | Administrators** application role.

User	Tasks
	Users with this application role: • Administrate custom application roles. • Set up other application roles for managers if required.
Manager for custom tasks	Managers must be assigned to the **Custom | Managers** application role or a child role. Users with this application role: • 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. You can use these application roles, for example, to guarantee One Identity Manager users write permissions on custom tables or columns. All application roles that you define here must obtain their write permissions through custom permissions groups. This application role gets its write access through a custom permissions group and the **vi_4_SYNCPROJECT_ADMIN** permissions group.

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 a custom application role for synchronization on page 8

Setting up a custom application role for synchronization

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 synchronization.
   - 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.

   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.

   The default permissions group must be assigned as a subgroup. 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 new 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, which are populated though 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.

   The permissions group for custom tables must be assigned as 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.

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

Setting up the synchronization server

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

- Windows operating system

  The following versions are supported:

  - Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 or later

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Installer
- Windows Management Framework 4.0 or Windows PowerShell Version 3.0 or later
- Target system-specific Windows PowerShell modules or snap-ins
- One Identity Manager Service
  - 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** machine role.

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

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

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

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

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

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. In the default case, 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 executes 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 program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the **Database connection** page.
3. Specify the server on which you want to install One Identity Manager Service on the **Server properties** page.
   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 exactly this 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. On the **Server functions** page, select **Windows PowerShell 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 already. 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, for example, user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files.
10. On the **Select private key file** page, select the file with the private key.

    > NOTE: This page is only displayed when the database is encrypted.

11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Name or IP address of the server that the service is installed and started on.
    - **Service account**: User account data for the One Identity Manager Service.
        - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.
        - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.
    - **Installation account**: Data for the administrative user account to install the service.
        - To use the current user's account, set the **Current user** option.
        - To user 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

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.

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

Table 5: Information required for setting up a synchronization project

Data	Explanation
Definition file	You provide the required Windows PowerShell cmdlets, schema types, schema properties and connection parameters in an XML file.
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.

Data	Explanation
	Installed components: • One Identity Manager Service (started) The synchronization server must be declared as a Job server in One Identity Manager. The Job server name is required. For more information, see Setting up the synchronization server on page 10.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well. For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.
Synchronization workflow	Set the option **Data import** in the synchronization step if synchronization data is imported from a secondary system. You cannot select the processing method "MarkAsOutstanding" for these synchronization steps. For more detailed information about synchronizing user data with different systems, see the One Identity Manager Target System Synchronization Reference Guide.
Base object	If no base object can be specified, you can assign a base table and the synchronization server.

Data	Explanation
	• Select the **Base table** from the menu in which to import the objects. The base table can be used to defined downstream processes for synchronization. For more information about downstream processes, see the One Identity Manager Target System Synchronization Reference Guide. • The **Synchronization server** menu displays all Job servers for which the "Windows PowerShell Connector" server function is enabled.
Variable set	If you implement specialized variable sets, ensure that the start up configuration and the base object use the same variable set.

To configure synchronization with the Windows PowerShell connector

1. Create a definition file, which described the structure of the target system and the Windows PowerShell cmdlets to use.
2. Create a new synchronization project.
3. Add mappings. Define property mapping rules and object matching rules.
4. Create synchronization workflows.
5. Create a start up configuration.
6. Define the synchronization scope.
7. Specify the base object of the synchronization.
8. Specify the extent of the synchronization log.
9. Run a consistency check.
10. Activate the synchronization project.
11. Save the new synchronization project in the database.

For more detailed information about create the various components of the synchronization configuration (for example, mappings, workflows, or start-up configuration), see the One Identity Manager Target System Synchronization Reference Guide.

Detailed information about this topic

- Creating definition files on page 15
- How to set up a synchronization project on page 16

Creating definition files

When you set up synchronization, you enter the required Windows PowerShell cmdlets, schema types, schema properties and the information required for logging in to the target system in XML notation. Create one XML file for this, which contains the entire definition. The definition file is loaded when you configure synchronization in the project wizard. You can create Synchronization Editor maps and synchronization workflows based on this definition.

You can find an example of a definition file on the One Identity Manager installation medium in `..\Modules\TSB\dvd\AddOn\SDK\ADSample.xml`.

How to set up a synchronization project

There is an wizard to assist you with setting up a synchronization project. This wizard takes you 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 you configure a synchronization project if Synchronization Editor is both:
>
> - Executed in default mode
> - Started from the launchpad
>
> If you execute the project wizard in expert mode or directly from 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 on 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 **Windows PowerShell Connector**. Click **Run**.

   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 Synchronization Editor, you do not need to make any settings.
   - If access is not possible from the workstation on which you started 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 for connecting with the Windows PowerShell.

4. Click **Next** on the start page of system connection wizard.
5. On the **Connector Definition** page, you enter the required Windows PowerShell cmdlets, schema types, schema properties, and the information required for logging

in to the target system in XML notation.

Table 6: Connector definition

Property	Description
System ID/Name	Unique name of the system connection.
Concurrent connections	Maximum number of simultaneous connections to the target system.
Definition	Definition that converts the target system schema into Cmdlet calls. Enter the definition in XML notation. a. To load the definition from a definition file, click . b. To check the consistency of the definition, click .

6. Enter the data for the required connection parameter on the **Connection data** page. All the parameters from the `ConnectionParameters` element of the XML definition are queried.
7. You can save the connection data on the last page of the system connection wizard.
   - 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.
8. 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.
9. 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.
10. Select a project template on the **Select project template** page to use for setting up the synchronization configuration.

    HINWEIS:The Windows PowerShell 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**.

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

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

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 loading 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 compressing 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.

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 executing times for synchronization.

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

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

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

- If another synchronization is started with the same start up configuration, this process is stop and is assigned the **Frozen** execution 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.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error 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 executed 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 of execution. For detailed information about start up configurations, 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. 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.

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 synchronization.
- 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 21.

Related topics

- How to post-process outstanding objects on page 23
- Users and permissions for synchronizing on page 4

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 master data.
4. Save the changes.

Enter the following data for a target system type.

Table 8: Master data for a target system type

Property	Description
Target system type	Target system type description.

Property	Description
Description	Spare field for additional explanation.
Display name	Name of the target system type as displayed in One Identity Manager tools.
Cross-boundary inheritance	Specifies whether user accounts can be assigned to groups if they belong to different custom target systems. NOTE: If this option is not set, the target system type is used to group the target systems.
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.

To add tables to the target system synchronization

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 custom-defined target system.
3. Select the **Assign synchronization tables** task.
4. Assign **custom** tables whose outstanding objects you want to handle in .
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select tables whose outstanding objects can be published in the target system and set the **Publishable** option.
8. 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 no 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 executes the provisioning of the objects. Use the `AdHocProjection` process function of the `ProjectorComponent` process component. For detailed information about defining processes, see the *One Identity Manager Configuration Guide*.

How to post-process outstanding objects

To post-process outstanding objects

1. In the Manager, select **Data synchronization | Target system synchronization: <target system type>**.

   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***
   >
   > a. Select the object on the target system synchronization form.
   >
   > b. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.
4. Click one of the following icons in the form toolbar to execute the respective method.

Table 9: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted in the One Identity Manager database. Deferred deletion is not taken into account. The **Outstanding** label is removed for the object. Indirect memberships cannot be deleted.
	Publish	The object is added in the target system. The **Outstanding** label is removed for the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • 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 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

- Deactivate in the form toolbar.

Related topics

- Configuring target system synchronization on page 21
- Users and permissions for synchronizing on page 4

Configuring the provisioning of memberships

Memberships, for example, 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 will probably 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 `Members` property of an Active Directory `group`).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; 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. Select the **Configure tables for publishing** task.
3. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - This option can only be enabled for assignment tables that have a base table with `XDateSubItem` or `CCC_XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in

the mapping must be marked identically (for example, `ADSAccountInADSGroup`, `ADSGroupInADSGroup` and `ADSMachineInADSGroup`).

4. Click **Enable merging**.
5. 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 the members list does not get entirely overwritten.

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 single provisioning has been disabled for a table, the condition is deleted. Table 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*.

Error handling

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

Help for the analysis of synchronization issues

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

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

V

W