One Identity Manager 9.2

# Administration Guide for Azure Cloud Access Governance

CIM Module Administration Guide for Azure Cloud Access Governance
Updated - 07 September 2023, 10:29
Version - 9.2

# Contents

# Managing Azure Cloud System

One Identity Manager CIM module for Azure Cloud System module provides the ability to connect to Azure Tenant and synchronize Azure objects to One Identity Manager and provision Role Assignments for Security Principals. Identity and Access Governance processes such as attesting, IT Shop, or report subscriptions can be used for Azure Tenant. The integration ensures a strong governance.

## Architecture overview

To access Azure Tenant data, the SCIM connector is installed on a synchronization server. The synchronization server ensures that the data is compared between the One Identity Manager database and Azure tenant. The SCIM connector uses the Starling Connect Azure Infrastructure Connector to synchronize the Azure objects to One Identity Manager. The Starling Connect Connector uses the Microsoft Azure REST API and accesses the Azure objects.

## One Identity Manager users for managing Azure Cloud System

The following users are used in Azure Tenant administration.

**Table 1: Users used in Azure Tenant system administration**

| Users | Task |
|---|---|
| Target system administrators | Target system administrators must be assigned to the **Target systems \| Administrators** application role.<br>Users with this application role<br>• Administrative application roles for individual target systems types |

| | |
|---|---|
| | • Specify the target system manager<br>• Set up other application roles for target system managers if required<br>• Specify which application roles are conflicting for target system managers<br>• Authorize other identity to be target system administrators<br>• Do not assume any administrative tasks within the target system |
| Target system managers | Target system managers must be assigned to **Target systems \| Azure Cloud Access Governance** or a sub-application role.<br>Users with this application role<br>• Assume administrative tasks for the target system<br>• View target system objects<br>• Configure synchronization in the **Synchronization Editor** and define the mapping for comparing target systems and One Identity Manager<br>• Edit the synchronization's target system types and outstanding objects<br>• Authorize other identities within their area of responsibility as target system managers and create child application roles if required |
| One Identity Manager administrators | • Create customized permissions groups for application roles for role-based login to administration tools in **Designer** as required<br>• Create system users and permissions groups for nonrole-based login to administration tools in **Designer** as required<br>• Enable or disable additional configuration parameters in **Designer** as required<br>• Create custom processes in **Designer** as required<br>• Create and configures schedules as required |
| Administrators for the IT Shop | Administrators must be assigned to the **Request & Fulfillment \| IT Shop \| Administrators** application role.<br>Users with this application role<br>• Assign to IT Shop structures |
| Product owner for the IT Shop | Product owners must be assigned to the **Request & Fulfillment \| IT Shop \| Product owner** application role or a child application role.<br>Users with this application role |

| | |
|---|---|
| | • Approve through requests<br>• Edit service items and service categories under their management |
| Administrators for Organizations | Administrators must be assigned to the application role **Identity Management \| Organizations \| Administrators**.<br>Users with this application role<br>• Assign to departments, cost centers and locations |
| Business roles administrators | Administrators must be assigned to the application role **Identity Management \| Business roles \| Administrators**.<br>Users with this application role<br>• Assign to business roles |

# Setting up synchronization with Azure Cloud System

The following steps must be performed before setting up the Azure cloud system:

- Azure Active Directory Tenant Synchronization project configured, and the data synchronized into OneIM (AAD Admin Guide)
- Azure Infrastructure Connector configured on Starling (refer Starling Connect Administration Guide)

## Setting up the synchronization server

To set up synchronization with Azure Infrastructure, a server has to be available that has the following software installed on it:

- Windows operating system

  **Versions supported**

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Microsoft .NET Framework Version 4.8 or later

    NOTE: Take the target system manufacturer's recommendations into account.
- Windows Installer
- One Identity Manager Service, Synchronization Editor, SCIM connector
- Install **One Identity Manager** components with the installation wizard.

1. Select **Select installation modules with existing database**.
2. Select the machine role **Server | Job server | SCIM**.

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

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

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of **One Identity Manager Service** components corresponding to the machine roles.
- Configuration of **One Identity Manager Service**.
- Starts the **One Identity Manager Service**.

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.

For remote installation of **One Identity Manager Service**, you require 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 install and configure One Identity Manager Service remotely 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.

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

   - OR -

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

   Enter the following data for the Job server.

**Table 2: Job Server Properties**

| Property | Description |
|---|---|
| Server | Job server name. |
| 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.<br>Example: `<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 **Designer**.

4. Select **SCIM** on the **Machine roles** page.
5. Select **SCIM** connector on the **Server functions** page.
6. Check the **One Identity Manager Service** configuration on the **Service settings** page.

   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 more information about configuring the service, see the *One Identity Manager Configuration Guide*.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on Select installation source.
10. Select the file with the private key on the page Select private key file.

    NOTE: This page is only displayed when the database is encrypted.
11. Enter the service's installation data on the Service access page.

**Table 3: Installation Data**

| Data | Description |
|---|---|
| Computer | Server on which to install and start the service from.<br>***To select a server***<br>Enter a name for the server.<br>- OR -<br>Select an entry from the list. |
| Service Account | User account data for the **One Identity Manager Service**.<br>***To enter a user account for the One Identity Manager Service***<br>Set the option Local system account. This starts the **One Identity Manager Service** under the **NT** |

| | |
|---|---|
| | **AUTHORITY\SYSTEM** account.<br>- OR -<br>Enter user account, password and password confirmation. |
| Installation account | Data for the administrative user account to install the service.<br>***To enter an administrative user account for installation***<br>1. Enable Advanced.<br>2. Enable Current user.<br>This uses the user account of the current user.<br>- OR -<br>1. Enter user account, password and password confirmation. |

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 **Server Installer**.

    NOTE: The service is entered with the name **One Identity Manager Service** in the server service management.

# Creating a synchronization project for initial synchronization of Azure Cloud System

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

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

The following information is required for setting up a synchronization project.

NOTE: Be aware of case sensitive parts of the URL during configuration.

**Table 4: Information Required for Setting up a Synchronization Project**

| Data | Explanation |
|---|---|
| Servers DNS name / URL | DNS name of the server that provides the SCIM interface or URL for connecting to the server. |
| Port | Port for accessing the cloud application. |
| URI service | URL for reaching the SCIM service. |
| Authentication endpoint or URL | URL available for authenticating. If authentication of another server or another root URL is used for authentication, the full URL must be entered here. |
| User account and password | User name and password for logging into the cloud application with the authentication types "Basic authentication", "OAuth authentication" and "Negotiated authentication". |
| Client secret | Security token for logging into the cloud application with the authentication type "OAuth authentication". |
| Application/Client ID | The application/client ID used to register the cloud application with the security token service. It is required for registering with the authentication type "OAuth-Authentication". |
| SCIM endpoint | Endpoint URIs or URLs for accessing the cloud application's schema, resource and service provider data. |
| 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.<br>The One Identity Manager Service with the SCIM connector must be installed on the synchronization server.<br>The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.<br>**Table 5: Additional properties for the Job server**<br>Property: Value<br>Server function: SCIM connector<br>Machine role: Server/Job server/SCIM<br>For more information, see Setting up a synchronization server. |
| One Identity Manager database connection data | Database server<br>• Database<br>• SQL Server Login and password |

| | |
|---|---|
| | Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication. |
| 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 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 to the workstation is not possible, you can set up a remote connection. The remote connection server and the workstation must be in the same **Active Directory** domain.<br><br>**Remote connection server configuration**<br>• One Identity Manager Service is started<br>• RemoteConnectPlugin is installed<br>• SCIM connector is installed<br><br>The remote connection server must be declared as a Job server in **One Identity Manager**. The Job server name is required.<br><br>NOTE: 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 information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide.* |

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

- Run in default mode, and
- Started from the launchpad

If you run 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 initial synchronization project for Azure Cloud System*

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

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

2. Select **Target system type SCIM interface** 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 **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**.

4. On the **Configuration data** page, enter the connection parameters required by the SCIM connector to login to the cloud application.

**Table 6: Server parameter**

| Property | Description |
|---|---|
| Servers DNS name / URL | DNS name of the server that provides the SCIM interface or URL for connecting to the server. |
| URI service | URL for reaching the SCIM service. Only the part of the URL used in common by all endpoints to be called, is required.<br>The SCIM connector take the URL from the server URL, the port and URI together.<br>For example, if the full URL is "https://identities.example.net:8080/scim/v2", then enter "scim/v2" as the URI. |

**Table 7: Authentication type**

| Property | Description |
|---|---|
| OAuth Authentication | Authentication using the OAuth protocol 2.0. |

5. On the OAuth authentication page, enter the security token for the authentication type "OAuth authentication" and select the access type.

**Table 8: Features of OAuth Authentication**

| Property | Description |
|---|---|
| Client secret | Security token for logging into the cloud application.<br>If the client secret is not known, enter the user name and password. |

**Table 8: Features of OAuth Authentication**

| | |
|---|---|
| Application/Client ID | The application/client ID used to register the cloud application with the security token service. |
| Grant type | Enable **Client credentials** |

6. You can test the connection on **Verify connection settings**. Click **Test.**
One Identity Manager tries to connect to the Starling connect Azure infrastructure Connector.

   TIP: The One Identity Manager saves the test result. When you reopen the page and the connection data has not changed, the result of the test is displayed. You do not have to run the connection test again if it was successful.

7. On the **Endpoint configuration** page, enter the URIs for the SCIM end points. The SCIM default is used there is no URI.

   **Table 9: End point configuration**

| Property | Description |
|---|---|
| Schema | End point for accessing the schema information for the cloud application. |
| Resources | End point for accessing resource information for the cloud application, for example groups or user accounts. |
| Supported service options | End point for accessing the service provider information for the cloud application. |

   To test the connection at the specified end points, click **Test**.

   TIP:The One Identity Manager saves the test result. If you reopen the page and the end point configuration has not changed, the save test result is displayed.

8. On the **Target product selection** page, you can select One Identity Starling Connect.
   - Set the **Save connection data on local computer** 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. Re-enter 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. Select the project template "**Azure Infrastructure Synchronization**" on the **Select project template** page to use for setting up the synchronization configuration.
12. On the **Restrict target system access** page, you can specify how system access should work by selecting one of the following options:

**Table 10: Specify target system access**

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

13. Select the synchronization server to run synchronization on the **Synchronization** server page.

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

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

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

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

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

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

    The synchronization project is created, saved and enabled immediately.

    NOTE:

    - If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the **Synchronization Editor**.
    - The connection data for the target system is saved in a variable set and can be modified under **Configuration | Variables** in **Synchronization Editor**.
    - **DO NOT** modify the variables in Synchronization Editor

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

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

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

***To synchronize on a regular basis***

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

***To start initial synchronization manually***

1. Open the synchronization project in the **Synchronization Editor.**
2. Select the category **Configuration | Start up configurations**.

3. Select a start up configuration in the document view and click **Execute**.
4. Confirm the security prompt with **Yes**.

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

### Related Topics

- Setting up the synchronization server
- Displaying synchronization results
- Customizing synchronization configuration
- Speeding up synchronization with revision filtering
- Appendix: Default project template for cloud applications

# Display Synchronization Results

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

***To display a synchronization log***

1. Open the synchronization project in the **Synchronization Editor**.
2. Select **Logs**.
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 on it.

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

   To modify the retention period for synchronization logs

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

# Customizing synchronization configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization with Azure Cloud System. You can use this synchronization project to load

Azure Infrastructure objects into the One Identity Manager cloud database.

You must customize the synchronization configuration in order to compare the database with the Azure Cloud System regularly and to synchronize changes.

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 stopped and is assigned the **Frozen** execution status. An error message is written to the **One Identity Manager Service** log file.
- 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.

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

# 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 category **Configuration | Target systems**.

   - OR -

   Select the category **Configuration | One Identity Manager connection**.
3. Select the view **General** 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 category **Mappings**.
3. Select a mapping in the navigation view.

   The **Mapping Editor** is displayed.

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.

# 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 post-process outstanding objects***

1. In **One Identity Manager**, select the **Azure Cloud Access Governance | Target system synchronization: Azure Cloud Access Governance** category.

   All tables assigned to the target system type CIM as synchronization tables are displayed in the navigation view.

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

   - The synchronization log has already been deleted.

   - OR -

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

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

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

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

   NOTE:

   ***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.

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

NOTE: Publish operation is not supported.

**Table 11: 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<br>• The table containing the object can be published.<br>• The target system connector has write access to the target system. |
|  | Reset | The **Outstanding label** is removed for the object. |

4.

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.

  You must customize synchronization to synchronize custom tables.

### *Speeding up synchronization with revision filtering*

When you start synchronization, all synchronization objects are loaded. Some of these objects have not been modified since the last synchronization and, therefore, must not be processed. Synchronization is accelerated by only loading those object pairs that have changed since the last synchronization. One Identity Manager uses revision filtering to accelerate synchronization.

SCIM supports revision filtering for schemas AzRoles, AzRoleAssignment, AzGroupRoleAssignment, AzUserRoleAssignment and AzSPRoleAssigbment. The Azure Cloud system object's date of last change is used as revision counter. Each synchronization saves its last execution date as a revision in the One Identity Manager database (table `DPRRevisionStore`, column Value). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is

synchronized the next time, the Azure cloud system object's change date is compared with the One Identity Manager revision saved in the database. Only those objects that have been changed since this date are loaded from the Azure Cloud System.

The revision is found at start of synchronization. Objects changed after this point are included with the next synchronization.

Revision filtering can be applied to workflows and start up configuration.

***To permit revision filtering on a workflow***

1. Open the synchronization project in the Synchronization Editor.
2. Edit the workflow properties. Select the entry Use revision filter from Revision filtering.

***To permit revision filtering for a start up configuration***

1. Open the synchronization project in the Synchronization Editor.
2. Edit the start up configuration properties. Select the entry Use revision filter from Revision filtering.

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

# Help for the analysis of synchronization issues

You can generate a report for analysing 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 synchronization buffer
- 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 menu **Help | Generate synchronization analysis** report and answer the security prompt with **Yes**.

   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.

# Deactivating synchronization

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

***To prevent regular synchronization***

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

   Now you can only start synchronization manually.

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

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

***To deactivate the synchronization project***

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

**Related Topics**

- Creating a synchronization project for initial synchronization of Azure Cloud System

# 3

# Basic Data for managing Azure Cloud System

To manage an Azure cloud system environment in One Identity Manager, the following basic data is relevant.

## Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign the identities who are authorized to read all Azure related objects and the Active directory User, Group and Service Principal objects for the Azure Active Directory tenants in One Identity Manager to this application role. Define additional application roles if you want to limit the edit or view permissions for target system managers to individual tenants. The application roles must be added under the default application role.

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

**Implementing application roles for target system managers**

- The One Identity Manager administrator assigns identities to be target system managers.
- These target system managers add identities to the default application role for target system managers. Target system managers with the default application role are authorized to edit all tenants in One Identity Manager.
- Target system managers can authorize other identities within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual connections.

Default Application Roles for Target System Managers

**Table 12: Default Application Roles for Target System Managers**

| Users | Tasks |
|---|---|
| Target system managers | Target system managers must be assigned to Target systems \| Azure Cloud Access Governance or a sub-application role. Users with this application role: |

Assume administrative tasks for the target system.

- Read objects like user accounts, groups, service principals, Management groups, subscriptions, resource groups, resource, roles and role assignments.
- 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 identities within their area of responsibility as target system managers and create child application roles if required.

***To initially specify identities to be target system administrators***

1. Log in to One Identity Manager as Manager administrator (Base role | Administrators).
2. Select One Identity Manager Administration | Target systems | Administrators.
3. Select Assign identities.

***To add the first identities to the default application as target system managers***

1. Log into One Identity Manager as Target System Administrator (Target systems | Administrators).
2. Select One Identity Manager Administration | Target systems | Azure Cloud Access Governance.
3. Select Assign identities in the Task view.
4. Assign the identities you want and save the changes.

***To authorize other identities as target system managers when you are a target system manager***

1. Log into One Identity Manager as target system manager.
2. Select the application role in Azure Cloud Access Governance | Basic configuration data | Target system managers.
3. Select Assign identities.
4. Assign the identities you want and save the changes.

***To specify target system managers for individual clients***

1. Log into One Identity Manager as target system manager.
2. Select Azure Cloud Access Governance | Tenants.
3. Select the client from the result list.
4. Select Change master data.

5. On the General tab, select the application role in the Azure Cloud System manager field.

   NOTE: In case the Azure Cloud Target System Manager field is not present, install the AAD.Forms.vif refer to KB article (CIM Enhancement for AAD Module).

6. Next to the Target system manager menu, click to create a new application role.
   a. Enter the application role name and assign the Target systems | Azure Cloud Access Governance parent application role.
   b. Click OK to add the new application role.
7. Save the changes.
8. Assign identities to this application role who are permitted to edit the client in One Identity Manager.

# Azure Active Directory Tenant

You must provide details about your organization the first time you register for a Microsoft cloud service. This detailed information is used to make a new Azure Active Directory partition. The organization represents one Azure Active Directory tenant. In One Identity Manager, you can edit the main data of each Azure Active Directory tenant.

However, you cannot create new Azure Active Directory tenants in One Identity Manager.

## General Master Data for Microsoft Azure Connection

***To edit CIM Target system manager for Azure Active Directory tenant data***

1. In the Manager, select the Azure Active Directory > Tenants category.
2. In the result list, select the Azure Active Directory tenant.
3. Select the Change main data task.
4. Edit the Azure Cloud Target System Manager field for Azure Active Directory tenant.
5. Save the changes.

**Detailed information about this topic**

More details can be found in *Azure Active Directory Synchronization Admin Guide*

# Managing Azure Cloud System Objects

The following are the Azure objects that are synchronized from the target azure tenant.

## Azure Scope Objects

### Root Scope(/)

RootScope is the top most level scope above the management group. If the user's access is elevated, the user is assigned the User Access Administrator role in Azure at root scope (/). All role assignments defined at the rootscope will be inherited at all levels below. Role assignments at the rootscope can be defined using Azure PowerShell, Azure CLI, or the REST API.

### Management Group

Management Groups provide a scope above Subscriptions. All Subscriptions within a Management Group inherit conditions applied at the management group. Governance policies can be applied to Management Group so that Subscriptions inherit it. By default, all Azure Tenants automatically have a Root Management Group created.

Each directory is given a single top-level management group called the root management group. The root management group is built into the hierarchy to have all management groups and subscriptions fold up to it.

Azure management groups support Azure role-based access control for all resource accesses and role definitions. These permissions are inherited to child resources that exist in the hierarchy.

# Subscription

Azure Subscriptions are the container that hosts all Azure Resources. It is the Resource access and billing boundary

# Resource Groups

Azure Resource Group is a container that holds the related resources needed for a particular solution. Resource Groups are created under an Azure Subscription.

The resource group stores metadata about the resources. Therefore, when you specify a location for the resource group, you are specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

# Resources

Azure Resource is the entity such as virtual machine that is managed by Azure.

These are the building blocks of an Azure IT environment. The resources are organized into Resource Groups inside of an Azure subscription. There are billable and non-billable resources. Billable resources have a Meter attached to them that runs while the resource is provisioned.

# Roles

Azure Roles is a collection of permissions and defines the following:

- List of Actions that can be performed the Resource
- List of Actions that are excluded from the allowed list of Actions
- List of Actions that can be performed on the underlying data
- List of Actions that are excluded from the allowed list of data actions

Role definitions are created at a particular scope (Management Group / Subscriptions / Resource Group) and can be assigned to AAD Users / AAD Service Principal / AAD Managed Identities at the scope at which Role was created or at a child scope level. Example: The Built in Owner role was created at the Root Management Scope level. This role can be assigned to an AADUser at the Management scope level or at a child scope level such as Subscription or Resource.

## Built in Roles

Built in Roles are created by Azure at Root Management Group Scope and cannot be modified.

## Custom Roles

Custom Roles can be created and assigned multiple scopes at Management Group / Subscriptions / Resource Group level.

# Locations / Regions

Azure Regions contain the Azure Data Centers. When a Resource Group / Resource is created we select the Azure Region where the resource is created, and its data resides

# Resource Types

Azure Resource Provider is a service that supplies resources. Example Microsoft.Compute. Resource Types are resources available through the Resource Provider. Example VMs. Each Resource Type is available for deployment on certain regions. The API lists the regions on which a particular Resource Type is available for deployment.

# Role Assignments

Built in Roles and Custom Roles can be assigned to AAD User, AAD Service Principal, AAD Group and Managed Identities at various scopes. The roles are also inherited based on scope hierarchy.

# Role Assignment to Security Principals

Role assignment to Security Principals helps you to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals at a particular scope.

You can assign and remove roles from a security principal in One Identity Manager, which can be provided to target system by provisioning.

To add role assignment to a user, group, service principal or managed identity, you can assign the role directly or it can be added indirectly through the IT Shop.

## Assigning Azure Roles directly to the AAD Security Principal

Azure Role can be assigned to the AAD security principal directly.

## To assign Azure Role directly to the AAD User

1. In One Identity Manager, navigate to Azure Active Directory.
2. Select the User account to which the Azure role must be assigned.
3. Select Assign Azure Role Scope Mapping from Tasks.
4. To add the Role, select the role scope mapping from the Add assignments list.
5. Save the changes.

# To assign Azure Role directly to the AAD Group

1. In One Identity Manager, navigate to Azure Active Directory.
2. Select the Group to which the Azure role must be assigned.
3. Select Assign Azure Role Scope Mapping from Tasks.
4. To add the Role, select the role scope mapping from the Add Assignments list.
5. Save the changes.

# To assign Azure Role directly to the AAD Service Principal

1. In One Identity Manager, navigate to Azure Active Directory.
2. Select the Service Principal to which the Azure role must be assigned.
3. Select Assign Azure Role Scope Mapping from Tasks.
4. To add the Role, select the role scope mapping from the Add Assignments list.
5. Select the Role Scope mapping from the dropdown list.
6. Save the changes.

# To add new Role Scope Mapping

A new Role Scope Mapping for Role Assignment can also be created from Tenant node from Azure Cloud Access Governance in One Identity Manager.

1. In One Identity Manager, navigate to Azure Cloud Access Governance.
2. To view/add Role Scope Mapping for specific tenant, Click on Tenants
3. Extend the node of Tenant where you want to add the Role Scope Mapping
4. Select Role Scope Mapping
5. To add new Role Scope mapping click on '+' button.
6. Click on Add new dynamic key button →
7. Select Scope from Table and item from scope as per requirement.
8. Click on Ok.
9. Save the changes.
10. To view/add for All Tenants, after clicking on Node 'Tenants' follow the same procedure from Step 4

# Assigning Azure Roles to the AAD Security Principal through ITShop

Azure Role can be assigned to the AAD Security Principal through ITShop. Identity with Azure Active Directory account can raise request for Role Assignment for his own user account, any AAD Group and any AAD Service Principal belonging to the tenant.

Once the request is raised, the owner of the scope object for which role assignment request is created (scope here refers to management group, subscription, resource group or resource) approves the request.

The way approval works is that if the owner of the scope object is not found, then request for approval is sent to the owner of the parent scope object and so on in the hierarchy and if none of the scope object owners are configured, the request for approval goes to the Target System Manager.

The hierarchy for approval workflow is:

Resource Scope Owner -> Resource Group Scope Owner -> Subscription Scope Owner -> Management Group Scope Owner -> Parent Management Group Scope Owner -> Tenant Root Scope Owner -> Target System Manager.

# To assign Azure Role to the AAD Security Principal through ITShop

1. Login in to ITShop portal
2. Add new request
3. Request Product from ITShop to Add to cart:
    a. Azure Infrastructure Azure AD Group Role Assignment, Azure Infrastructure Azure AD Service Principal Role Assignment, Azure Infrastructure Azure AD User Role Assignment.
4. Enter required values:
    a. AAD Organization Name, AAD Group/Service Principal/User Name, Azure Scope, Azure Roles
5. Click Submit.
6. Once approved by approver, the role assignment will be done.

# Remove Azure Roles directly from AAD Security Principal

Azure Role Assignments can be removed for an AAD User, AAD Group or AAD Service Principal. Using One Identity Managers role assignments done at Root Scope can also be removed.

## To remove Azure Role from the AAD User

1. In One Identity Manager, navigate to Azure Active Directory.
2. Select the User account from which the Azure role must be assigned.
3. Select Assign Azure Role Scope Mapping from Tasks.
4. To remove the Role Assignment, select the role scope mapping from the Remove Assignments list.
5. Save the changes.

## To remove Azure Role from the AAD Group

1. In One Identity Manager, navigate to Azure Active Directory.
2. Select the Group from which the Azure role must be removed.
3. Select Assign Azure Role Scope Mapping from Tasks.
4. To remove the Role Assignment, select Azure Role Assignment to be removed from the list.
5. Save the changes.

## To remove Azure Role from AAD Service Principal

1. In One Identity Manager, navigate to Azure Active Directory.
2. Select the Service Principal from which the Azure role must be removed.
3. Select Assign Azure Role Scope Mapping from Tasks.
4. To remove the Role Assignment, select Azure Role Assignment to be removed from the list.
5. Save the changes.

# Remove Azure Roles from AAD Security Principal through IT Shop

***To remove Azure Role for an AAD Security Principal through ITShop***

1. Login to the ITShop portal as the user who raised the ITShop request
2. Go to request history
3. Click on Details
4. Click on Unsubscribe Product
5. Add comment and Save

# Default project template for Microsoft Azure

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

Use a default project template for setting up the synchronization project initially. For custom implementations, you can extend the synchronization project with the Synchronization Editor. The various One Identity Manager tables that is used for mapping. One Identity Manager schema tables for Microsoft Azure

| Table in the One Identity Manager Schema | Description |
|---|---|
| AzLocations | Azure Locations details |
| AzManagementGroups | Azure Management Groups details |
| AzResource | Azure Resources details |
| AzResourceGroups | Azure Resource Groups details |
| AzResourceTypes | Azure Resource types details |
| AzRoles | Azure Roles details |
| AzSubscriptions | Azure Subscription details |
| AzRoleAssignment | Azure Role Assignment to Scope details |
| AzGroupRoleAssignment | Azure Roles Assigned to a Group |
| AzSPRoleAssignment | Azure Roles Assigned to a Service Principal |
| AzUserRoleAssignment | Azure Roles Assigned to a User |
| AzRoleScopeMap | Azure Role’s scope definition |

# 8

# Reports about Azure cloud system objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. You can generate the following reports for Microsoft Azure objects.

**Table 13: Reports about Microsoft Azure objects**

| Report | Published for | Description |
|---|---|---|
| CIM Azure RoleAssignments Overview By AADGroup | AAD Group | Get all Role Assignments for AADGroups including Role Assignments inherited through AAD Group Memberships |
| CIM Azure RoleAssignments Overview By AADServicePrincipal | AAD ServicePrincipal | Get all Role Assignments for AADServicePrincipals |
| CIM Azure RoleAssignments Overview By AADUser | AAD User | Get all Role Assignments for AADUsers including Role Assignments inherited through AAD Group Memberships |
| CIM Azure RoleAssignments Overview By AADUser AADGroup AADSP | AAD Organization | Get all Role Assignments for AADUsers, AADGroups and AADServicePrincipals. AADUser and AADGroup Role Assignments include Role Assignments inherited through AAD Group Memberships |
| CIM Azure RoleAssignments Overview By ManagementGroup | Azure Management Group | Report that provides an overview of direct Role assignments for Azure Management Groups as well as inherited role assignments. |
| CIM Azure RoleAssign-ments Overview By Resource | Azure Resource | Report that provides an overview of direct Role assignments for Azure Resource as well as inherited role assignments. |

| | | |
|---|---|---|
| CIM Azure RoleAssignments Overview By ResourceGroup | Azure Resource Group | Report that provides an overview of direct Role Assignments for Azure Resource Groups as well as inherited role assignments. |
| CIM Azure Role Assignment Overview By Subscription | Azure Subscription | Report that provides an overview of direct Role Assignments for Azure Subscription Groups as well as inherited role assignments. |

# Appendix 9

# Troubleshooting

Troubleshooting issues related to CIM module include:

- Synchronization issues - Check synchronization logs for inconsistencies after the synchronization is complete. For more details about the log, you can view the jobs server logs, which is assigned to handle CIM module synchronizations.
- Provisioning / Synchronization has Forbidden Errors in logs - Check to make sure the Azure AD Service Principal configured in Starling Connect has owner permissions at Root Scope level.
- Issues related to throttling (HTTP 429 Too Many Requests) - There are throttling limits setup for Azure objects. The connector automatically detects throttling and handles it. If there is still a throttling issue and you receive an error "HTTP 429 Too Many Requests", this is because the requests have reached a particular limit and Azure is unable to process further requests. If it happens, please connect with to Microsoft to increase the throttling limit.

# Recommendations for Synchronization project creation

- Revision filter in synchronization project should be enabled only for Role Assignment Tables - Roles, RoleAssignment, GroupRoleAssignment, SPRoleAssignment and UserRoleAssignment
- For projection to happen write permissions on synchronization project should be enabled only for Role Assignment Tables - Roles, RoleAssignment, GroupRoleAssignment, SPRoleAssignment and UserRoleAssignment.

# 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