ONE IDENTITY

by Quest

One Identity Manager 9.2

Administration Guide for Connecting to Google Workspace

Contents

Mapping a Google Workspace environment in One Identity Manager

One Identity Manager offers simplified user administration for Google Workspace. One Identity Manager concentrates on setting up and editing user accounts and providing the required permissions. For this, groups, organizations, permissions, admin roles, products, and SKUs are mapped in One Identity Manager.

One Identity Manager provides company identities with the necessary user accounts. There are different ways for you to connect identities to their user accounts. You can also manage user accounts independently of identities and thus set up administrator user accounts.

For more detailed information about the Google Workspace structure, see the Google Workspace documentation from Google.

Architecture overview

To access Google Workspace data, the Google Workspace connector is installed on a synchronization server. The Google Workspace connector establishes communication with the Google Workspace to be synchronized through several Google Inc. REST APIs. The synchronization server ensures the comparison of data between the One Identity Manager database and Google Workspace.

Figure 1: Architecture for synchronization
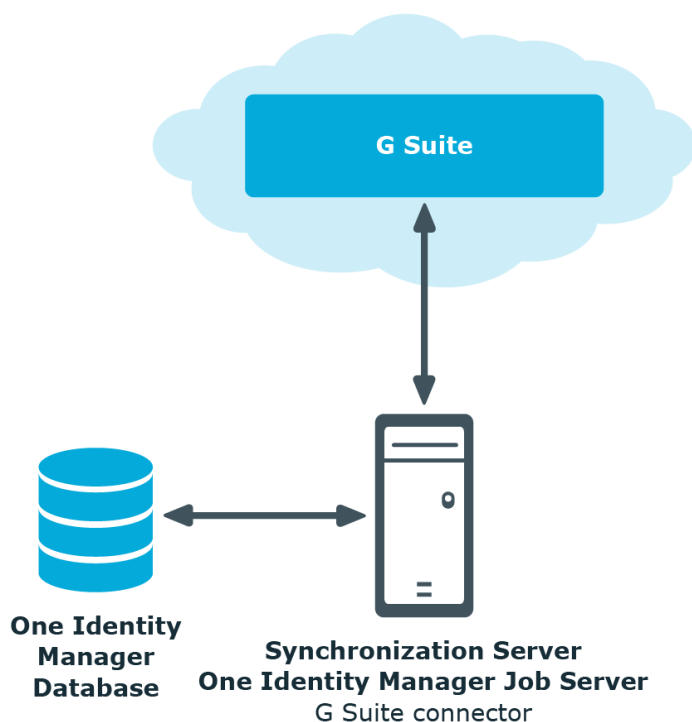
One Identity Manager users for managing a Google Workspace customer

The following users are used for setting up and administration of a customer.

Table 1: Users

User	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required.

User	Tasks
	• Specify which application roles for target system managers are mutually exclusive.
	• Authorize other identities 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 | Google Workspace** 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.
	• Edit password policies for the target system.
	• Prepare entitlements to add to the IT Shop.
	• Can add identities that do not have the **Primary identity** identity type.
	• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.
	• Edit the synchronization's target system types and outstanding objects.
	• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.
	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.

Configuration parameters

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

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

Synchronizing a Google Workspace customer

One Identity Manager supports synchronization with Google Workspace. The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and Google Workspace.

This sections explains how to:

- Set up synchronization to import initial data from a customer in to the One Identity Manager database.

- Adjust a synchronization configuration, for example, to synchronize different customers with the same synchronization project.

- Start and deactivate the synchronization.

- Analyze synchronization results.

TIP: Before you set up synchronization with a customer, familiarize yourself with the Synchronization Editor. For more information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

Setting up initial synchronization of a Google Workspace customer

The Synchronization Editor provides a project template that can be used to set up the synchronization of user accounts and permissions for the customer. You use these project templates to create synchronization projects with which you import the data from a customer into your One Identity Manager database. In addition, processes are created that are required to provision changes to target system objects from the One Identity Manager database into the target system.

To load customer objects into the One Identity Manager database for the first time

1. In the customer, prepare a user with sufficient permissions for synchronization.

2. The One Identity Manager components for managing Google Workspace are available if the **TargetSystem | GoogleApps** configuration parameter is set.

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

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

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

3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.

4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with a Google Workspace customer on page 16
- System requirements for the Google Workspace synchronization server on page 19
- Creating a synchronization project for initial synchronization of a Google Workspace customer on page 22
- Configuration parameters for managing a Google Workspace environment on page 186
- Default project template for Google Workspace on page 189

Users and permissions for synchronizing with a Google Workspace customer

The following users play a role in synchronizing One Identity Manager with Google Workspace.

Table 2: Users for synchronization

User	Permissions
User for accessing the target system (synchronization user)	You must provide at least one user with super user permissions and a service account for authentication for full synchronization of customer objects with the supplied One Identity Manager default configuration. • The Google cloud platform project requires access to the following API's. Admin SDK Enterprise License Manager API Groups Settings API • A service account with the associated JSON key and cross domain Google Workspace delegation is required for authentication. • API access must be enabled in the Google Admin console. • The service account's client ID must be authorized for various API scopes in the Google Admin console: A list of API scopes is available on the One Identity Manager installation medium. You can use this list as a copy template. Directory: `Modules\GAP\dvd\AddOn\ApiAccess` File: `GoogleWorkspaceRequiredAPIAccess.txt` For more information, see Setting up the necessary permissions for accessing the Google Workspace customer on page 17.
One Identity Manager Service user account	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires permissions for the internal

User	Permissions
	web service.
	NOTE: If the One Identity Manager Service runs under the network service (**NT Author-ity\NetworkService**), you can grant permissions for the internal web service with the following command line call:
	`netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"`
	The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.
	In the default installation, One Identity Manager is installed under:
	• `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems)
	• `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to run synchronization using an application server.

Related topics

- API scopes for the service account on page 191
- Advanced settings for the system connection to Google Workspace on page 33

Setting up the necessary permissions for accessing the Google Workspace customer

To provide the Google Workspace connector with access to the target system, the required permissions must be set up in two Google web interfaces.

To set up the service account and enable APIs

1. Open the Google Cloud Platform console (https://console.cloud.google.com).
2. Log in as the Google Workspace super admin.
3. Select a project or create a new one.
4. Enable the APIs **Admin SDK**, **Enterprise License Manager API** and **Groups Settings API**.
5. Create a service account.

Table 3: Service account properties

Property	Value
Role	
Provide new private key	Enabled
Key type	JSON
Activate cross-domain Google Workspace delegation	Enabled

6. Note the service account's client ID.

    You will need it for setting up the API privileges.

7. Save the key file locally.

    You will need it for creating the synchronization project.

To enable API access and authorize the service account's client ID for the required API scopes

1. Open the Google Admin console (https://admin.google.com).

2. Log in as the Google Workspace super admin.

3. Enable API access.

4. Authorize the service account's client ID for the required API scope.

    For more information, see User for accessing the target system (synchronization user) on page 16.

5. Set up other users with super admins privileges if necessary.

    Up to eight users with super admin privileges can be used. Each user must log in to Google Workspace at least once and accept the terms of use.

Setting up the Google Workspace synchronization server

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

The One Identity Manager Service with the Google Workspace connector must be installed on the synchronization server.

Detailed information about this topic

- System requirements for the Google Workspace synchronization server on page 19
- Installing the One Identity Manager Service on page 19

System requirements for the Google Workspace synchronization server

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

- Windows operating system

    The following versions are 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.

Installing the One Identity Manager Service

The One Identity Manager Service must be installed on the synchronization server with the Google Workspace connector. The synchronization server must be declared as a Job server in One Identity Manager.

Table 4: Properties of the Job server

Property	Value
Server function	Google Workspace connector
Machine role	Server | Job Server | Google Workspace

NOTE: If several target system environments of the same type are synchronized under the same synchronization server, it is recommended that you set up a Job server for each target system for performance reasons. 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).

To set up a Job server, perform the following steps.

1. Create a Job server and install and configure the One Identity Manager Service.

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

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

Use the Server Installer to install the One Identity Manager Service locally or remotely.

To remotely install the One Identity Manager Service, provide an administrative workstation on which the One Identity Manager components are installed. Ensure that the One Identity Manager components are installed on the server before installing locally. For more information about installing One Identity Manager components, see the *One Identity Manager Installation Guide*.

2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.

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

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

1. Start the Server Installer program.

   NOTE: To install remotely, start the Server Installer program on your administrative workstation. To install locally, start the program on the server.

2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

   You can connect via the application server or directly to connect to the database.

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

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

      - OR -

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

   b. Enter the following data for the Job server.

      - **Server**: Name of the Job server.
      - **Queue**: Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process

steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.

- **Full server name**: Full server name in accordance with DNS syntax.

  Syntax:

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

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

4. On the **Machine roles** page, select **Google Workspace**.

5. On the **Server functions** page, select **Google Workspace connector**.

6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

   For a direct connection to the database:

   a. In the module list, 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.

   d. Click **OK**.

   For a connection to the application server:

   a. In the module list, select the **Process collection** entry and click the **Insert** button.

   b. Select **AppServerJobProvider** and click **OK**.

   c. In the module list, select **Process collection > AppServerJobProvider**.

   d. Click the **Connection parameter** entry, then click the **Edit** button.

   e. Enter the address (URL) for the application server and click **OK**.

   f. Click the **Authentication data** entry and click the **Edit** button.

   g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

   h. Click **OK**.

7. To configure the installation, click **Next**.

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

9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.

10. On the **Service access** page, enter the service's installation data.

    - **Computer**: Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.

      To run the installation locally, select **Local installation** from the menu.

    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

    You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

11. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.

12. Click **Finish** on the last page of the Server Installer.

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

Creating a synchronization project for initial synchronization of a Google Workspace customer

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Google Workspace. The following describes the steps for initial configuration of a synchronization project. For more information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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.

Detailed information about this topic

- Information required for setting up a synchronization project on page 23
- Creating an initial synchronization project for a Google Workspace customer on page 25

Information required for setting up a synchronization project

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

Table 5: Information required for setting up a synchronization project

Data	Explanation
Primary domain	Name of the Google Workspace customer's primary domain.
Service account's key file	JSON key file that was saved when the service account was set up .
Super admin email addresses for logging in	You can enter up to eight super administrators for use in synchronizing the customer. The more that are entered, the more accesses can be done in parallel. This improves the total runtime of a request.
	Provide at least one user with super administrator permissions. For more information, see Users and permissions for synchronizing with a Google Workspace customer on page 16.
Synchronization server for Google Workspace	All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.
	The One Identity Manager Service with the Google Workspace connector must be installed on the synchronization server.

Table 6: Additional properties for the Job server

Property	Value
Server function	Google Workspace connector
Machine role	Server/Job server/Google Workspace

For more information, see System requirements for the Google Workspace synchronization server on page 19.

One Identity Manager	• Database server

Data	Explanation
database connection data	• Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used Use of the integrated Windows 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 the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.
	
	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
	
	    • Google Workspace connector 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 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*.

Creating an initial synchronization project for a Google Workspace customer

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

- Run in default mode
- Started from the Launchpad

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

NOTE: Just one synchronization project can be created per target system and default project template used.

To set up initial synchronization project for a customer

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

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

2. Select the **Target system type Google Workspace** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. On the wizard's start page, click **Next**.

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

   - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.

   - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.

5. On the **Primary domain and service account** page, enter the primary domain of the Google Workspace account and the key file for the service account.

   Table 7: Login credentials for connection to Google Workspace

Property	Description
Primary domain	Name of this Google Workspace's primary domain.
Service account's key file	JSON key file saved when the service account was set up. • Drag and drop the key on the field to load it.

Property	Description
	- OR -
	• Click **Open key file** and select the path to the key file.

6. On the **Google Workspace Administrators** page, enter the email addresses of all the super administrators who can use the Google Workspace connector for logging into the target system.

   You can enter up to eight super administrators. The more that are entered, the more accesses can be done in parallel. This improves the total runtime of a request.

   • Click **Test connection** to test the connection data.

     All administrator accounts are verified and a check is run on whether the correct API scopes are authorized.

7. Specify, on the **Local cache** page, whether the Google Workspace connector's local cache should be used. This minimizes the number of times the customer is accessed during full synchronization. It prevents the API contingent from being exceeded through synchronization.

   This option is set by default and should only be disabled for troubleshooting.

8. 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.

9. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE:

   • If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again.

   • This page is not shown if a synchronization project already exists.

10. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.

11. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 8: Specify target system access

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

12. On the **Synchronization server** page, select the synchronization server to run the synchronization.

   If the synchronization server is not declared as a Job server for this target system 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.

      TIP: You can also implement an existing Job server as the synchronization server for this target system.

      • To select a Job server, click .

      This automatically assigns the server function matching this Job server.

   c. Click **OK**.

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

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

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

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

This sets up, saves and immediately activates the synchronization project.

NOTE:

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

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

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

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

Related topics

Configuring the synchronization log

All the information, tips, warnings, and errors that occur during synchronization are recorded in the synchronization log. You can configure the type of information to record separately for each system connection and synchronization workflow.

To configure the content of the synchronization log for a system connection

1. To configure the synchronization log for target system connection, in the Synchronization Editor, select the **Configuration > Target system** category.

   - OR -

To configure the synchronization log for the database connection, in the Synchronization Editor, select the **Configuration > One Identity Manager connection** category.

2. In the **General** section, click **Setup**.

3. In the **Synchronization log** section, set **Create synchronization log**.

4. Enable the data to be logged.

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

5. Click **OK**.

To configure the content of the synchronization log for a synchronization workflow

1. In the Synchronization Editor, select the **Workflows** category.

2. Select a workflow in the navigation view.

3. In the **General** section, click **Edit**.

4. Select the **Synchronization log** tab.

5. Enable the data to be logged.

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

6. Click **OK**.

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.

Related topics

- Displaying synchronization results on page 44

Customizing the synchronization configuration for Google Workspace

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

NOTE: If you want to change the configuration of existing synchronization projects, check the possible effects of these changes on the data that has already been synchronized.

You must customize the synchronization configuration to be able to regularly compare the database with the customer and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.

- To specify which Google Workspace objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.

- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.

- Use variables to set up a synchronization project for synchronizing different customers. Store a connection parameter as a variable for logging in to the respective customer.

- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema. Include the schema extensions in the mapping.

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

Detailed information about this topic

Configuring synchronization with Google Workspace customers

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object

modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the primary system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing the customer

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

2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.

3. Create a new workflow with the workflow wizard.

   This creates a workflow with **Target system** as its direction of synchronization.

4. Create a new start up configuration. Use the new workflow to do this.

5. Save the changes.

6. Run a consistency check.

Related topics

- Configuring synchronization of different Google Workspace customers on page

Configuring synchronization of different Google Workspace customers

In some circumstances, you can use a synchronization project to synchronize different customers.

Prerequisites

- The customer target systems schema are identical.

- All virtual schema properties used in the mapping must exist in the customer's extended schemas.

- The connection parameters to the target system are defined as variables.

To customize a synchronization project for synchronizing another customer

1. Supply a user in the customer with sufficient permissions for accessing Google Workspace.

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

3. Create a new base object for the other customer.

   - Use the wizard to attach a base object.

   - In the wizard, select the Google Workspace connector.

- Declare the connection parameters. The connection parameters are saved in a special variable set.

   A start up configuration is created that uses the newly created variable set.

4. Change other elements of the synchronization configuration as required.

5. Save the changes.

6. Run a consistency check.

Related topics

- Configuring synchronization with Google Workspace customers on page 30

Updating schemas

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

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

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

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

To update a system connection schema

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

2. Select the **Configuration > Target system** category.

   - OR -

Select the **Configuration > One Identity Manager connection** category.

3. Select the **General** view and click **Update schema**.

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

   This reloads the schema data.

To edit a mapping

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

2. Select the **Mappings** category.

3. Select a mapping in the navigation view.

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

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

Speeding up synchronization with revision filtering

Synchronization with Google Workspace does not support revision filtering.

Advanced settings for the system connection to Google Workspace

You can make various additional changes to the target system connection settings, for example, defining the number of retries or timeouts. When you set up synchronization for the first time, these system connection properties are set to default values. You can modify the default values to help analysis of synchronization problems, for example.

There are two ways to change the default values.

a. Specify a specialized variable set and change the values of the affected variables. (Recommended action).

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time.

   For more information, see .

b. Edit the target system connection with the system connection wizard and change the effected values.

   The system connection wizard supplies additional explanations of the settings. The

default values can only be restored under particular conditions.

For more information, see

NOTE: If the project wizard is started directly from the Synchronization Editor when you set up initial synchronization, you can edit the advanced settings when you set up the synchronization project. In this case, the default values are immediately overwritten by your settings.

Table 9: Target system connection advanced settings

Property	Description
Read-only API access	Specifies whether the API scopes were only entered for read-only access in the Google Admin Console Enable this option if no write access to the target system may be assigned. The connector only has read access to the target system. • The service account's client ID must be authorized for various API scopes in the Google Admin console: A list of API scopes is available on the One Identity Manager installation medium. You can use this list as a copy template. Directory: `Modules\GAP\dvd\AddOn\ApiAccess` File: `GoogleWorkspaceRequiredAPIAccessReadOnly.txt` If this option is disabled, read-write access is possible. Other API scopes must be authorized for this.
Use the local cache	Specifies whether the Google Workspace connector's local cache is used. Local cache is used to prevent the API contingent from being exceeded through synchronization. Accesses to Google Workspace are minimized during full synchronization. The option is ignored during provisioning. This option is set by default and can be disabled for troubleshooting. For more information about this, see the *One Identity Manager Target System Synchronization Reference Guide*.
Polling count	Specifies how many attempts are made to load a new value into the target system during provisioning or synchronization before an error occurs. The result of saving certain user account properties (such as phone numbers or Instant Messenger settings) appears after a delay in Google Workspace and cannot be used for other operations straightaway.
Batch retry count	Specifies the number of retries allowed for failed batch operations in the target system, for example, when synchronizing group memberships.
Batch timeout	Timeout between retries of failed batch operations.
Transfer user data before	Specifies whether Google application user data is transferred to a different user account before user accounts are deleted.

Property	Description
delete	User data such as Google Drive data, Google+ pages, and Google calendar, can be transferred to a different user account before final deletion. Variable: `CP_TransferUserDataBeforeDelete`

User data transfer XML	Google application user data is transferred to a different user account before user accounts are deleted. By default all user data is transferred. To replace the default list, an XML document can be stored here.
	
	To restore the default list, delete the XML document.
	
	Example of a user data transfer XML
	
	``xml
	<Applications>
	    <Application name="Drive and Docs">
	        <TransferParam key="PRIVACY_LEVEL">
	            <TransferValue value="SHARED" />
	            <TransferValue value="PRIVATE" />
	        </TransferParam>
	    </Application>
	    <Application name="Calendar">
	        <TransferParam key="RELEASE_RESOURCES">
	            <TransferValue value="TRUE" />
	        </TransferParam>
	    </Application>
	    <Application name="Google+" />
	</Applications>
	``
	
	This connection parameter cannot be converted to a variable.

Default email address for data transfer	Default email address of the destination user account for the transfer of user data when a user account is deleted. The email address of the destination user account belongs to the primary domain of the customer to which the deleted user account belongs. This email address is used if no email address can be determined by the manager of the deleted user account. Variable: `CP_DefaultDataTransferTargetEmail`
Products and SKUs XML	Product IDs and Stock keeping unit IDs as XML file. The list of available products and SKUs is defined by Google and therefore fixed in the Google Workspace connector. If Google changes this list, you can enter an XML file here that overwrites the list in the Google Workspace connector. To restore the default list, delete the XML document. **Example of a Products and SKUs XML**

Property	Description

```
<products>
    <product name="Google Workspace" id="Google-Apps">
        <sku id="Google-Apps-Unlimited" name="Google Workspace
Business"/>
        <sku id="Google-Apps-For-Business" name="Google Workspace
Basic" />
        <sku id="Google-Apps-Lite" name="oogle Workspace Lite"/>
        <sku id="Google-Apps-For-Postini" name="Google Apps Message
Security"/>
    </product>
    <product name="Google Drive storage" id="Google-Drive-storage">
        <sku id="Google-Drive-storage-20GB" name="Google Drive storage
20 GB"/>
        <sku id="Google-Drive-storage-50GB" name="Google Drive storage
50 GB"/>
        <...>
        <sku id="Google-Drive-storage-16TB" name="Google Drive storage
16 TB"/>
    </product>
    <...>
</products>
```

This connection parameter cannot be converted to a variable.

Related topics

- Transferring user data to a different Google Workspace user account on page 144
- API scopes for the service account on page 191
- Users and permissions for synchronizing with a Google Workspace customer on page 16

Editing connection parameters in the variable set

The connection parameters for advanced settings were saved as variables in the default variable when synchronization was set up. You can change the values in these variables to suit you requirements and assign the variable set to a start up configuration and a base object. This means that you always have the option to use default values from the default variable set.

NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project is used for synchronizing different customers.

To customize connection parameters in a specialized variable set

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

2. Select the **Configuration > Target system** category.

3. Open the **Connection parameters** view.

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

4. Select one of the following parameters and click **Convert**.

   - Polling count
   - Batch retry count
   - Batch timeout
   - Use the local cache
   - Read-only API access

5. Select the **Configuration > Variables** category.

   All specialized variable sets are shown in the lower part of the document view.

6. Select a specialized variable set or click on ⊞ in the variable set view's toolbar.

   - To rename the variable set, select the variable set and click the variable set view in the toolbar ✎. Enter a name for the variable set.

7. Select the previously added variable and enter a new value.

8. Select the **Configuration > Start up configurations** category.

9. Select a start up configuration and click **Edit**.

10. Select the **General** tab.

11. Select the specialized variable set in the **Variable set** menu.

12. Select the **Configuration > Base objects** category.

13. Select the base object and click ✎.

    - OR -

    To add a new base object, click ⊞ .

14. Select the specialized variable set in the **Variable set** menu.

15. Save the changes.

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

Detailed information about this topic

- Advanced settings for the system connection to Google Workspace on page 33

Editing target system connection properties

The advanced settings of the target system connection can be changed using the system connection wizard. If variables are defined for the settings, the changes are transferred to the active variable set.

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

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

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

To edit advanced settings with the system connection wizard

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

2. In the toolbar, select the active variable set to be used for the connection to the target system.

   NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.

3. Select the **Configuration > Target system** category.

4. Click **Edit connection**.

   This starts the system connection wizard.

5. On the system connection wizard's start page, enable **Show advanced options**.

6. On the **Google Workspace administrators** page, you can also enable the **Read-only API access** option.

   When you test the connection, a check is carried out to verify if the appropriate API scopes are authorized.

7. On the **Local cache** page, you can set the **Use the local cache** option.

8. Customize the properties as required on the **Advanced settings** page.

9. Save the changes.

Detailed information about this topic

- Advanced settings for the system connection to Google Workspace on page 33

Configuring the provisioning of memberships

Memberships, such as user accounts in groups, are saved in assignment tables in the One Identity Manager database. During provisioning of modified memberships, changes

made in the target system may be overwritten. This behavior can occur under the following conditions:

- Memberships are saved as an object property in list form in the target system.

  Example: List of user accounts in the `Member` property of a Google Workspace group (`Group`)

- Memberships can be modified in either of the connected systems.

- A provisioning workflow and provisioning processes are set up.

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and previously deleted memberships are added again.

To prevent this, provisioning can be configured such that only the modified membership is provisioned in the target system. The corresponding behavior is configured separately for each assignment table.

To allow separate provisioning of memberships

1. In the Manager, select the **Google Workspace > Basic configuration data > Target system types** category.

2. In the result list, select the **Google Workspace** target system type.

3. Select the **Configure tables for publishing** task.

4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.

5. Click **Merge mode**.

   NOTE:

   - This option can only be enabled for assignment tables that have a base table with a `XDateSubItem` column.

   - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.

6. Save the changes.

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

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

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

To restore the original condition

1. Select the auxiliary table for which you want to restore the condition.

2. Right-click on the selected row and select the **Restore original values** context menu item.

3. Save the changes.

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

Example of a condition on the GAPUserInPaSku assignment table:

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

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

Configuring single object synchronization

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

Prerequisites

- A synchronization step exists that can import the changes to the changed object into One Identity Manager.

- The path to the base object of the synchronization is defined for the table that contains the changed object.

Single object synchronization is fully configured for synchronization projects created using the default project template. If you want to incorporate custom tables into this type of synchronization project, you must configure single object synchronization for these tables. For more information about this, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

1. In the Manager, select the **Google Workspace > Basic configuration data > Target system types** category.

2. In the result list, select the **Google Workspace** target system type.

3. Select the **Assign synchronization tables** task.

4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.

5. Save the changes.

6. Select the **Configure tables for publishing** task.

7. Select the custom table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

   Example: `FK(UID_GAPCustomer).XObjectKey`

8. Save the changes.

Related topics

Accelerating provisioning and single object synchronization

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

Load balancing is used only for individual provisioning processes into the customer environment to prevent parallel processing from creating inconsistent data in the target system. If the maximum number of instances on the process task or process component is set to **1** or **-1**, load balancing cannot take place.

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

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
   - Job servers that share processing must have the **No process assignment** option enabled.
   - Assign the **Google Workspace connector** server function to the Job server.

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

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

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

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

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

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

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- Editing Google Workspace Job servers on page 177

Running synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Starting synchronization on page 43
- Deactivating synchronization on page 44
- Displaying synchronization results on page 44
- Pausing handling of target system specific processes (Offline mode) on page 51

Starting synchronization

When you set up the initial synchronization project using the Launchpad, a default schedule for regular synchronization is created and assigned. Activate this schedule to synchronize on a regular basis.

To synchronize on a regular basis

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

2. Select the **Configuration > Start up configurations** category.

3. Select a start up configuration in the document view and click **Edit schedule**.

4. Edit the schedule properties.

5. To enable the schedule, click **Activate**.

6. Click **OK**.

You can also start synchronization manually if there is no active schedule.

To start initial synchronization manually

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

2. Select the **Configuration > Start up configurations** category.

3. Select a start up configuration in the document view and click **Run**.

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

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.

  - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.

- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.

  - Use the schedule to ensure that the start up configurations are run in sequence.

  - Group start up configurations with the same start up behavior.

Displaying synchronization results

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

To display a synchronization log

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

2. Select the **Logs** category.

3. Click ▶ in the navigation view toolbar.

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

4. Select a log by double-clicking it.

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

To display a provisioning log

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

2. Select the **Logs** category.

3. Click ⚡ in the navigation view toolbar.

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

4. Select a log by double-clicking it.

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

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

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

Related topics

- Configuring the synchronization log on page 28
- Troubleshooting on page 49

Deactivating synchronization

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

To prevent regular synchronization

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

2. Select the start up configuration and deactivate the configured schedule.

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited 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. In the Synchronization Editor, open the synchronization project.

2. Select the **General** view on the home page.

3. Click **Deactivate project**.

Related topics

-

Synchronizing single objects

Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated.

NOTE: If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

To synchronize a single object

1. In the Manager, select the **Google Workspace** category.

2. Select the object type in the navigation view.

3. In the result list, select the object that you want to synchronize.

4. Select the **Synchronize this object** task.

   A process for reading this object is entered in the job queue.

Features of synchronizing memberships

If you synchronize changes in an object's member list, run single object synchronization on the assignment's root object, The base table of an assignment contains an `XDateSubItem` column containing information about the last change to the memberships.

> **Example:**
>
> Base object for assignment of user accounts to admin roles is the admin role assignment.
>
> In the target system, a user was assigned to an admin role. To synchronize this assignment, in the Manager, select the admin role assignment that the user account was assigned to and run single object synchronization. When you do this, all memberships for this admin role assignment are synchronized.
>
> The user account must already exist as an object in the One Identity Manager database for the assignment to be made.

Detailed information about this topic

- Configuring single object synchronization on page 40

Tasks following synchronization

After the synchronization of data from the target system into the One Identity Manager database, rework may be necessary. Check the following tasks:

- Post-processing outstanding objects on page 46
- Managing Google Workspace user accounts through account definitions on page 49

Post-processing outstanding objects

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select the **Google Workspace > Target system synchronization: Google Workspace** category.

   The navigation view lists all the synchronization tables assigned to the **Google Workspace** target system type.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

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

   - The synchronization log has already been deleted.

     - OR -

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

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

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

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

   TIP:

   ### *To display object properties of an outstanding object*

   1. Select the object on the target system synchronization form.
   2. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.

4. Click on one of the following icons in the form toolbar to run the respective method.

   Table 10: Methods for handling outstanding objects

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

Icon	Method	Description
		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.
	Reset	The **Outstanding** label is removed for the object.

> TIP: If a method cannot be run due to certain restrictions, the respective icon is disabled.
>
> • To display the constraint's details, click the **Show** button in the **Constraints** column.

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

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

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

> ***To disable bulk processing***
>
> • Disable the icon in the form's toolbar.

> NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. This means that the **Connection is read-only** option is not set in the target system connection and the **Read-only API access** option is not set in the in the system connection wizard.

Related topics

- Adding custom tables to the target system synchronization on page 48
- Advanced settings for the system connection to Google Workspace on page 33

Adding custom tables to the target system synchronization

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

To add tables to target system synchronization

1. In the Manager, select the **Google Workspace > Basic configuration data > Target system types** category.

2. In the result list, select the **Google Workspace** target system type.

3. Select the **Assign synchronization tables** task.

4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.

5. Save the changes.

6. Select the **Configure tables for publishing** task.

7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.

8. Save the changes.

Related topics

- Post-processing outstanding objects on page 46

Managing Google Workspace user accounts through account definitions

In the default installation, after synchronizing, identities are automatically created for the user accounts.If an account definition for the customer is not known at the time of synchronization, user accounts are linked with identities. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

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

Detailed information about this topic

- Assigning account definitions to linked user accounts on page 79

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

  The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.

- Analyzing synchronization

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

- Logging messages

  One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.

- Reset start information

  If synchronization stopped unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.

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

Related topics

-

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

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

2. Select the **Configuration > One Identity Manager connection** category.

3. In the **General** view, click **Edit connection**.

   This starts the system connection wizard.

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

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

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

5. Save the changes.

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

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

Pausing handling of target system specific processes (Offline mode)

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

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

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

Prerequisites

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

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

To allow offline mode for a base object

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

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

The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and

the target system, all pending processes must be handled before synchronization can start.

Only use offline mode, if possible, for short system downtimes such as mainten-ance windows.

To flag a target system as offline

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

2. Select **Manage > System monitoring > Flag target systems as offline**.

3. Click **Run**.

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

4. Select the base object whose target system connection is not available.

5. Click **Switch offline**.

6. Confirm the security prompt with **OK**.

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

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

Related topics

- Deactivating synchronization on page 44

Managing Google Workspace user accounts and identities

The main feature of One Identity Manager is to map identities together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to identities. This provides an overview of the permissions for each identity in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Identities are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

Because requirements vary between companies, One Identity Manager offers different methods for supplying user accounts to identities. One Identity Manager supports the following methods for linking identities and their user accounts:

- Identities can automatically obtain their account definitions using user account resources.

    If an identity does not yet have a user account in a customer, a new user account is created. This is done by assigning account definitions to an identity using the integrated inheritance mechanisms and subsequent process handling.

    When you manage account definitions through user accounts, you can specify the way user accounts behave when identities are enabled or deleted.

- When user accounts are inserted, they can be automatically assigned to an existing identity or a new identity can be created if necessary. In the process, the identity main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding identities for automatic identity assignment.

- Identities and user accounts can be entered manually and assigned to each other.

For more information about basic handling and administration of identities and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

Account definitions for Google Workspace user accounts

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

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

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

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

For more detailed information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Collecting IT operating data
- Assigning account definitions to identities and target systems

Detailed information about this topic

Creating account definitions

Create one or more account definitions for the target system.

To create a new account definition

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.
2. Click ➕ in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Related topics

Editing account definitions

You can edit the main data of account definitions.

To edit an account definition

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Change main data** task.

4. Enter the account definition's main data.

5. Save the changes.

Related topics

- Main data for account definitions on page 56
- Creating account definitions on page 55

Main data for account definitions

Enter the following data for an account definition:

Table 11: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically.
	Leave empty for Google Workspace customers.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assigning the account definition to identities. Set a value in the range **0** to **1**. This

Property	Description
	input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set.
	For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The resource can also be assigned directly to identities and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to identities	Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the **Enable automatic assignment to identities** The account definition is assigned to every identity that is not marked as external. Once a new internal identity is created, they automatically obtain this account definition.
	To automatically remove the account definition assignment from all identities, use the **Disable automatic assignment to identities**. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated identities.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily deactivated identities.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): The account definition assignment is

Property	Description
	not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of identities.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to identities posing a security risk.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests. • If you add an identity with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
Products and SKUs can be inherited	Specifies whether the user account can inherit products and SKUs through the linked identity. If the option is set, the user account inherits profiles through hierarchical roles, in which the identity is a member, or through IT Shop requests.
Admin roles assignments can be inherited	Specifies whether the user account can inherit admin role assignments through the linked identity. If the option is set, the user account inherits admin role assignments through hierarchical roles, in which the identity is a member, or through IT Shop requests.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the identity but they do no inherit any further properties. When a new user account is added with this manage level and an identity is assigned, some of the identity's properties are transferred initially. If the identity properties are changed at a later date, the changes are not passed onto the user account.

- **Full managed**: User accounts with the **Full managed** manage level inherit defined properties of the assigned identity. When a new user account is created with this manage level and an identity is assigned, the identity's properties are transferred in an initial state. If the identity properties are changed at a later date, the changes are passed onto the user account.

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

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

Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

- Identity user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the identity is reinstated at a later date, the user accounts are also reactivated.

- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the identity's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this identity. Existing group memberships are deleted.

To edit a manage level

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

Related topics

- Main data for manage levels on page 61
- Creating manage levels on page 60
- Assigning manage levels to account definitions on page 60

Creating manage levels

One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

IMPORTANT: In the Designer, extend the templates by adding the procedure for the additional manage levels. For more information about templates, see the *One Identity Manager Configuration Guide*

To create a manage level

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Manage levels** category.

2. Click ⬛ in the result list.

3. On the main data form, edit the main data of the manage level.

4. Save the changes.

Related topics

- Main data for manage levels on page 61
- Editing manage levels on page 59

Assigning manage levels to account definitions

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

To assign manage levels to an account definition

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Assign manage level** task.

4. In the **Add assignments** pane, assign the manage level.

    TIP: In the **Remove assignments** pane, you can remove assigned manage levels.

    ### *To remove an assignment*

    - Select the manage level and double-click ✅.

5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 12: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. (Default) • **Always**: Data is always updated. • **Only initially**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated identities are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated identities retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated identities are locked.
Retain groups on deferred deletion	Specifies whether user accounts of identities marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of identities marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of identities posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of identities posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating mapping rules for IT operating data

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

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

- Google Workspace Organization
- Groups can be inherited
- Products and SKUs can be inherited
- Admin roles assignments can be inherited
- Change password at next login
- Identity
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Edit IT operating data mapping** task.

4. Click **Add** and enter the following information:

   - **Column**: User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

   - **Source**: Specifies which roles to use in order to find the user account properties. You have the following options:

      - Primary department
      - Primary location
      - Primary cost center
      - Primary business roles

         NOTE: The business role can only be used if the Business Roles Module is available.

      - Empty

If you select a role, you must specify a default value and set the **Always use default value** option.

- **Default value**: Default value of the property for an identity's user account if the value is not determined dynamically from the IT operating data.

- **Always use default value**: Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.

- **Notify when applying the default**: Specifies whether an email is sent to a specific mailbox when the default value is used. The **Identity - new user account with default properties created** mail template is used.

    To change the mail template, in the Designer, adjust the **TargetSystem | GoogleApps | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Entering IT operating data

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity is assigned a primary business role, primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example:

Normally, each identity in department A obtains a default user account in the customer A. In addition, certain identities in department A obtain administrative user accounts in the customer A.

Create an account definition A for the default user account of the customer A and an account definition B for the administrative user account of customer A.In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

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

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.

2. Select the **Edit IT operating data** task.

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

    -   **Effects on**: Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

        ### *To specify an application scope*

        a. Click ➔ next to the field.

        b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table or an account definition.

        c. Select the specific target system or account definition under **Effects on**.

        d. Click **OK**.

    -   **Column**: Select the user account property for which the value is set.

        In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

    -   **Value**: Enter a fixed value to assign to the user account's property.

4. Save the changes.

Related topics

-   Creating mapping rules for IT operating data on page 62

Modify IT operating data

If IT operating data changes, you must transfer the changes to the existing user accounts. To do this, templates must be rerun on the affected columns. Before you can run the templates, you can check what effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

Prerequisites

-   The IT operating data of a department, a cost center, a business role, or a location have been changed.

    - OR -

-   The default values in the IT operating data template were modified for an account definition.

NOTE: If the assignment of an identity to a primary department, cost center, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Run templates** task.

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

    - **Old value**: Value of the object property before changing the IT operating data.

    - **New value**: Value of the object property after changing the IT operating data.

    - **Selection**: Specifies whether the new value is copied to the user account.

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

5. Click **Apply**.

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

Assigning Google Workspace account definitions to identities

Account definitions are assigned to company identities.

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

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

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

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

NOTE: As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

Prerequisites for indirect assignment of account definitions to identities

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task and configure the permitted assignments.

   - To generally allow an assignment, enable the **Assignments allowed** column.
   - To allow direct assignment, enable the **Direct assignments permitted** column.

3. Save the changes.

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

Assigning Google Workspace account definitions to departments, cost centers, and locations

Assign account definitions to departments, cost centers, and locations in order to assign identities to them through these organizations.

To add account definitions to hierarchical roles

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Assign organizations** task.

4. In the **Add assignments** pane, assign the organizations:

   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.

- On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

- Select the organization and double-click ⊘.

5. Save the changes.

Assigning account definitions to business roles

NOTE: This function is only available if the Business Roles Module is installed.

You can assign account definitions to business roles in order to assign them to identities through business roles.

To add account definitions to hierarchical roles

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Assign business roles** task.

4. In the **Add assignments** pane, select the role class and assign business roles.

   TIP: In the **Remove assignments** pane, you can remove assigned business roles.

   To remove an assignment

   - Select the business role and double-click ⊘.

5. Save the changes.

Assigning account definitions to all identities

Use this task to assign the account definition to all internal identities. Identities that are marked as external do not obtain this account definition. Once a new internal identity is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

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

To assign an account definition to all identities

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Change main data** task.

4. Select the **Disable automatic assignment to identities** task.

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

6. Save the changes.

NOTE: To automatically remove the account definition assignment from all identities, run the DISABLE AUTOMATIC ASSIGNMENT TO IDENTITIES task. The account definition cannot be reassigned to identities from this point on. Existing assignments remain intact.

Assigning account definitions directly to identities

Account definitions can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and account definitions in company structures, like departments, cost centers, locations, or business roles.

To react quickly to special requests, you can assign account definitions directly to identities.

To assign an account definition directly to identities

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Assign to identities** task.

4. In the **Add assignments** pane, add identities.

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

   ### *To remove an assignment*

   - Select the identity and double-click ⊘.

5. Save the changes.

Assigning account definitions to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add an account definition to system roles.

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

To add account definitions to a system role

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

> TIP: In the **Remove assignments** pane, you can remove assigned system roles.
>
> ***To remove an assignment***
>   - Select the system role and double-click ✓.

5. Save the changes.

Adding account definitions in the IT Shop

An account definition can be requested by shop customers when it is assigned to an IT Shop shelf. To ensure it can be requested, further prerequisites need to be guaranteed.

- The account definition must be labeled with the **IT Shop** option.

- The account definition must be assigned to a service item.

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

- If the account definition is only assigned to identities using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

> NOTE: IT Shop administrators can assign account definitions to IT Shop shelves if login is role-based. Target system administrators are not authorized to add account definitions in the IT Shop.

To add an account definition to the IT Shop (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.

5. Save the changes.

To add an account definition to the IT Shop (non role-based login)

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.

5. Save the changes.

To remove an account definition from individual IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.

5. Save the changes.

To remove an account definition from individual IT Shop shelves (non role-based login)

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.

5. Save the changes.

To remove an account definition from all IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Remove from all shelves (IT Shop)** task.

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

5. Click **OK**.

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

To remove an account definition from all IT Shop shelves (non role-based login)

1. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Remove from all shelves (IT Shop)** task.

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

5. Click **OK**.

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

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

Related topics

- Main data for account definitions on page 56

Assigning Google Workspace account definitions to target systems

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

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

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

To assign the account definition to a target system

1. In the Manager, select the customer in the **Google Workspace > Customers** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Related topics

- Assigning identities automatically to Google Workspace user accounts on page 74

Deleting Google Workspace account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all identities.

   a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Change main data** task.

   d. Select the **Disable automatic assignment to identities** task.

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

   f. Save the changes.

2. Remove direct assignments of the account definition to identities.

   a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Assign to identities** task.

   d. In the **Remove assignments** pane, remove identities.

   e. Save the changes.

3. Remove the account definition's assignments to departments, cost centers, and locations.

   a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Assign organizations** task.

   d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.

   e. Save the changes.

4. Remove the account definition's assignments to business roles.

   a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Assign business roles** task.

   d. In the **Remove assignments** pane, remove the business roles.

   e. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

To remove an account definition from all IT Shop shelves (role-based login)

a. In the Manager, select the **Entitlements > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Remove from all shelves (IT Shop)** task.

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

e. Click **OK**.

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

To remove an account definition from all IT Shop shelves (non role-based login)

a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Remove from all shelves (IT Shop)** task.

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

e. Click **OK**.

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

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Change main data** task.

d. From the **Required account definition** menu, remove the account definition.

e. Save the changes.

7. Remove the account definition's assignments to target systems.

a. In the Manager, select the customer in the **Google Workspace > Customers** category.

b. Select the **Change main data** task.

c. On the **General** tab, remove the assigned account definitions.

d. Save the changes.

8. Delete the account definition.

a. In the Manager, select the **Google Workspace > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Click ✖ to delete an account definition.

Assigning identities automatically to Google Workspace user accounts

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

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

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

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

For more information about assigning identities automatically, see the *One Identity Manager Target System Base Module Administration Guide*.

Run the following tasks to assign identities automatically.

- If you want identities to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | GoogleApps | PersonAutoFullsync** configuration parameter and select the required mode.

- If you want identities to be assigned outside synchronization, in the Designer, set the **TargetSystem | GoogleApps | PersonAutoDefault** configuration parameter and select the required mode.

- In the **TargetSystem | GoogleApps | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to identities shall take place.

  Example:

  ADMINISTRATOR*

  TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic identity assignment** dialog.

To edit the exclude list for automatic identity assignment

1. In the Designer, edit the **PersonExcludeList** configuration parameter.

2. Click **...** next to the **Value** field.

   This opens the **Exclude list for Google Workspace user accounts** dialog.

3. To add a new entry, click **Add**.

   To edit an entry, select it and click **Edit**.

4. Enter the name of the user account that does not allow identities to be assigned automatically.

   Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.

5. To delete an entry, select it and click **Delete**.

6. Click **OK**.

- Use the **TargetSystem | GoogleApps | PersonAutoDisabledAccounts** configuration parameter to specify whether identities can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.

- Assign an account definition to the customer. Ensure that the manage level to be used is entered as the default manage level.

- Define the search criteria for identity assignment to this customer.

NOTE:

The following applies for synchronization:

- Automatic identity assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:

- Automatic identity assignment takes effect if user accounts are added.

NOTE:

In the default installation, after synchronizing, identities are automatically created for the user accounts. If an account definition for the customer is not known at the time of synchronization, user accounts are linked with identities. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

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

For more information, see Managing Google Workspace user accounts through account definitions on page 49.

Related topics

- Creating account definitions on page 55
- Assigning Google Workspace account definitions to target systems on page 71
- Changing the manage level in Google Workspace user accounts on page 78
- Editing search criteria for automatic identity assignment on page 76

Editing search criteria for automatic identity assignment

The criteria for identity assignments are defined for the customer. You specify which user account properties must match the identity's properties such that the identity can be assigned to the user account. You can limit search criteria further by using format definitions.

The search criterion is written in XML notation to the **Search criteria for automatic identity assignment** column (`AccountToPersonMatchingRule`) in the `GAPCustomer` table.

Search criteria are evaluated when identities are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of identities to user accounts based on the search criteria and make the assignment directly.

NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

To specify criteria for identity assignment

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.
2. Select the customer in the result list.
3. Select the **Define search criteria for identity assignment** task.
4. Specify which user account properties must match with which identity so that the identity is linked to the user account.

   Table 13: Standard search criteria for user accounts

Apply to	Column for identity	Column for user account
Google Workspace user accounts	Default email address (`DefaultEmailAddress`)	Primary email address (`PrimaryEmail`)

5. Save the changes.

For more information about defining search criteria, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Assigning identities automatically to Google Workspace user accounts on page 74
- Finding identities and directly assigning them to user accounts on page 77

Finding identities and directly assigning them to user accounts

Based on the search criteria, you can create a suggestion list for the assignment of identities to user accounts and make the assignment directly. User accounts are grouped in different views for this.

- **Suggested assignments**: This view lists all user accounts to which One Identity Manager can assign an identity. All identities are shown that were found using the search criteria and can be assigned.

- **Assigned user accounts**: This view lists all user accounts to which an identity is assigned.

- **No identity assignment**: This view lists all user accounts to which no identity is assigned and for which no identity was found using the search criteria.

NOTE: To display disabled user accounts or deactivated identities in the view, enable the **Even locked accounts are mapped** option.

If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.

To apply search criteria to user accounts

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.

2. Select the customer in the result list.

3. Select the **Define search criteria for identity assignment** task.

4. At the bottom of the form, click **Reload**.

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

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

The assignment of identities to user accounts creates connected user accounts (**Linked** state). To create managed user accounts (**Linked configured** state), you can assign an account definition at the same time.

To assign identities directly to user accounts

- Click **Suggested assignments**.

  1. Click the **Selection** box of all user accounts to which you want to assign the suggested identities. Multi-select is possible.

  2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.

3. Click **Assign selected**.

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

   The identities determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

   - OR -

- Click **No identity assignment**.

   1. Click **Select identity** for the user account to which you want to assign an identity. Select an identity from the menu.

   2. Click the **Selection** box of all user accounts to which you want to assign the selected identities. Multi-select is possible.

   3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.

   4. Click **Assign selected**.

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

      The identities displayed in the **Identity** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.

   1. Click the **Selection** box of all the user accounts with the identity assignment you want to delete. Multi-select is possible.

   2. Click **Remove selected**.

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

      The assigned identities are removed from the selected user accounts.

Changing the manage level in Google Workspace user accounts

The default manage level is applied if you create user accounts using automatic identity assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list.

3. Select the **Change main data** task.

4. Select the manage level in the **Manage level** list on the **General** tab.

5. Save the changes.

Related topics

- General main data of Google Workspace user accounts on page 130

Assigning account definitions to linked user accounts

An account definition can be subsequently assigned to user accounts with **Linked** status. For example, this may be necessary if:

- Identities and user accounts have been linked manually.
- Automatic identity assignment is configured, but an account definition is not yet assigned to the customer when inserting a user account.

To manage user accounts through account definitions

1. Create an account definition.

2. Assign an account definition to the customer.

3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.

   a. In the Manager, select the **Google Workspace > User accounts > Linked but not configured > <customer>** category.

   b. Select the **Assign account definition to linked accounts** task.

   c. In the **Account definition** menu, select the account definition.

   d. Select the user accounts that contain the account definition.

   e. Save the changes.

Detailed information about this topic

- Account definitions for Google Workspace user accounts on page 54
- Assigning Google Workspace account definitions to target systems on page 71

Manually linking identities to Google Workspace user accounts

An identity can be linked to multiple Google Workspace user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One

identity can also use default user accounts with different types.

To manually assign user accounts to an identity

1. In the Manager, select the **Identities > Identities** category.

2. Select the identity in the result list and run the **Assign Google Workspace user accounts** task.

3. Assign the user accounts.

4. Save the changes.

Related topics

- Supported user account types on page 80

Supported user account types

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

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

- Identity type

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

Table 14: Identity types of user accounts

Identity type	Description	Value of the IdentityType column
Primary identity	Identity's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the company, for example for subcontracts with other functional areas.	Organizational
Personalized administrator identity	User account with administrative permissions, used by an identity.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions,	Shared

Identity type	Description	Value of the IdentityType column
	used by multiple identities.	
Service identity	Service account.	Service

- Privileged user account

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

Detailed information about this topic

Default user accounts

Normally, each identity obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the identity. The effect of the link and the scope of the identity's inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.

2. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level.

3. Create a formatting rule for IT operating data.

    You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through an identity's primary roles.

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

- In the mapping rules for the `IsGroupAccount_Group`, `IsGroupAccount_PaSku`, and `IsGroupAccount_OrgAdminRole` columns, use the default value **1** and set the **Always use default value** option.

- In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

5. Assign the account definition to identities.

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

Related topics

- Account definitions for Google Workspace user accounts on page 54

Administrative user accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as **Administrator**.

Administrative user accounts are imported into One Identity Manager during synchronization.

NOTE: Some administrative user accounts can be automatically identified as privileged user accounts. To do this, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

Related topics

- Providing administrative user accounts for one identity on page 83
- Providing administrative user accounts for several people on page 84

Providing administrative user accounts for one identity

Use this task to create an administrative user account that can be used by an identity.

Prerequisites

- The user account must be labeled as a personalized administrator identity.
- The identity that will be using the user account must be marked as a personalized administrator identity.
- The identity that will be using the user account must be linked to a main identity.

To prepare an administrative user account for an identity

1. Label the user account as a personalized administrator identity.

   a. In the Manager, select the **Google Workspace > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

   d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.

2. Link the user account to the identity that will be using this administrative user account.

   a. In the Manager, select the **Google Workspace > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

   d. On the **General** tab, in the **Identity** selection list, select the identity that will be using this administrative user account.

      TIP: If you are the target system manager, you can selected 📇 to create a new identity.

For more information about mapping identity types, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Providing administrative user accounts for several people on page 84

Providing administrative user accounts for several people

Use this task to create an administrative user account that can be used by more that one identity.

Prerequisite

- The user account must be labeled as a shared identity.
- There must be an identity with the type **Shared identity** available. The shared identity must have a manager.
- The identities who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple identities

1. Label the user account as a shared identity.

   a. In the Manager, select the **Google Workspace > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

   d. On the **General** tab, in the **Identity** menu, select **Shared identity**.

2. Link the user account to an identity.

   a. In the Manager, select the **Google Workspace > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

   d. On the **General** tab, in the **Identity** menu, select an identity the type **Shared identity**.

   > TIP: If you are the target system manager, you can use the ⊞ button to create a new shared identity.

3. Assign the identities who will use this administrative user account to the user account.

   a. In the Manager, select the **Google Workspace > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Assign identities authorized to use** task.

   d. In the **Add assignments** pane, add identities.

   > TIP: In the **Remove assignments** pane, you can remove assigned identities.

To remove an assignment

- Select the identity and double-click ✅.

For more information about mapping identity types, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

-

Privileged user accounts

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

NOTE: The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the `TSBVAccountIsPrivDetectRule` table (which is a table of the **Union** type). The evaluation is done in the `TSB_SetIsPrivilegedAccount` script.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.

2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.

3. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships in the manage level.

4. Create a formatting rule for the IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through an identity's primary roles.

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

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.

   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.

   - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount_Group`,

IsGroupAccount_PaSku, and IsGroupAccount_OrgAdminRole columns with a default value of **0** and set the **Always use default value** option.

5. Enter the effective IT operating data for the target system.

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

6. Assign the account definition directly to identities who work with privileged user accounts.

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

TIP: If customization requires that the login names of primary mail addresses of privileged user accounts follow a defined naming convention, specify how the email addresses are formatted in the template.

Related topics

Specifying deferred deletion for Google Workspace user accounts

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or locked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is **30** days.

  In the Designer, enter a different value for deferred deletion in the `Deferred deletion [days]` property of the **GAPUser** table.

- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

  To use object-specific deferred deletion, in the Designer, create a `Script (deferred deletion)` for the **GAPUser** table.

Example:

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

```
If Not $IsPrivilegedAccount:Bool$ Then

      Value = 10

End If
```

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

Login credentials for Google Workspace user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login credentials generated to users.

Detailed information about this topic

- Password policies for Google Workspace user accounts on page 88
- Initial password for new Google Workspace user accounts on page 100
- Email notifications about login data on page 100

Password policies for Google Workspace user accounts

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the identities' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined password policies on page 89
- Using password policies on page 90
- Creating password policies on page 92
- Custom scripts for password requirements on page 96

Predefined password policies

You can customize predefined password policies to meet your own requirements if necessary.

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time log in on the Web Portal (`Person.Passcode`).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for identities, user accounts, or system users.

For more information about password policies for identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming identities' central passwords

An identity's central password is formed from the target system specific user accounts by respective configuration. The **Identity central password policy** defines the settings for the (`Person.CentralPassword`) central password. Members of the **Identity Management | Identities | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Identity central password policy** does not violate the target system-specific requirements for passwords.

For more information about password policies for identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

The **Google Workspace password policy** is predefined for the customer. You can apply this password policy to customer user accounts (`GAPUser.Password`).

If the customers' password requirements differ, it is recommended that you set up your own password policies for each customer.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Using password policies

The **Google Workspace password policy** is predefined for the customer. You can apply this password policy to customer user accounts (GAPUser.Password).

If the customers' password requirements differ, it is recommended that you set up your own password policies for each customer.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's Google Workspace customer.
4. The **One Identity Manager password policy** (default policy).

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.
   - **Apply to**: Application scope of the password policy.

   To specify an application scope
   1. Click ➜ next to the field.
   2. Select one of the following references under **Table**:
      - The table that contains the base objects of synchronization.
      - To apply the password policy based on the account definition, select the **TSBAccountDef** table.
      - To apply the password policy based on the manage level, select the **TSBBehavior** table.
   3. Under **Apply to**, select the table that contains the base objects.

- If you have selected the table containing the base objects of synchronization, next select the specific target system.

- If you have selected the **TSBAccountDef** table, next select the specific account definition.

- If you have selected the **TSBBehavior** table, next select the specific manage level.

4. Click **OK**.

- **Password column**: Name of the password column.

- **Password policy**: Name of the password policy to use.

5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.

2. Select the password policy in the result list.

3. Select the **Assign objects** task.

4. In the **Assignments** pane, select the assignment you want to change.

5. From the **Password Policies** menu, select the new password policy you want to apply.

6. Save the changes.

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Edit the password policy's main data.

5. Save the changes.

Detailed information about this topic

- General main data of password policies on page 92

- Policy settings on page 93

Creating password policies

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

To create a password policy

1. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.
2. Click ➕ in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

Detailed information about this topic

General main data of password policies

Enter the following main data of a password policy.

Table 15: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the 🌐 button.
Description	Text field for additional explanation. Translate the given text using the 🌐 button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the 🌐 button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be

Property	Meaning
	changed.
	NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for identities, user accounts, or system users.

Policy settings

Define the following settings for a password policy on the **Password** tab.

Table 16: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into account.
	This data is only taken into account if the One Identity Manager login was through a system user or identity based authentication module. If a user has exceeded the maximum number of failed logins, the identity or system user will not be able to log in to One Identity Manager.
	You can use the Password Reset Portal to reset the passwords of identities and system users who have been locked. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then

Property	Meaning
	the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 17: Character classes for passwords

Property	Meaning
Required number of character classes	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for **Min. number letters**, **Min. number lowercase**, **Min. number uppercase**, **Min. number digits**, and **Min. number special characters**. That means: • Value **0**: All character class rules must be fulfilled. • Value **>0**: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value **>0**. │ NOTE: Generated passwords are not tested for this.
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.

Property	Meaning
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

Checking passwords with a script

You can implement a script if additional policies need to be used for checking a password that cannot be mapped with the available settings.

Syntax of check scripts

Public Sub CCC_CustomPwdValidate(policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)

With parameters:

policy = password policy object

spwd = password to check

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

Example: Script that checks a password

A password cannot start with **?** or **!** . The password cannot start with three identical characters. The script checks a given password for validity.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)

    Dim pwd = spwd.ToInsecureArray()

    If pwd.Length>0

        If pwd(0)="?" Or pwd(0)="!"

            Throw New Exception(#LD("Password can't start with '?' or
            '!'")#)

        End If
```

```
        End If
        If pwd.Length>2
            If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
                Throw New Exception(#LD("Invalid character sequence in
                password")#)
            End If
        End If
 End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.

2. Edit the password policy.

   a. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.

   b. In the result list, select the password policy.

   c. Select the **Change main data** task.

   d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.

   e. Save the changes.

Related topics

-

Generating passwords with a script

You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script

`Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)`

With parameters:

`policy` = password policy object

`spwd` = generated password

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

> **Example: Script that generates a password**
>
> In random passwords, this script replaces the invalid characters **?** and **!** at the beginning of a password with **_**.
>
> ```
> Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd
> As System.Security.SecureString)
>
>      Dim pwd = spwd.ToInsecureArray()
>
>      ' replace invalid characters at first position
>
>      If pwd.Length>0
>
>           If pwd(0)="?" Or pwd(0)="!"
>
>                spwd.SetAt(0, CChar("_"))
>
>           End If
>
>      End If
>
> End Sub
> ```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
    e. Save the changes.

Related topics

- Checking passwords with a script on page 96

Editing the excluded list for passwords

You can add words to a list of restricted terms to prohibit them from being used in passwords.

| NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.

2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.

3. Save the changes.

Checking passwords

When you verify a password, all the password policy settings, custom scripts, and the restricted passwords are taken into account.

To verify if a password conforms to the password policy

1. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Select the **Test** tab.

5. Select the table and object to be tested in **Base object for test**.

6. Enter a password in **Enter password to test**.

   A display next to the password shows whether it is valid or not.

Testing the generation of passwords

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. In the Manager, select the **Google Workspace > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Select the **Test** tab.

5. Click **Generate**.

   This generates and displays a password.

Initial password for new Google Workspace user accounts

You can issue an initial password for a new user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
    - In the Designer, set the **TargetSystem | GoogleApps | Accounts | InitialRandomPassword** configuration parameter.
    - Apply target system specific password policies and define the character sets that the password must contain.
    - Specify which identity will receive the initial password by email.

Related topics

- Password policies for Google Workspace user accounts on page 88
- Email notifications about login data on page 100

Email notifications about login data

You can configure the login credentials for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text in a mail template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

The following prerequisites must be fulfilled in order to use notifications:

- Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
- In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.
- Ensure that all identities have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
- Ensure that a language can be determined for all identities. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

When a randomly generated password is issued for the new user account, the initial login data for a user account is sent by email to a previously specified identity.

To send initial login data by email

1. Enable the **TargetSystem | GoogleApps | Accounts | InitialRandomPassword** configuration parameter in the Designer.

2. In the Designer, set the **TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the notification recipient as a value.

   If no recipient can be found, the email is sent to the address stored in the **TargetSystem | GoogleApps | DefaultAddress** configuration parameter.

3. In the Designer, set the **TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

   By default, the message sent uses the mail template **Identity - new user account created**. The message contains the name of the user account.

4. In the Designer, set the **TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

   By default, the message sent uses the mail template **Identity - initial password for new user account**. The message contains the initial password for the user account.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Managing Google Workspace entitlement assignments

In a customer, users can have different entitlements, which are mapped in One Identity Manager as follows:

- Entitlement for logging in to Google Workspace

  Table: **Google Workspace Products and SKUs** (GAPPaSku)

- Administrative entitlements

  Table: **Google Workspace Admin role assignments** (GAPOrgAdminRole)

- Entitlement for the use of Google Workspace groups

  Table: **Google Workspace Groups** (GAPGroup)

Entitlement assignments refer to the assignment of the various entitlements to user accounts. These include:

- Google Workspace user accounts: assignments to products and SKUs (GAPUserInPaSku table)

- Google Workspace user accounts: assignments to admin role assignments (GAPUserInOrgAdminRole table)

- Google Workspace user accounts: assignments to groups (GAPUserInGroup table)

- Google Workspace groups: assignments to customers (GAPCustomerInGroup table)

In addition, external users can participate in groups as members, owners, or managers. External users are represented by an external email address and assigned to the groups.

Assigning Google Workspace entitlements to user accounts in One Identity Manager

In One Identity Manager, Google Workspace entitlements can be assigned directly or indirectly to identities.

In the case of indirect assignment, identities and entitlements are organized in hierarchical roles. The number of entitlements assigned to an identity is calculated from the position in the hierarchy and the direction of inheritance. If the identity has a Google Workspace user account, the entitlements are assigned to this user account.

Entitlements can also be assigned to identities through IT Shop requests. To enable the assignment of entitlements using IT Shop requests, identities are added as customers in a shop. All entitlements assigned to this shop as products can be requested by the customers. After approval is granted, requested entitlements are assigned to the identities.

You can use system roles to group entitlements together and assign them to identities as a package. You can create system roles that contain only Google Workspace entitlements. You can also group any number of company resources into a system role.

To react quickly to special requests, you can also assign the entitlements directly to user accounts.

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide*
	One Identity Manager Business Roles Administration Guide
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Adding Google Workspace entitlements to the IT Shop on page 108
- Assigning Google Workspace entitlements directly to a user account on page 111
- Assigning Google Workspace groups directly to a customer on page 112
- Assigning Google Workspace customers directly to a group on page 113

Prerequisites for indirect assignment of Google Workspace entitlements to Google Workspace user accounts

In the case of indirect assignment, identities and Google Workspace entitlements are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning Google Workspace entitlements indirectly, check the following settings and modify them if necessary.

1. The assignment of identities, Google Workspace products and SKUs, Google Workspace admin role assignments, and Google Workspace groups is permitted for departments, cost centers, locations, or business roles.

   For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

   To configure assignments to roles of a role class

   1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

      - OR -

      In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

   2. Select the **Configure role assignments** task and configure the permitted assignments.

      - To generally allow an assignment, enable the **Assignments allowed** column.

      - To allow direct assignment, enable the **Direct assignments permitted** column.

   3. Save the changes.

2. Settings for assigning Google Workspace entitlements to Google Workspace user accounts.

   - Google Workspace user accounts are labeled with the **Products and SKUs can be inherited**, **Admin roles assignments can be inherited**, and **Groups can be inherited** options.

- Google Workspace user accounts are linked with an identity through the `UID_Person` (**Person**) column.
- Google Workspace user accounts and entitlements belong to the same customer.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of identities not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Editing main data of Google Workspace user accounts on page 128
- General main data of Google Workspace user accounts on page 130

Assigning Google Workspace entitlements to departments, cost centers, and locations

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

To assign a permission to a department, cost center or location (non role-based login):

1. In the Manager, select one of the following categories:
   - **Google Workspace > Groups**
   - **Google Workspace > Products and SKUs**
   - **Google Workspace > Admin role assignments**
2. Select the entitlements in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

   To remove an assignment
   - Select the organization and double-click ⊘.
5. Save the changes.

To assign permissions to a department, cost center or location (role-based login)

1. In the Manager, select the **Organizations > Departments** category.

   - OR -

   In the Manager, select the **Organizations > Cost centers** category.

   - OR -

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

2. Select the department, cost center, or location in the result list.

3. Select one of the following tasks.

   - **Google Workspace Assign groups**

   - **Google Workspace Assign products and SKUs**

   - **Assign Google Workspace admin role assignments**

4. In the **Add assignments** pane, assign the entitlements.

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

   To remove an assignment

   - Select the entitlement and double-click ⊘.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Google Workspace entitlements to Google Workspace user accounts on page 104

- One Identity Manager users for managing a Google Workspace customer on page 11

Assigning Google Workspace entitlements to business roles

NOTE: This function is only available if the Business Roles Module is installed.

You assign entitlements to business roles so that these entitlements are assigned to user accounts through these business roles.

To assign an entitlement to business roles (non role-based login):

1. In the Manager, select one of the following categories.

   - **Google Workspace > Groups**

   - **Google Workspace > Products and SKUs**

   - **Google Workspace > Admin role assignments**

2. Select the entitlements in the result list.

3. Select the **Assign business roles** task.

4. In the **Add assignments** pane, select the role class and assign business roles.

   TIP: In the **Remove assignments** pane, you can remove assigned business roles.

   To remove an assignment

   - Select the business role and double-click ✓.

5. Save the changes.

To assign entitlements to a business role (role-based login):

1. In the Manager, select the **Business roles > <role class>** category.

2. Select the business role in the result list.

3. Select one of the following tasks.

   - **Google Workspace Assign groups**
   - **Google Workspace Assign products and SKUs**
   - **Assign Google Workspace admin role assignments**

4. In the **Add assignments** pane, assign the entitlements.

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

   To remove an assignment

   - Select the entitlement and double-click ✓.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Google Workspace entitlements to Google Workspace user accounts on page 104
- One Identity Manager users for managing a Google Workspace customer on page 11

Adding Google Workspace entitlements to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add an entitlement to system roles. If you assign a system role to identities, all user accounts owned by these identities inherit the entitlement.

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

To assign an entitlement to system roles:

1. In the Manager, select one of the following categories.

    *   **Google Workspace > Groups**
    *   **Google Workspace > Products and SKUs**
    *   **Google Workspace > Admin role assignments**

2. Select the entitlements in the result list.

3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

    TIP: In the **Remove assignments** pane, you can remove assigned system roles.

    To remove an assignment

    *   Select the system role and double-click ⊘.

5. Save the changes.

Related topics

*   Prerequisites for indirect assignment of Google Workspace entitlements to Google Workspace user accounts on page 104

Adding Google Workspace entitlements to the IT Shop

When you assign a permission to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed:

*   The permissions must be labeled with the **IT Shop** option.

*   The permission must be assigned a service item.

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

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

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

To add a permission to the IT Shop.

1. In the Manager, select the one of the following categories (non role-based login).

    - **Google Workspace > Groups**
    - **Google Workspace > Products and SKUs**
    - **Google Workspace > Admin role assignments**

    - OR -

    In the Manager, select one of the following categories (role-based login).

    - **Entitlements > Google Workspace groups**
    - **Entitlements > Google Workspace products and SKUs**
    - **Entitlements > Google Workspace admin role assignments**

2. In the result list, select the permission.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane, the entitlement to the IT Shop shelves.
6. Save the changes.

To remove, an entitlement from individual shelves of the IT Shop

1. In the Manager, select the one of the following categories (non role-based login).

    - **Google Workspace > Groups**
    - **Google Workspace > Products and SKUs**

    - OR -

    In the Manager, select one of the following categories (role-based login).

    - **Entitlements > Google Workspace groups**
    - **Entitlements > Google Workspace products and SKUs**

2. In the result list, select the permission.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, the entitlement from the IT Shop shelves.
6. Save the changes.

To remove, an entitlement from all shelves of the IT Shop

1. In the Manager, select the one of the following categories (non role-based login).

    - **Google Workspace > Groups**
    - **Google Workspace > Products and SKUs**

    - OR -

    In the Manager, select one of the following categories (role-based login).

- **Entitlements > Google Workspace groups**
- **Entitlements > Google Workspace products and SKUs**

2. In the result list, select the permission.

3. Select the **Remove from all shelves (IT Shop)** task.

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

5. Click **OK**.

   The entitlement is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this entitlement are canceled.

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

Related topics

- Prerequisites for indirect assignment of Google Workspace entitlements to Google Workspace user accounts on page 104
- General main data of Google Workspace groups on page 146
- General main data of Google Workspace products and SKUs on page 155
- One Identity Manager users for managing a Google Workspace customer on page 11

Assigning Google Workspace user accounts directly to an entitlement

To react quickly to special requests, you can assign the entitlements directly to user accounts.

To assign an entitlement directly to user accounts

1. In the Manager, select one of the following categories.
   - **Google Workspace > Groups**
   - **Google Workspace > Products and SKUs**
   - **Google Workspace > Admin role assignments**

2. Select the entitlements in the result list.

3. Select in the **Assign user accounts** task.

4. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment
   - Select the user account and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Google Workspace entitlements directly to a user account on page 111
- Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
- Assigning Google Workspace entitlements to business roles on page 106
- Adding Google Workspace entitlements to system roles on page 107
- Adding Google Workspace entitlements to the IT Shop on page 108
- Assigning Google Workspace customers directly to a group on page 113
- Assigning Google Workspace groups directly to a customer on page 112

Assigning Google Workspace entitlements directly to a user account

To react quickly to special requests, you can assign entitlements directly to a user account. You cannot directly assign permissions that have the **Only use in IT Shop** option set.

To assign entitlements directly to a user account

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list.

3. Select one of the following tasks.

    - **Assign groups**

    - **Assign products and SKUs**

    - **Admin role assignments**

4. In the **Add assignments** pane, assign the entitlements.

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

    To remove an assignment

    - Select the entitlement and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Google Workspace user accounts directly to an entitlement on page 110
- Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
- Assigning Google Workspace entitlements to business roles on page 106
- Adding Google Workspace entitlements to system roles on page 107

Assigning Google Workspace groups directly to a customer

To add all user accounts of a customer as members in a Google Workspace group, assign the groups directly to the Google Workspace customer. In the calculation of inheritance, for all user accounts of the customer, an entry is made in the GAPUserInGroup table. The origin of the assignment is indicated in the XOrigin column with the value **16**.

To assign groups directly to a customer

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.

2. Select the customer in the result list.

3. Select **Assign groups** category.

4. In the **Add assignments** pane, assign the groups.

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

   To remove an assignment

   - Select the group and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Google Workspace user accounts directly to an entitlement on page 110
- Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
- Assigning Google Workspace entitlements to business roles on page 106
- Adding Google Workspace entitlements to system roles on page 107
- Adding Google Workspace entitlements to the IT Shop on page 108
- Assigning Google Workspace entitlements directly to a user account on page 111
- Assigning Google Workspace customers directly to a group on page 113
- Special features in the assignment of Google Workspace groups on page 194

Assigning Google Workspace customers directly to a group

To add all user accounts of a customer as members in a Google Workspace group, assign the Google Workspace customers directly to the group. In the calculation of inheritance, for all user accounts of the customer, an entry is made in the `GAPUserInGroup` table. The origin of the assignment is indicated in the `XOrigin` column with the value **16**.

To assign customers directly to a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select **Assign Google Workspace customer as member**.

4. Assign the customers in the **Add assignments** view.

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

   To remove an assignment

   - Select the customer and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Google Workspace user accounts directly to an entitlement on page 110
- Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
- Assigning Google Workspace entitlements to business roles on page 106
- Adding Google Workspace entitlements to system roles on page 107
- Adding Google Workspace entitlements to the IT Shop on page 108
- Assigning Google Workspace entitlements directly to a user account on page 111
- Assigning Google Workspace groups directly to a customer on page 112
- Special features in the assignment of Google Workspace groups on page 194

Effectiveness of Google Workspace entitlement assignments

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

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

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.

- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.

- One Identity Manager does not check if membership of an excluded group is permitted in another group (GAPGroupInGroup table).

The effectiveness of the assignments is mapped in the GAPUserInGroup and GAPBaseTreeHasGroup tables by the XIsInEffect column.

Example: The effect of group memberships

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

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

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

Table 18: Specifying excluded groups (GAPGroupExclusion table)

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

Table 19: Effective assignments

Identity	Member in role	Effective group
Pat Identity1	Marketing	Group A

Identity	Member in role	Effective group
Jan User3	Marketing, finance	Group B
Jo User1	Marketing, finance, control group	Group C
Chris User2	Marketing, control group	Group A, Group C

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

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

Table 20: Excluded groups and effective assignments

Identity	Member in role	Assigned group	Excluded group	Effective group
Chris User2	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

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

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

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

- Mutually exclusive groups belong to the same customer.

To exclude a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select a group in the result list.

3. Select the **Exclude groups** task.

4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.

5. Save the changes.

Inheritance of Google Workspace entitlements based on categories

In One Identity Manager, user accounts can selectively inherit entitlements. To do this, entitlements, and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables, enter your categories for the permissions. Each table contains the category positions **position 1** to **position 63**.

Every user account can be assigned to one or more categories. Each entitlement can also be assigned to one or more categories. If at least one of the category positions between the user account and the assigned entitlement is the same, the entitlement is inherited by the user account. If the entitlement or the user account is not classified in a category, the entitlement is also inherited by the user account.

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

Table 21: Category examples

Category position	Categories for user accounts	Categories for entitlements
1	Default user	Default group
2	Administrator	Administrator group

Figure 2: Example of inheriting through categories.
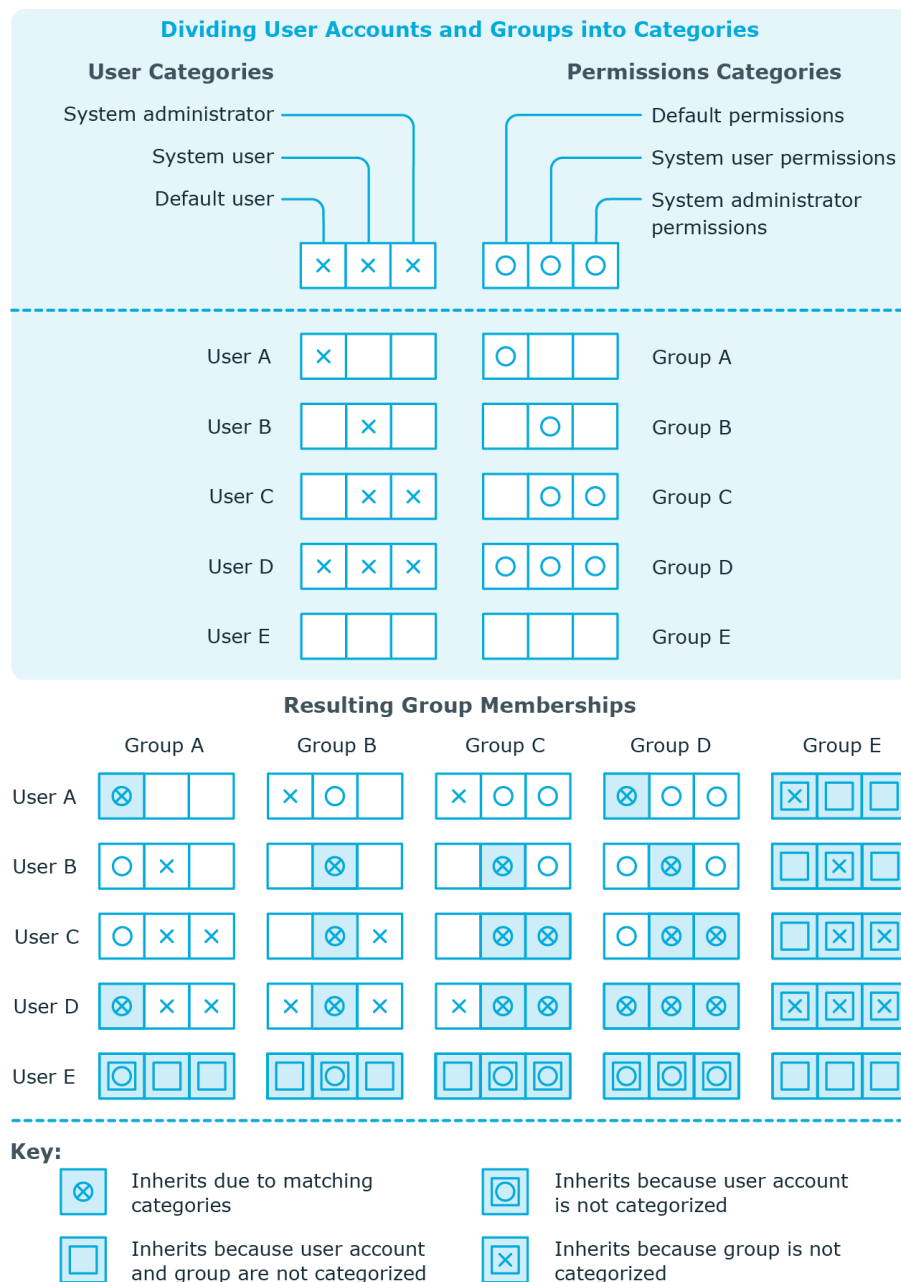
To use inheritance through categories

1. Define the categories for the Google Workspace customer.

2. Assign categories to user accounts through their main data.

3. Assign categories to groups, products, and SKUs through their main data.

Related topics

- Defining categories for the inheritance of Google Workspace entitlements on page 124
- General main data of Google Workspace user accounts on page 130
- General main data of Google Workspace groups on page 146
- General main data of Google Workspace products and SKUs on page 155

Assigning Google Workspace groups to an external user

You can add an external user as a member in different groups by assigning the external email address directly to the groups. The **Allow external members** option must be enabled on the groups.

To assign groups directly to an external email address

1. In the Manager, select the **Google Workspace > External email addresses**.
2. Select the external email address in the result list.
3. Select the **Assign groups** category.
4. In the **Add assignments** pane, assign the groups.

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

   To remove an assignment
   - Select the group and double-click ⊘.
5. Save the changes.

Related topics

- Assigning external users to a Google Workspace group on page 119
- Google Workspace external email addresses on page 168
- Assigning group owners to Google Workspace groups on page 151
- Assigning group managers to Google Workspace groups on page 150

Assigning external users to a Google Workspace group

By assigning external email addresses to a group, you add external users as members to the group. The **Allow external members** option must be enabled for this group.

To assign external email addresses directly to a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign external email addresses** task.

4. In the **Add assignments** pane, assign the external email addresses.

   TIP: In the **Remove assignments** pane, you can remove external email addresses.

   ### *To remove an assignment*

   - Select the external email address and click ✅.

5. Save the changes.

Related topics

- Assigning Google Workspace groups to an external user on page 118
- Google Workspace external email addresses on page 168
- Assigning group managers to Google Workspace groups on page 150
- Assigning group owners to Google Workspace groups on page 151

Overview of all assignments

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

Example:

- If the report is created for a resource, all roles are determined in which there are identities with this resource.

- If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.

- If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.

- If the report is created for a department, all roles are determined in which identities of the selected department are also members.

- If the report is created for a business role, all roles are determined in which identities of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.

- Click the 🖳 **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain identities with the selected base object.

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

- Double-click a control to show all child roles belonging to the selected role.

- By clicking the ⌄ button in a role's control, you display all identities in the role with the base object.

- Use the small arrow next to ⌄ to start a wizard that allows you to bookmark this list of identities for tracking. This creates a new business role to which the identities are assigned.

Figure 3: Toolbar of the Overview of all assignments report.

🛈 | 🖫 | 🖳 Used by ▾ | ▼ | ▶ Department ▶ Dresden

Table 22: Meaning of icons in the report toolbar

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

Mapping Google Workspace objects in One Identity Manager

You use One Identity Manager to manage all customer objects that are required for optimizing access control in the target system. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

Google Workspace customers

The target system for the synchronizing Google Workspace is the primary domain of a Google Workspace customer. Google Workspace customers are created as base objects for the synchronization in One Identity Manager. They are used to configure provisioning processes, automatic assignment of identities to user accounts, and to pass down Google Workspace entitlements to user accounts.

Creating Google Workspace customers

NOTE: The Synchronization Editor sets up the Google Workspace customers in the One Identity Manager database. If necessary, customers can also be created in the Manager.

To set up a customer

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.

2. Click ⊞ in the result list.

3. On the main data form, edit the main data of the customer.

4. Save the changes.

Related topics

-
-
-
-

Editing main data of Google Workspace customers

To edit the main data of a customer

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.

2. Select the customer in the result list.

3. Select the **Change main data** task.

4. Edit the main data of the customer.

5. Save the changes.

Related topics

-
-
-
-

General main data of Google Workspace customers

On the **General** tab, you enter the following main data:

Table 23: General main data of Google Workspace customers

Property	Description
Google Workspace customer	Unique ID of the Google Workspace customer.

Property	Description
Customer primary domain	Name of this customer's primary domain.
Customer creation time	Time at which the customer was created.
Alternative email address	Second email address for the customer. This email address must not be in the customer's domain.
Phone	Customer's telephone number in E.164 format.
Country	Unique country ID.
Language	Name of the language.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of identities to user accounts is used for this customer and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied.
	User accounts are only linked to the identity (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role in which the customer's target system managers are defined. Target system managers only edit objects from customers to whom they are assigned. A different target system manager can be assigned to each customer.
	Select the One Identity Manager application role whose members are responsible for the administration of this customer. Use the button to add a new application role.
Synchronized by	Type of synchronization through which data is exchanged between the customer and One Identity Manager. You can no longer change the synchronization type once objects for this customer are present in One Identity Manager.
	When you create a customer with the Synchronization Editor is **One Identity Manager** used.

Table 24: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Google Workspace connector	Google Workspace connector
No synchronization	none	none

Property	Description
	NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.

Related topics

- Assigning Google Workspace account definitions to target systems on page 71
- Account definitions for Google Workspace user accounts on page 54
- Assigning identities automatically to Google Workspace user accounts on page 74
- Target system managers for Google Workspace customers on page 181

Google Workspace customer address data

On the **Postal address** tab, enter the following main data:

Table 25: Google Workspace customer address data

Property	Description
Organization name	Name of the organization for the customer's postal address.
Name of contact person	Customer's contact person.
Address line 1-3	Customer's postal address.
Region	Region of the postal address
City	City of the postal address
Zip code	Zip code of the postal address

Defining categories for the inheritance of Google Workspace entitlements

In One Identity Manager, user accounts can selectively inherit entitlements. To do this, entitlements, and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables, enter your categories for the permissions. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the customer in the **Google Workspace > Customers** category.

2. Select the **Change main data** task.

3. Switch to the **Mapping rule category** tab.

4. Extend the relevant roots of a table.

5. To enable the category, double-click ⊗.

6. Enter a category name of your choice for user accounts and groups and products and SKUs in the login language that you use.

7. Save the changes.

Detailed information about this topic

- Inheritance of Google Workspace entitlements based on categories on page 116

Additional tasks for managing Google Workspace customers

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

Task	Theme
Google Workspace customers overview	Displaying the Google Workspace customer overview on page 126
Assign groups	Assigning Google Workspace groups directly to a customer on page 112
Define search criteria for identity assignment	Editing search criteria for automatic identity assignment on page 76
Edit synchronization project	Editing the synchronization project for a Google Workspace customer on page 126
Synchronize this object	Synchronizing single objects on page 45

Displaying the Google Workspace customer overview

To obtain an overview of a Google Workspace customer

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.

2. Select the customer in the result list.

3. Select the **Google Workspace customer overview** task.

Editing the synchronization project for a Google Workspace customer

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

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

To open an existing synchronization project in the Synchronization Editor:

1. In the Manager, select the **Google Workspace > Google Workspace customers** category.

2. Select the customer in the result list.

3. Select the **Change main data** task.

4. Select the **Edit synchronization project** task.

Related topics

- Customizing the synchronization configuration for Google Workspace on page 29

Google Workspace user accounts

Using One Identity Manager you can manage a customer's users. The user data for the registered users is represented in One Identity Manager as user accounts. You can use the user accounts to manage the user's permissions, for example, membership of Google Workspace groups or administrative permissions.

A user account can be linked to an identity in One Identity Manager. You can also manage user accounts separately from identities.

NOTE: It is recommended to use account definitions to set up user accounts for company identities. In this case, some of the main data described in the following is mapped through templates from identity main data.

NOTE: If identities are to obtain their user accounts through account definitions, the identities must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

Related topics

- Managing Google Workspace user accounts and identities on page 53
- Account definitions for Google Workspace user accounts on page 54
- Default project template for Google Workspace on page 189
- Editing main data of Google Workspace user accounts on page 128
- Managing Google Workspace entitlement assignments on page 102

Creating Google Workspace user accounts

To create a user account

1. In the Manager, select the **Google Workspace > User accounts** category.
2. Click ⬛ in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

Various communication data and organizational data can be assigned to user accounts, such as email addresses, website, information about the user's organization or relationships to other users.

To assign communication data to a user account

1. Select the required tabs on the main data form.
2. Click **Add**.

   This inserts a new row in the table.
3. Select this row and edit the main data.
4. Save the changes.

To edit communication data

1. Select the required tabs on the main data form.
2. In the table, select the row that you want to edit.
3. Edit the main data.
4. Save the changes.

To remove the assignment of communication data

1. Select the required tabs on the main data form.
2. In the table, select the row that you want to remove.
3. Click **Delete**.
4. Save the changes.

Detailed information about this topic

- General main data of Google Workspace user accounts on page 130
- Password data for Google Workspace user accounts on page 134
- Phone numbers for Google Workspace user accounts on page 135
- Addresses for Google Workspace user accounts on page 135
- Email addresses for Google Workspace user accounts on page 136
- External IDs for Google Workspace user accounts on page 137
- Instant messenger data for Google Workspace user accounts on page 137
- User details for Google Workspace user accounts on page 138
- Relationships of Google Workspace user accounts on page 139
- Websites of Google Workspace user accounts on page 139

Related topics

- Editing main data of Google Workspace user accounts on page 128
- Deleting and restoring Google Workspace user accounts on page 143

Editing main data of Google Workspace user accounts

To edit main data of a user account

1. In the Manager, select the **Google Workspace > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

Various communication data and organizational data can be assigned to user accounts, such as email addresses, website, information about the user's organization or relationships to other users.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
Google Workspace

Mapping Google Workspace objects in One Identity Manager

128

To assign communication data to a user account

1. Select the required tabs on the main data form.

2. Click **Add**.

   This inserts a new row in the table.

3. Select this row and edit the main data.

4. Save the changes.

To edit communication data

1. Select the required tabs on the main data form.

2. In the table, select the row that you want to edit.

3. Edit the main data.

4. Save the changes.

To remove the assignment of communication data

1. Select the required tabs on the main data form.

2. In the table, select the row that you want to remove.

3. Click **Delete**.

4. Save the changes.

Detailed information about this topic

- General main data of Google Workspace user accounts on page 130
- Password data for Google Workspace user accounts on page 134
- Phone numbers for Google Workspace user accounts on page 135
- Addresses for Google Workspace user accounts on page 135
- Email addresses for Google Workspace user accounts on page 136
- External IDs for Google Workspace user accounts on page 137
- Instant messenger data for Google Workspace user accounts on page 137
- User details for Google Workspace user accounts on page 138
- Relationships of Google Workspace user accounts on page 139
- Websites of Google Workspace user accounts on page 139

Related topics

- Creating Google Workspace user accounts on page 127
- Deleting and restoring Google Workspace user accounts on page 143
- Locking Google Workspace user accounts on page 141

General main data of Google Workspace user accounts

On the **General** tab, you enter the following main data:

Table 26: Additional main data of a user account

Property	Description
Identity	Identity that uses this user account.
	• An identity is already entered if the user account was generated by an account definition.
	• If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account.
	• If you create the user account manually, you can select an identity in the menu.
	The menu displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the **QER	Person| HideDeactivatedIdentities** configuration parameter.
	NOTE: If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.
	You can create a new identity for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click ➕ next to the input field and enter the required identity main data. Which login data is required depends on the selected identity type.
No link to an identity required	Specifies whether the user account is intentionally not assigned an identity. The option is automatically set if a user account is included in the exclusion list for automatic identity assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an identity (for example, if several identities use the user account).
	If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an identity can be filtered according to various criteria.
Not linked to an identity	Indicates why the **No link to an identity required** option is enabled for this user account. Possible values:

Property	Description
	• **By administrator**: The option was set manually by the administrator.
	• **By attestation**: The user account was attested.
	• **By exclusion criterion**: The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the user account was created.
	Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned identity and enters it in the corresponding fields in the user account.
	NOTE: The account definition cannot be changed once the user account has been saved.
	NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the identity. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (`XOrigin=1`).
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Google Workspace customer	Customer to which the user account belongs.
Unique ID	Google Workspace internal ID of the user account.
Gender	Gender of the user. Select a value from the menu.
Custom gender	User defined gender of the user.
Address me as	A human-readable string containing the proper way to refer to the user. Example: **he/him/his** or **they/them/their**
First name	User's first name.
Last name	User's last name.
Primary email address	Primary email address for the user account.

Property	Description
Google Workspace Organization	Google Workspace organization to which the user account belongs.
Creation time	Time at which the user account was created.
Deletion time	Time at which the user account was deleted. The user account can be restored within five days.
Risk index (calculated)	Maximum risk index value of all assigned entitlements. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of Google Workspace permissions to the user account. User accounts can selectively inherit permissions. To do this, entitlements, and user accounts are divided into categories.
	Select one or more categories from the menu.
Notes content type	Format of notes.
Notes	Text field for additional explanation.
Suspended	Specifies whether the user account is locked.
Suspension reason	Reason for the suspension of the user account.
Aliases	List of all alias email addresses that are set up for this user account.
Non editable aliases	List of all email addresses that cannot be changed. These email addresses do not belong to the primary domain or its subdomains.
Identity type	User account's identity type Permitted values are:

- **Primary identity**: Identity's default user account.
- **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.
- **Personalized administrator identity**: User account with administrative permissions, used by one identity.
- **Sponsored identity**: User account to use for a specific purpose. Training, for example.
- **Shared identity**: User account with administrative permissions, used by several identities. Assign all identities that use this user account.
- **Service identity**: Service account.

Property	Description
Groups can be inherited	Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests. • If you add an identity with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
Products and SKUs can be inherited	Specifies whether the user account can inherit products and SKUs through the linked identity. If the option is set, the user account inherits profiles through hierarchical roles, in which the identity is a member, or through IT Shop requests.
Admin roles assign- ments can be inherited	Specifies whether the user account can inherit admin role assign- ments through the linked identity. If the option is set, the user account inherits admin role assignments through hierarchical roles, in which the identity is a member, or through IT Shop requests.
Privileged user account.	Specifies whether this is a privileged user account.
Include in global address list	Specifies whether the user account is displayed in the global address list.
Included in allow list	Specifies whether the IP address for the user account is included in the allow list for emails.
Is super admin	Specifies whether the user account has super admin permissions.
Delegated admin- istrator	Specifies whether the user account has delegated admin permis- sions.
Google Workspace Agreement accepted	Specifies whether the user has initially logged in to Google Workspace and has accepted the Google Workspace (online) agreement.
Google mailbox is created	Specifies whether a Google mailbox has been created for the user account.
2-step verification is enrolled	Specifies whether **2-step verification** for the user account is enrolled.
2-step verification enforced	Specifies whether **2-step verification** for the user account is enforced.

Related topics

Password data for Google Workspace user accounts

On the **Password** tab, enter the password for logging in to Google Workspace.

Table 27: User account password data

Property	Description
Password	Password for the user account. The identity's central password can be mapped to the user account password. For more information about an identity's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.
	If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created.
	The password is deleted from the database after publishing to the target system.
	NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
Confirmation	Reconfirm password.
Last login	Time of the last login to Google Workspace.
Change password at next login	Specifies whether the user has to change their password the next time they log in.

Property	Description
Recovery email address	Email address for user account recovery.
Recovery phone number	Phone number for user account recovery. Enter the phone number in E.164 format.

Related topics

- Initial password for new Google Workspace user accounts on page 100

Phone numbers for Google Workspace user accounts

On the **Phone numbers** tab, you can edit user account email addresses.

Table 28: Phone number properties

Property	Description
Type	Type of the telephone number.
Custom type	User-defined type of the telephone number. If the **Custom** value is selected in the **Type** field, you can enter your own phone number type here.
Phone	Telephone number in any format.
Primary phone number	Specifies whether this is the primary telephone number.

Related topics

- Editing main data of Google Workspace user accounts on page 128

Addresses for Google Workspace user accounts

On the **Addresses** tab, you can edit the addresses of the user account.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
Google Workspace

Mapping Google Workspace objects in One Identity Manager

135

Table 29: Properties of an address

Property	Description
Type	Type of the address
Custom type	User-defined type of the address. If the **Custom** value is selected in the **Type** field, you can enter your own address type here.
Extended address	Extended address, for example, for entering a specific region
Address	Full address.
Street	The street name of the address.
Zip code	The zip code of the address.
City	The city of the address.
Region	Region, if required
Mailbox	Mailbox, if applicable
Country ID	Unique country ID.
Primary address	Specifies whether this address is the user's primary address.
Source is structured	Specifies whether the address is provided in a structured format.

Related topics

-

Email addresses for Google Workspace user accounts

On the **Email addresses** tab, you can edit user account email addresses.

Table 30: Properties of an email address

Property	Description
Type	Type of the email address.
Custom type	User-defined type of the email address. If the **Custom** value is selected in the **Type** field, you can enter your own email address type here.
Email address	Additional email addresses. This value can also be the user account's primary email address or an alias.

Related topics

- Editing main data of Google Workspace user accounts on page 128

External IDs for Google Workspace user accounts

On the **External IDs** tab, you can edit the external IDs of the user account.

Table 31: Properties of an external ID

Property	Description
Type	Type of the external ID.
Custom type	User-defined type of the external ID. If the **Custom** value is selected in the **Type** field, you can enter your own ID type type here.
External ID	Value of the external ID.

Related topics

- Editing main data of Google Workspace user accounts on page 128

Instant messenger data for Google Workspace user accounts

On the **Instant Messenger** tab, you can edit the Instant Messenger data for the user account.

Table 32: Instant messenger properties

Property	Description
Type	Type of Instant Messenger
Custom type	Type of Instant Messenger defined by the user If the **Custom** value is selected in the **Type** field, you can enter your own Instant Messenger type here.
Protocol	Network protocol of the Instant Messenger You can set a custom protocol or a standard protocol.
Custom protocol	If the **Custom** value is selected in the **Protocol** field, you can enter your own protocol type here.

Property	Description
Network ID of the Instant Messenger	Network ID of the Instant Messenger.
Primary Instant Messenger	Specifies whether this is the primary Instant Messenger.

Related topics

Editing main data of Google Workspace user accounts on page 128

User details for Google Workspace user accounts

On the **Organizations** tab, you can edit various organization data for the user account.

Table 33: Properties of user details

Property	Description
Type	Type of the organization.
Custom type	User-defined type of the organization. If the **Unknown** value is selected in the **Type** field, you can enter your own organization type here.
Organization name	Name of the organization for which the user details are being maintained.
Cost center	A cost center within the organization.
Department	A department within the organization.
Domain	Domain to which the organization belongs.
Location	Location of the organization.
Icon	Text symbol for the organization, for example **GOOG** for Google.
Title	Title of the user withing the organization, for example **Member** or **Engineer**.
Description	Description of user details.
Primary organization	Specifies whether this organization is the user's primary organization.

Related topics

- Editing main data of Google Workspace user accounts on page 128

Relationships of Google Workspace user accounts

On the **Relations** tab, you can edit the relationships of the user account.

Table 34: Properties of a relationship

Property	Description
Type	Type of the relationship.
Custom type	User-defined type of the relationship. If the **Custom** value is selected in the **Type** field, you can enter your own relation type here.
Relation	Primary email address of the user to whom the relationship exists.

Related topics

- Editing main data of Google Workspace user accounts on page 128

Websites of Google Workspace user accounts

On the **Websites** tab, you can edit the websites of the user account.

Table 35: Properties of a website

Property	Description
Type	Type or purpose of the website.
Custom type	User-defined type of the website. If the **Custom** value is selected in the **Type** field, you can enter your own website type here.
Website URL	URL of the website.
Primary website.	Specifies whether this is the primary website.

Related topics

- Editing main data of Google Workspace user accounts on page 128

Additional tasks for managing Google Workspace user accounts

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

Task	Topic
Overview of Google Workspace user accounts	Displaying the Google Workspace user account overview on page 140
Assign groups	Assigning Google Workspace entitlements directly to a user account on page 111
Assign products and SKUs	Assigning Google Workspace entitlements directly to a user account on page 111
Admin role assignments	Assigning Google Workspace entitlements directly to a user account on page 111
Assigning extended properties	Assigning extended properties to Google Workspace user accounts on page 140
Synchronize object	Synchronizing single objects on page 45
Change Google Workspace organization	Moving Google Workspace user accounts to a different organization on page 141

Displaying the Google Workspace user account overview

To obtain an overview of a user account

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list.

3. Select the **Google Workspace user account overview** task.

Assigning extended properties to Google Workspace user accounts

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

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

To specify extended properties for a user account

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list.

3. Select **Assign extended properties**.

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

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

   ### To remove an assignment

   - Select the extended property and double-click ⊘.

5. Save the changes.

Moving Google Workspace user accounts to a different organization

Within the organizational hierarchy of a Google Workspace customer, user accounts can be moved to a different organization.

To move a user account to another organization

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list and run the **Change main data** task.

3. Select the **Change Google Workspace organizational unit** task.

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

5. Select the new organization from the **Google Workspace organization unit** menu on the **General** tab.

6. Save the changes.

Locking Google Workspace user accounts

The way you lock user accounts depends on how they are managed.

Scenario: The user accounts are linked to identities and are managed through account definitions.

User accounts managed through account definitions are locked when the identity is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the GAPUser.IsSuspended column.

Scenario: The user accounts are linked to identities. No account definition is applied.

User accounts managed through user account definitions are locked when the identity is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the identity's user accounts are locked when the identity is permanently or temporarily disabled.
- If the configuration parameter is not set, the identity's properties do not have any effect on the associated user accounts.

To lock the user account when the configuration parameter is disabled

1. In the Manager, select the **Google Workspace > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Locked** option.
5. Save the changes.

Scenario: The user accounts are not linked to identities.

To lock a user account that is no longer linked to an identity

1. In the Manager, select the **Google Workspace > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Locked** option.
5. Save the changes.

To unlock a user account

1. In the Manager, select the **Google Workspace > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Disable the **Locked** option on the **General** tab.
5. Save the changes.

For more information about deactivating and deleting identities and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Account definitions for Google Workspace user accounts on page 54
- Creating manage levels on page 60

Deleting and restoring Google Workspace user accounts

NOTE: As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

In the Manager, you can delete a user account that was not created using an account definition in the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

For more information about deactivating and deleting identities and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

To delete a user account that is not managed using an account definition

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list.

3. Click ![icon] in the result list.

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

To restore a user account

1. In the Manager, select the **Google Workspace > User accounts** category.

2. Select the user account in the result list.

3. Click ![icon] in the result list.

Related topics

- Locking Google Workspace user accounts on page 141
- Transferring user data to a different Google Workspace user account on page 144
- Specifying deferred deletion for Google Workspace user accounts on page 86

Transferring user data to a different Google Workspace user account

When a user account is deleted, various user data can be transferred to a different user account. After the deletion delay has expired, the data transfer is first initiated in the Google Workspace environment. As soon as the data transfer has been successfully completed in the target system, the user account is permanently deleted.

Prerequisites

- Data transfer is approved for the customer. To enable this, the **Transfer user data before delete** setting must be enabled, or the `CP_TransferUserDataBeforeDelete` variable is set to **True**.

- A manager has been assigned to the identity to whom the deleted user account is linked.

  - OR -

  The deleted user account has a relationship of the **Manager** type.

- The manager's email address belongs to the primary domain of the customer to which the deleted user account belongs.

- In the event that no valid email address can be determined in this way, a valid default email address is defined. This is specified in the target system connection using the **Default email address for data transfer** setting or in the `CP_ DefaultDataTransferTargetEmail` variable.

Detailed information about this topic

- Advanced settings for the system connection to Google Workspace on page 33
- General main data of Google Workspace user accounts on page 130
- Relationships of Google Workspace user accounts on page 139

Related topics

- Deleting and restoring Google Workspace user accounts on page 143

Google Workspace groups

Users of Google Workspace can use groups to exchange information or organize meetings. This information is only made available to the members of a group. In
One Identity Manager, you can create and edit groups and manage group members.

Creating Google Workspace groups

To create a group

1. In the Manager, select the **Google Workspace > Groups** category.
2. Click ⬛ in the result list.
3. On the main data form, edit the main data of the group.
4. Save the changes.

Detailed information about this topic

- General main data of Google Workspace groups on page 146
- Additional settings for Google Workspace groups on page 147

Related topics

- Entering main data of Google Workspace groups on page 145
- Deleting Google Workspace groups on page 154

Entering main data of Google Workspace groups

To edit group main data

1. In the Manager, select the **Google Workspace > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Detailed information about this topic

- General main data of Google Workspace groups on page 146
- Additional settings for Google Workspace groups on page 147

Related topics

- Creating Google Workspace groups on page 145
- Deleting Google Workspace groups on page 154

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
Google Workspace

Mapping Google Workspace objects in One Identity Manager

145

General main data of Google Workspace groups

On the **General** tab, edit the following main data.

Table 36: Entering main data of a group

Property	Description
Google Workspace customer	Customer to which the group belongs.
Group ID	Unique ID of the group.
Group name	Name of the group.
Email address	Group's email address
Service item	Service item data for requesting the group through the IT Shop.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range **0** to **1**. This input field is only visible if the **QER	CalculateRiskIndex** configuration parameter is activated. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
Is admin created	Specifies whether the group was created by an administrator. If this option is disable, the group was created by a user.
Aliases	List of additional email addresses under which emails can be sent to the group.
Non editable aliases	List of all email addresses that cannot be changed. These email addresses do not belong to the primary domain or its subdomains.

Related topics

- Inheritance of Google Workspace entitlements based on categories on page 116
- Adding Google Workspace entitlements to the IT Shop on page 108

Additional settings for Google Workspace groups

On the **Settings** tab, edit the following main data.

Table 37: Additional settings for groups

Property	Description
Contact owners	Specifies who is allowed to contact the group owners.
View members	Defines who can see the members of the group.
View topics	Permissions for showing group topics.
Publish posts	Specifies who can post messages to the group. If **None** is selected, then the group is deactivated and archived. No user can post messages to the group.
Manage members	Specifies who is allowed to manage memberships.
Join the group	Specifies which users are permitted to become members of the group. You can only select the **Public** value if the **Allow external members** option is set.
Allow external members	Specifies whether users from other domains are permitted as members. If this option is set, in the **Join the group** field, define which users are permitted to become members.
Language	Name of the language.
Moderate content	Specifies who can moderate content.
Group visibility	Specifies for which users the group is visible.
Spam messages	Specifies how to handle messages suspected of being spam. Possible values: • **Allow**: Post in the group without moderation. • **Moderate**: Send to the moderation queue and send a message to the moderators. • **Silently moderate**: Send to the moderation queue, but do not send a message to the moderators.

Property	Description
	• **Reject**: Reject immediately.
Post replies	Specifies who receives the replies to posts. If **Use a custom address to send replies to** is selected, a valid email address must be entered in the **Post replies to** field.
Send replies to	Email address to which the replies to posts are sent. If **Use a custom address to send replies to** is selected in the **Post replies** field, you must enter a valid email address.
Notify authors when their messages are rejected	Specifies whether the author of a post is informed if their post is rejected by the moderators. If this option is set, enter a notification text in the **Rejected author notification** field.
Rejected author notific-ation	Notification that is sent to authors if their post is rejected. The maximum text length is 10,000 characters. Notifications are only sent if the **Notify authors when moderators reject their messages** option is set.
Max message size	Maximum size of the messages that can be sent to this group in bytes.
Allow web posting	Specifies whether users are permitted to post in the group from the web interface. If this option is disabled, the users can only use GMail for communication with the group.
Post as the group	Specifies whether group members are permitted to use the email address of the group to post posts.
Archive messages to the group	Specifies whether messages sent to the group are archived.
Include in global address list	Specifies whether the group is displayed in the global address list.

Additional tasks for managing Google Workspace groups

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

Task	Topic
Overview of Google Workspace	Displaying the Google Workspace group overview on page 149

Task	Topic
Groups	
Assigning extended properties	Assigning extended properties to Google Workspace groups on page 150
Assigning group managers	Assigning group managers to Google Workspace groups on page 150
Assigning group owners	Assigning group owners to Google Workspace groups on page 151
Assign external email addresses	Assigning external users to a Google Workspace group on page 119
assign user accounts	Assigning Google Workspace user accounts directly to an entitlement on page 110
Assign groups	Assigning Google Workspace groups to Google Workspace groups on page 153
Assign customer as member	Assigning Google Workspace customers directly to a group on page 113
Exclude groups	Effectiveness of Google Workspace entitlement assignments on page 113
Assign system roles	Adding Google Workspace entitlements to system roles on page 107
Assign business roles	Assigning Google Workspace entitlements to business roles on page 106
Assign organizations	Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
Add to IT Shop	Adding Google Workspace entitlements to the IT Shop on page 108
Synchronize object	Synchronizing single objects on page 45

Displaying the Google Workspace group overview

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

To obtain an overview of a group

1. In the Manager, select the **Google Workspace > Groups** category.
2. Select the group in the result list.
3. Select the **Google Workspace group overview** task.

Assigning extended properties to Google Workspace groups

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

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

To specify extended properties for a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select **Assign extended properties**.

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

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

   ### *To remove an assignment*

   - Select the extended property and double-click ⊘.

5. Save the changes.

Assigning group managers to Google Workspace groups

Define the group managers for a group. Both user accounts and external users can be assigned as group managers.

To specify user accounts as group managers of a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group managers** task.

4. In the **Table** menu, select the **Google Workspace user accounts** table.

5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   ### *To remove an assignment*

   - Select the user account and double-click ⊘.

6. Save the changes.

In order to assign external users as group managers, the **Allow external members** option must be set for this group.

To specify external users as group managers of a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group managers** task.

4. In the **Table** menu, select the **Google Workspace external email addresses** table.

5. In the **Add assignments** pane, assign the external email addresses.

   TIP: In the **Remove assignments** pane, you can remove external email addresses.

   ### *To remove an assignment*

   - Select the external email address and click ⊘.

6. Save the changes.

NOTE: By default, Google Workspace customers and groups cannot be assigned as group managers. However, these assignments are possible in the Google admin console. If these assignments exist in the target system, they are imported into the One Identity Manager database during synchronization. Existing assignments can be displayed in the Manager.

To check whether groups are assigned to a group as the group manager

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group managers** task.

4. In the **Table** menu, select the **Google Workspace groups** table.

   In the **Remove assignments** pane, all assigned groups are displayed.

To check whether the customer is assigned to a group as the group manager

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group managers** task.

4. In the **Table** menu, select the **Google Workspace customers** table.

   In the **Remove assignments** pane, the assigned customer is displayed.

In the Manager, customers and groups cannot be assigned as group managers.

Assigning group owners to Google Workspace groups

Define the group owners for a Google Workspace group. Both user accounts and external users can be assigned as group owners.

To define user accounts as group owners of a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group owners** task.

4. In the **Table** menu, select the **Google Workspace user accounts** table.

5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   #### To remove an assignment

   - Select the user account and double-click ✅.

6. Save the changes.

In order to assign external users as group owners, the **Allow external members** option must be set for this group.

To specify external users as group owners of a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group owners** task.

4. In the **Table** menu, select the **Google Workspace external email addresses** table.

5. In the **Add assignments** pane, assign the external email addresses.

   TIP: In the **Remove assignments** pane, you can remove external email addresses.

   #### To remove an assignment

   - Select the external email address and click ✅.

6. Save the changes.

NOTE: By default, Google Workspace customers and groups cannot be assigned as group owners. However, these assignments are possible in the Google admin console. If these assignments exist in the target system, they are imported into the One Identity Manager database during synchronization. Existing assignments can be displayed in the Manager.

To check whether groups are assigned to a group as the group owner

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group owners** task.

4. In the **Table** menu, select the **Google Workspace groups** table.

   In the **Remove assignments** pane, all assigned groups are displayed.

To check whether the customer is assigned to a group as the group owner

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign group owners** task.

4. In the **Table** menu, select the **Google Workspace customers** table.

   In **Remove assignments**, the assigned customer is displayed.

In the Manager, customers and groups cannot be assigned as group owners.

Assigning Google Workspace groups to Google Workspace groups

Google Workspace groups can themselves be members of other Google Workspace groups. This means that the groups can be hierarchically structured.

To assign groups directly to a group as members

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign groups** task.

4. Select the **Has members** tab.

5. Assign child groups in **Add assignments**.

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

   To remove an assignment
   - Select the group and double-click ⊘.

6. Save the changes.

To add a group as a member of other groups

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Select the **Assign groups** task.

4. Select the **Is member of** tab.

5. In the **Add assignments** pane, assign parent groups.

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

To remove an assignment

- Select the group and double-click ⊘.

6. Save the changes.

Related topics

- Assigning Google Workspace user accounts directly to an entitlement on page 110

Deleting Google Workspace groups

Groups are deleted permanently from the One Identity Manager database and from Google Workspace.

To delete a group

1. In the Manager, select the **Google Workspace > Groups** category.

2. Select the group in the result list.

3. Click ⊠ in the result list.

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

Google Workspace products and SKUs

Products and related services, as well as the licenses required for login, are represented in One Identity Manager as products and SKUs (Stock-Keeping-Units). To provide users with the required permissions to log on to Google Workspace, assign the product SKUs to the user accounts.

Editing main data of Google Workspace products and SKUs

To edit the main data of a product SKU

1. In the Manager, select the **Google Workspace > Products and SKUs** category.

2. Select the product SKU in the result list.

3. Select the **Change main data** task.

4. Edit the main data of the product SKU.

5. Save the changes.

Detailed information about this topic

General main data of Google Workspace products and SKUs

For products and SKUs, edit the following main data.

Table 38: General main data of a product SKU

Property	Description
Google Workspace customer	Customer to which the product SKU belongs.
Product name	Display name of the product.
SKU name	Display name of the SKU.
Service item	Enter a service item for requesting the product SKU through the IT Shop.
IT Shop	Specifies whether the product SKU can only be requested through the IT Shop. The product SKU can be requested by your employees through the Web Portal and allocated by defined approval processes. The product SKU can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the product SKU can only be requested through the IT Shop. The product SKU can be requested by your employees through the Web Portal and allocated by defined approval processes. Direct assignment of the product SKU to hierarchical roles or user accounts is not permitted.
Risk index	Value for evaluating the risk of assignments to the product SKU. Enter a value between **0** and **1**. This field is only visible if the **QER	CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for passing on the product SKU to user accounts. Product SKUs can be selectively passed on to user accounts. To do this, the product SKUs and user accounts are divided into categories. Select one or more categories from the menu.

Related topics

Additional tasks for managing Google Workspace products and SKUs

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

Task	Theme
Overview of the Google Workspace product and the SKU	Displaying the Google Workspace products and SKUs overview on page 156
Assigning extended properties	Assigning extended properties to Google Workspace products and SKUs on page 157
assign user accounts	Assigning Google Workspace user accounts directly to an entitlement on page 110
Assign system roles	Adding Google Workspace entitlements to system roles on page 107
Assign business roles	Assigning Google Workspace entitlements to business roles on page 106
Assign organizations	Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
Add to IT Shop	Adding Google Workspace entitlements to the IT Shop on page 108
Synchronize object	Synchronizing single objects on page 45

Displaying the Google Workspace products and SKUs overview

You use this task to obtain an overview of the most important information for a product SKU.

To obtain an overview of a product SKU

1. In the Manager, select the **Google Workspace > Products and SKUs** category.
2. Select the product SKU in the result list.

3. Select the **Google Workspace product and SKU overview** task.

Assigning extended properties to Google Workspace products and SKUs

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

To specify extended properties for a product SKU

1. In the Manager, select the **Google Workspace > Products and SKUs** category.

2. Select the product SKU in the result list.

3. Select the **Assign extended properties** task.

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

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

   To remove an assignment

   - Select the extended property and double-click ✓.

5. Save the changes.

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

Google Workspace organizations

Organizations are used to define the settings for Google Workspace users. Each customer has one parent organization. You can set up additional organizations below this organization and therefore create an organizational hierarchy. Child organizations inherit the settings of the relevant parent organization. User accounts are assigned to exactly one organization.

Creating Google Workspace organizations

To create an organization

1. In the Manager, select **Google Workspace > Organizations**.

2. Click ⊞ in the result list.

3. On the main data form, edit the main data of the organization.

4. Save the changes.

Related topics

Editing main data of Google Workspace organizations

To edit organization main data

1. In the Manager, select **Google Workspace > Organizations**.
2. Select the organization from the result list.
3. Select the **Change main data** task.
4. Edit the main data of the organization.
5. Save the changes.

Related topics

General main data of Google Workspace organizations

For organizations, edit the following main data:

Table 39: General main data of organizations

Property	Description
Google Workspace customer	Customer to which the organization belongs.
Organization ID	ID of the organization
Organization name	Display name of the organization
Full path	Full path of the organization.
Parent organization	The parent organization.
Description	Text field for additional explanation.

ONE IDENTITY
by Quest

One Identity Manager 9.2 Administration Guide for Connecting to
Google Workspace

Mapping Google Workspace objects in One Identity Manager

158

Additional tasks for managing Google Workspace organizations

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

Task	Theme
Overview of the Google Workspace organization	Displaying the Google Workspace organizations overview on page 159
Synchronize object	Synchronizing single objects on page 45
Changing parent organizations	Moving Google Workspace organizations on page 159

Displaying the Google Workspace organizations overview

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

To obtain an overview of an organization

1. In the Manager, select **Google Workspace > Organizations**.
2. Select the organization from the result list.
3. Select the **Google Workspace organization overview** task.

Moving Google Workspace organizations

Child organizations can be moved within an organizational hierarchy. To move a child organization, assign a different parent organization to the child organization.

To move an organization

1. In the Manager, select **Google Workspace > Organizations**.
2. Select the organization from the result list.
3. Select the **Change main data** task.
4. Select the **Change parent organizational unit** task.
5. Confirm the security prompt with **Yes**.
6. Select the new organization from the **Parent organization** menu.
7. Save the changes.

Deleting Google Workspace organizations

To delete an organization

1. In the Manager, select **Google Workspace > Organizations**.

2. Select the organization from the result list.

3. Click ⊠.

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

The organization is permanently deleted from the One Identity Manager database and from Google Workspace.

Google Workspace domains

In Google Workspace, the primary domain of a customer and additional Internet domains are mapped as One Identity Manager domains. Domains are imported into the One Identity Manager database during synchronization. You cannot edit their properties. Changes to the object properties of individual domains can be transferred by single object synchronization.

To display the properties of a domain:

1. In the Manager, select the **Google Workspace > Domains** category.

2. Select the domain in the result list.

3. Select the **Change main data** task.

To obtain an overview of a domain

1. In the Manager, select the **Google Workspace > Domains** category.

2. Select the domain in the result list.

3. Select the **Google Workspace domain overview** task.

Related topics

- Synchronizing single objects on page 45

Google Workspace domain aliases

Domain aliases provide the users of a primary domain with additional email addresses. Domain aliases are imported into the One Identity Manager database during synchronization. You cannot edit their properties. Changes to the object properties of individual domain privileges can be transferred by single object synchronization.

To display the properties of a domain alias

1. In the Manager, select the **Google Workspace > Domain aliases** category.

2. Select a domain alias in the result list.

3. Select the **Change main data** task.

To obtain an overview of a domain alias

1. In the Manager, select the **Google Workspace > Domain aliases** category.

2. Select a domain alias in the result list.

3. Select the **Google Workspace domain alias overview** task.

Related topics

- Synchronizing single objects on page 45

Google Workspace admin roles

Admin roles are used to grant users administrative privileges in Google Workspace. You can create custom admin roles in One Identity Manager. To ensure that the users receive the privileges, assign the admin roles to user accounts.

Creating Google Workspace admin roles

To create an admin role

1. In the Manager, select the **Google Workspace > Admin roles** category.

2. Click ➕ in the result list.

3. On the main data form, edit the main data of the admin role.

4. Save the changes.

Related topics

- General main data of Google Workspace admin roles on page 162
- Editing main data of Google Workspace admin roles on page 162

Editing main data of Google Workspace admin roles

To edit the main data of an admin role

1. In the Manager, select the **Google Workspace > Admin roles** category.

2. Select the admin role in the result list.

3. Select the **Change main data** task.

4. Edit the main data of the admin role.

5. Save the changes.

Related topics

- General main data of Google Workspace admin roles on page 162
- Creating Google Workspace admin roles on page 161

General main data of Google Workspace admin roles

For admin roles, edit the following main data:

Table 40: General main data of an admin role

Property	Description
Google Workspace customer	Customer to which the admin role belongs.
Role identifier	Unique ID of the role. For new admin roles, the ID is allocated in the target system.
Role name	Display name of the role
Description	Text field for additional explanation.
Is super admin	Specifies whether the admin role is a super admin role.
Is system role	Specifies whether the admin role is a predefined admin role.

Additional tasks for managing Google Workspace admin roles

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

Task	Theme
Google Workspace admin role overview	Overview of Google Workspace admin roles on page 163
Assign admin privileges	Assigning admin privileges to Google Workspace admin roles on page 163
Synchronize object	Synchronizing single objects on page 45

Overview of Google Workspace admin roles

You use this task to obtain an overview of the most important information for an admin role.

To obtain an overview of an admin role

1. In the Manager, select the **Google Workspace > Admin roles** category.

2. Select the admin role in the result list.

3. Select the **Google Workspace admin role overview** task.

Assigning admin privileges to Google Workspace admin roles

Assign all the privileges to the custom admin roles that you want the user accounts to receive through this admin role. You cannot edit assignments to admin roles that are labeled as system roles.

To assign admin privileges to a custom admin role

1. In the Manager, select the **Google Workspace > Admin roles** category.

2. Select the admin role in the result list.

3. Select the **Assign admin privileges** task.

4. In the **Add assignments** pane, assign the admin privileges.

   TIP: You can remove the assignment of admin privileges in **Remove assignments**.

   ### *To remove an assignment*
   - Select the admin privilege and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Google Workspace admin privileges to admin roles on page 165

Deleting Google Workspace admin roles

You can delete user-defined admin roles in the Manager that are not used in admin role assignments. System roles cannot be deleted.

To delete a custom admin role

1. In the Manager, select the **Google Workspace > Admin roles** category.

2. Select the admin role in the result list.

3. Click 📄.

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

The admin role is permanently deleted from the One Identity Manager database and from Google Workspace.

Google Workspace admin privileges

Admin privileges represent the administrative privileges that user accounts receive through the assigned admin roles. Admin privileges are imported into the One Identity Manager database during synchronization. You cannot edit their properties. Changes to the object properties of individual admin privileges can be transferred by single object synchronization.

Display main data of Google Workspace admin privileges

To display the main data of an admin privilege

1. In the Manager, select the **Google Workspace > Admin privileges** category.

2. Select the admin privileges in the result list.

3. Select the **Change main data** task.

Related topics

- Overview of Google Workspace admin privileges on page 165

Additional tasks for managing Google Workspace admin privileges

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

Task	Theme
Overview of Google Workspace admin privileges	Overview of Google Workspace admin privileges on page 165
Admin role assignments	Assigning Google Workspace admin privileges to admin roles on page 165
Synchronize object	Synchronizing single objects on page 45

Overview of Google Workspace admin privileges

You use this task to obtain an overview of the most important information for an admin privilege.

To obtain an overview of admin privileges

1. In the Manager, select the **Google Workspace > Admin privileges** category.

2. Select the admin privileges in the result list.

3. Select the **Google Workspace admin privilege overview** task.

Assigning Google Workspace admin privileges to admin roles

You assign an admin privilege to various custom admin roles. You cannot edit assignments of admin roles that are labeled as system roles.

To assign admin privileges to custom admin roles

1. In the Manager, select the **Google Workspace > Admin privileges** category.

2. Select the admin privileges in the result list.

3. Select the **Assign admin role** task.

4. In the **Add assignments** pane, assign the admin roles.

   TIP: You can remove the assignment of admin roles in **Remove assignments**.

To remove an assignment

- Select the admin role and double-click ✓.

5. Save the changes.

Related topics

- Assigning admin privileges to Google Workspace admin roles on page 163

Google Workspace admin role assignments

Administrative privileges can be limited to individual organizations. To enable this, assign the admin roles to organizations. User accounts that are assigned this type of admin role can use the related administrative privileges only in the assigned organization.

Creating Google Workspace admin role assignments

To assign an organization to an admin role

1. In the Manager, select the **Google Workspace > Admin role assignments** category.

2. Click ⬛ in the result list.

3. On the main data form, edit the assignment.

   - Select the required admin role from the **Admin role** menu.

   - Select the required organization from the **Google Workspace organization** menu.

4. Save the changes.

Additional tasks for managing Google Workspace admin role assignments

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

Task	Theme
Google Workspace admin role assignment overview	Overview of Google Workspace admin role assignments on page 167
assign user accounts	Assigning Google Workspace user accounts directly to an entitlement on page 110
Assigning extended properties	Assigning extended properties to Google Workspace admin role assignments on page 167
Assigning system roles	Adding Google Workspace entitlements to system roles on page 107
Assign business roles	Assigning Google Workspace entitlements to business roles on page 106
Assign organizations	Assigning Google Workspace entitlements to departments, cost centers, and locations on page 105
Adding to the IT Shop	Adding Google Workspace entitlements to the IT Shop on page 108
Synchronize object	Synchronizing single objects on page 45

Overview of Google Workspace admin role assignments

You use this task to obtain an overview of the most important information for an admin role assignment.

To obtain an overview of admin role assignments

1. In the Manager, select the **Google Workspace > Admin role assignments** category.

2. Select the admin role assignment in the result list.

3. Select the **Google Workspace admin role assignment overview** task.

Assigning extended properties to Google Workspace admin role assignments

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

To specify extended properties for an admin role assignment

1. In the Manager, select the **Google Workspace > Admin role assignments** category.

2. Select the admin role assignment in the result list.

3. Select **Assign extended properties**.

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

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

   To remove an assignment

   - Select the extended property and double-click ✅.

5. Save the changes.

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

Deleting Google Workspace admin role assignments

To delete an admin role assignment

1. In the Manager, select the **Google Workspace > Admin role assignments** category.

2. Select the admin role assignment in the result list.

3. Click 🗙.

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

The admin role is permanently deleted from the One Identity Manager database and from Google Workspace.

Google Workspace external email addresses

Google Workspace allows external users that do not have any user accounts in the customer, to have membership in Google Workspace groups. External users are represented by an external email address. They can be assigned as members, owners, or managers to groups that allow external members.

Assigning Google Workspace external email addresses to customers

In the Manager, external email addresses can be assigned to a Google Workspace customer.

To assign an external email address to a customer

1. In the Manager, select the **Google Workspace > External email addresses**.
2. Click in the result list.
3. Enter the following main data.
   - **Google Workspace Customer**: Select the customer from the menu.
   - **Email address**: External user's email address.
4. Save the changes.

Related topics

- Displaying the Google Workspace external email address overview on page 169
- Assigning Google Workspace groups to an external user on page 118

Additional tasks for managing Google Workspace external email addresses

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

Task	Theme
Google Workspace external email address overview	Displaying the Google Workspace external email address overview on page 169
Assign groups	Assigning Google Workspace groups to an external user on page 118

Displaying the Google Workspace external email address overview

Use this task to obtain an overview of the most important information about an external email address.

To obtain an overview of an external email address

1. In the Manager, select the **Google Workspace > External email addresses**.

2. Select the external email address in the result list.

3. Select the **Google Workspace external email address overview** task.

Related topics

- Assigning Google Workspace external email addresses to customers on page 169
- Additional tasks for managing Google Workspace external email addresses on page 169

Deleting Google Workspace external email addresses

To delete an external email address

1. In the Manager, select the **Google Workspace > External email addresses**.

2. Select the external email address in the result list.

3. Click ⌧.

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

The external email address is permanently deleted from the One Identity Manager database and assignments to groups in Google Workspace are removed.

Reports about Google Workspace objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for Google Workspace environments.

Table 41: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.

Report	Published for	Description
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	group Product and SKU	This report finds all roles containing identities who have the selected system entitlement.
Show overview	group Product and SKU Admin role assignment	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group Product and SKU Admin role assignment	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	group Product and SKU Admin role assignment	This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts overview (incl. history)	Organization Google Workspace customer	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show system entitlements overview (incl. history)	Organization Google Workspace customer	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Google Workspace customer	This report finds all roles containing identities with at least one user account in the selected target system.

Table 42: Additional reports for the target system

Report	Description
Google Workspace user account and group administration	This report contains a summary of user account and permission assignment in all customer environments. You can find the report in the **My One Identity Manager > Target system overviews** category.
Data quality summary for Google Workspace user accounts	This report contains different evaluations of user account data quality in all customer environments. You can find the report in the **My One Identity Manager > Data quality analysis** category.

Handling of Google Workspace objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and identities

  An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized identity, such as a manager.

- Managing entitlement assignments

  When an entitlement is assigned to an IT Shop shelf, the Google Workspace entitlement can be requested by the customer in the Web Portal. The request undergoes a defined approval process. The entitlement is not assigned until it has been approved by an authorized identity.

  In the Web Portal, managers and administrators of organizations can assign Google Workspace entitlements to the departments, cost centers, or locations for which they are responsible. The entitlements are inherited by all persons who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, managers and administrators of business roles in the Web Portal can assign Google Workspace entitlements to the business roles for which they are responsible. The entitlements are inherited by all persons who are members of these business roles.

  If the System Roles Module is available, supervisors of system roles in the Web Portal can assign Google Workspace entitlements to the system roles. The entitlements are inherited by all persons to whom these system roles are assigned.

- Attestation

  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

  If the Compliance Rules Module is available, you can define rules that identify the invalid entitlement assignments and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check rule violations and to grant exception approvals.

  If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

  You can use the risk index of Google Workspace entitlements to evaluate the risk of entitlement assignments for the company.One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the identities, user accounts, and their entitlements and risks.

For more information about the named topics, see Assigning Google Workspace entitlements to user accounts in One Identity Manager on page 103 and refer to the following guides:

- One Identity Manager Web Designer Web Portal User Guide
- One Identity Manager Attestation Administration Guide
- One Identity Manager Compliance Rules Administration Guide
- One Identity Manager Company Policies Administration Guide
- One Identity Manager Risk Assessment Administration Guide

Basic configuration data for managing a Google Workspace customer

To manage a Google Workspace customer in One Identity Manager, the following basic data is relevant.

- Account definitions

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

  For more information, see Account definitions for Google Workspace user accounts on page 54.

- Password policies

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the identities' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

  Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

  For more information, see Password policies for Google Workspace user accounts on page 88.

- Target system types

  Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

  For more information, see Post-processing outstanding objects on page 46.

- Servers

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

  For more information, see Job server for Google Workspace-specific process handling on page 176.

- Target system managers

  A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all Google Workspace objects in One Identity Manager.

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

  For more information, see Target system managers for Google Workspace customers on page 181.

Job server for Google Workspace-specific process handling

In order to handle target system specific processes in One Identity Manager, the synchronization server and its server functionality must be declared. You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.

- In the Manager, select an entry for the Job server in the **Google Workspace > Basic configuration data > Server** category and edit the Job server's main data.

  Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

NOTE: One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

Related topics

- System requirements for the Google Workspace synchronization server on page 19

Editing Google Workspace Job servers

Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

To edit a Job server and its functions

1. In the Manager, select the **Google Workspace > Basic configuration data > Server** category.

2. Select the Job server entry in the result list.

3. Select the **Change main data** task.

4. Edit the Job server's main data.

5. Select the **Assign server functions** task and specify server functionality.

6. Save the changes.

Detailed information about this topic

General main data of Job servers

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

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

Table 43: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: `<Name of servers>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs**

Property	Meaning
	to cluster properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported.
	If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled.
	This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.

Property	Meaning
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

Specifying server functions

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

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

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

Table 44: Permitted server functions

Server function	Remark
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks.
	The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.
	Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Google Workspace connector	Server on which the Google Workspace connector is installed. This server synchronizes the Google Workspace target system.

Related topics

- General main data of Job servers on page 177

Target system managers for Google Workspace customers

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all Google Workspace objects in One Identity Manager.

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

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

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates identities to be target system administrators.

2. These target system administrators add identities to the default application role for target system managers.

   Target system managers with the default application role are authorized to edit all the customer systems in One Identity Manager.

3. 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 customers.

Table 45: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Google Workspace** 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. • Edit password policies for the target system. • Prepare entitlements to add to the IT Shop. • Can add identities that do not have the **Primary identity** identity type.

User	Tasks

- Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.

- Edit the synchronization's target system types and outstanding objects.

- Authorize other 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 the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)

2. Select the **One Identity Manager Administration > Target systems > Administrators** category.

3. Select the **Assign identities** task.

4. Assign the identity and save the changes.

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

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).

2. Select the **One Identity Manager Administration > Target systems > Google Workspace** category.

3. Select the **Assign identities** task.

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 in to the Manager as a target system manager.

2. Select the application role in the **Google Workspace > Basic configuration data > Target system managers** category.

3. Select the **Assign identities** task.

4. Assign the identities you want and save the changes.

To specify target system managers for individual customers

1. Log in to the Manager as a target system manager.

2. Select the **Google Workspace > Customers** category.

3. Select the customer in the result list.

4. Select the **Change main data** task.

5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

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

   a. Enter the application role name and assign the **Target systems | Google Workspace** parent application role.

   b. Click **OK** to add the new application role.

6. Save the changes.

7. Assign identities to this application role who are permitted to edit the customer in One Identity Manager.

Related topics

- One Identity Manager users for managing a Google Workspace customer on page 11
- General main data of Google Workspace customers on page 122

Troubleshooting the connection to a Google Workspace customer

Newly added Google Workspace user accounts are marked as outstanding

If the One Identity Manager database is synchronized shortly after provisioning new user accounts in the customer, these user accounts might be marked as outstanding in One Identity Manager (or deleted, depending on the configuration of the synchronization). This error only occurs if a scope has been defined in the synchronization project for the target system.

Probable reason

Adding new user account in Google Workspace takes about 24 hours. If synchronization with the One Identity Manager database is started within these 24 hours, the error described can occur.

Solution

To prevent this error

- Avoid declaring a scope for this target system.

If a scope is required

1. Configure the user account synchronization so that objects that do not exist in One Identity Manager are marked as outstanding.

2. If the error occurs, run a target system comparison.

   For more information, see Post-processing outstanding objects on page 46.

   a. Select the object that have been wrongly marked as outstanding.

   b. Apply the **Reset** method.

This removes the **Outstanding** mark. the next time synchronization is run, the error should not occur.

For more detailed information about defining a scope and specifying handling methods for synchronization steps, see the *One Identity Manager Target System Synchronization Reference Guide*.

Configuration parameters for managing a Google Workspace environment

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

Table 46: Configuration parameters for synchronizing Google Workspace

Configuration parameter	Meaning if Set
TargetSystem | GoogleApps	Preprocessor relevant configuration parameter for controlling database model components for Google Workspace target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
	If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
TargetSystem | GoogleApps | Accounts	Parameter for configuring Google Workspace user account data.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo	Specifies to which identity the email with the random generated password should be sent (manager cost center/department/location/role, identity's manager or XUserInserted). If no recipient can be found, the email is sent to the address stored in the configuration parameter

Configuration parameter	Meaning if Set
	TargetSystem | GoogleApps | DefaultAddress.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Identity - new user account created** mail template is used.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The **Identity - initial password for new user account** mail template is used.
TargetSystem | GoogleApps | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Identity - new user account with default properties created** mail template is used.
TargetSystem | GoogleApps | Accounts | PrivilegedAccount	Allows configuration of privileged user account settings.
TargetSystem | GoogleApps | Accounts | TransferJPegPhoto	This configuration parameter specifies whether changes to the identity's picture are published in existing Google Workspace user accounts. The picture is not part of default synchronization. It is only published when an identity's main data is changed.
TargetSystem | GoogleApps | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | GoogleApps | MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem | GoogleApps | PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem | GoogleApps |	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account

Configuration parameter	Meaning if Set
PersonAutoDisabledAccounts	definition.
TargetSystem | GoogleApps | PersonAutoFullsync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem | GoogleApps | PersonExcludeList	Listing of all user account without automatic identity assignment. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.* |SUPPORT_.*|.* | $

Default project template for Google Workspace

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

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

The project template uses mappings for the following schema types.

Table 47: Mapping Google Workspace schema types to tables in the One Identity Manager schema

Schema type in Google Workspace	Table in the One Identity Manager Schema
AdminPrivilege	GAPPrivilege
AdminRole	GAPAdminRole
AdminRoleAssignment	GAPOrgAdminRole
Customer	GAPCustomer
Domain	GAPDomain
DomainAlias	GAPDomainAlias
Group	GAPGroup
OrgUnit	GAPOrgUnit
ProductAndSku	GAPPaSku
User	GAPUser
UserAddress	GAPUserAddress
UserEmail	GAPUserEmail

Schema type in Google Workspace	Table in the One Identity Manager Schema
UserExternalId	GAPUserExternalId
UserIm	GAPUserIM
UserOrganization	GAPUserOrganization
UserPhone	GAPUserPhone
UserRelation	GAPUserRelation
UserWebsite	GAPUserWebSite

API scopes for the service account

The service account's client ID must be authorized for various API scopes in the Google Admin console:

For read and write access:

```
https://www.googleapis.com/auth/admin.directory.customer,
https://www.googleapis.com/auth/admin.directory.device.chromeos,
https://www.googleapis.com/auth/admin.directory.device.mobile,
https://www.googleapis.com/auth/admin.directory.device.mobile.action,
https://www.googleapis.com/auth/admin.directory.domain,
https://www.googleapis.com/auth/admin.directory.group,
https://www.googleapis.com/auth/admin.directory.group.member,
https://www.googleapis.com/auth/admin.directory.notifications,
https://www.googleapis.com/auth/admin.directory.orgunit,
https://www.googleapis.com/auth/admin.directory.resource.calendar,
https://www.googleapis.com/auth/admin.directory.rolemanagement,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/admin.directory.user.alias,
https://www.googleapis.com/auth/admin.directory.user.security,
https://www.googleapis.com/auth/admin.directory.userschema,
https://www.googleapis.com/auth/apps.groups.settings,
https://www.googleapis.com/auth/admin.datatransfer,
https://www.googleapis.com/auth/apps.licensing
```

For read-only access:

```
https://www.googleapis.com/auth/admin.directory.customer.readonly,
https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly,
https://www.googleapis.com/auth/admin.directory.device.mobile.readonly,
https://www.googleapis.com/auth/admin.directory.domain.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.group.member.readonly,
https://www.googleapis.com/auth/admin.directory.orgunit.readonly,
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly,
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/admin.directory.user.alias.readonly,
https://www.googleapis.com/auth/admin.directory.userschema.readonly,
https://www.googleapis.com/auth/apps.groups.settings,
https://www.googleapis.com/auth/admin.datatransfer.readonly,
https://www.googleapis.com/auth/apps.licensing
```

Processing methods of Google Workspace system objects

The following table describes permitted editing methods of Google Workspace schema types and names restrictions required by system object processing.

Table 48: Methods available for editing schema types

Schema type	Read	Paste	Delete	Refresh
Customer (`Customer`)	Yes	No	No	Yes
Domain (`Domain`)	Yes	No	No	No
Domain alias (`DomainAlias`)	Yes	No	No	No
Organization (`OrgUnit`)	Yes	Yes	Yes	Yes
User account (`User`)	Yes	Yes	Yes	Yes
Group (`Group`)	Yes	Yes	Yes	Yes
Product and SKU (`ProductAndSku`)	Yes	No	No	Yes
User account: address(`UserAddress`)	Yes	Yes	Yes	Yes
User account: Email address (`UserEmail`)	Yes	Yes	Yes	Yes
User account: external ID (`UserExternalId`)	Yes	Yes	Yes	Yes
User account: instant messenger (`UserIm`)	Yes	Yes	Yes	Yes
User account: user details (`UserOrganization`)	Yes	Yes	Yes	Yes
User account: phone number (`UserPhone`)	Yes	Yes	Yes	Yes
User account: relation (`UserRelation`)	Yes	Yes	Yes	Yes
User account: website (`UserWebsite`)	Yes	Yes	Yes	Yes
Admin role (`AdminRole`)	Yes	Yes	Yes	Yes
Admin privilege (`AdminPrivilege`)	Yes	No	No	No

Schema type	Read	Paste	Delete	Refresh
Admin roles assignments (AdminRoleAssignment)	Yes	Yes	Yes	Yes

Special features in the assignment of Google Workspace groups

In One Identity Manager, entitlements can be assigned directly or indirectly to user accounts. The type of assignment is indicated in the `XOrigin` column in the assignment tables. In the `GAPUserInPaSku`, `GAPUserInOrgAdminRole`, and `GAPUserInGroup` assignment tables, `XOrigin` can take the default values **1** to **3** (bits 0 and 1).

Through the assignment of a Google Workspace groups to a Google Workspace customer, all the customer's user accounts can become members of the group. In the calculation of inheritance, an entry is made in the `GAPUserInGroup` table for each of the customer's user accounts. The origin of these assignments is indicated in `GAPUserInGroup.XOrigin` with the value **16** (bit 4).

Table 49: Origin of entitlement assignments

Assignment table	Type of assignment	Origin (`XOrigin` **column**)
GAPUserInPaSku	direct	1
GAPUserInGroup		
GAPUserInOrgAdminRole	indirect	2
GAPUserInGroup	via customers	16

For more information about calculating assignments in One Identity Manager, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Assigning Google Workspace entitlements to user accounts in One Identity Manager on page 103

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

ONE IDENTITY
by Quest