One Identity Manager 8.0.1

Administration Guide for Connecting to G Suite

One Identity Manager Administration Guide for Connecting to G Suite
Updated - April 2018
Version - 8.0.1

Contents

1

Managing G Suite

One Identity Manager offers simplified user administration for G Suite. 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.

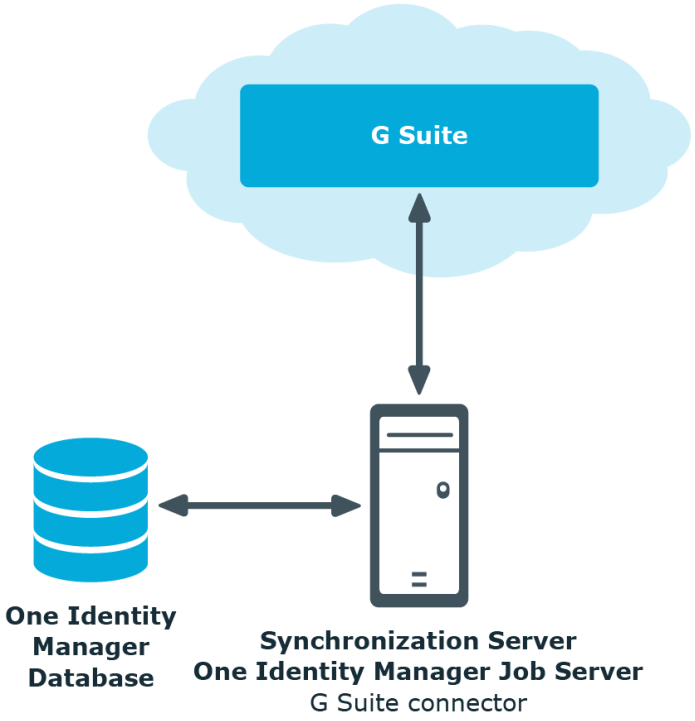
One Identity Manager provides company employees with the necessary user accounts. For this, you can use different mechanisms to connect employees to their user accounts. You can also manage user accounts independently of employees and therefore set up administrator user accounts.

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

Architecture Overview

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

Figure 1: Architecture for synchronization



One Identity Manager Users for Managing G Suite

The following users are used for setting up and managing a G Suite system.

Table 1: Users

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

User	Task
	• Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the application role **Target systems | G Suite** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare system entitlements for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
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, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.

Setting Up G Suite Synchronization

One Identity Manager supports synchronization with G Suite. One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and G Suite.

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

1. Prepare a user with sufficient permissions for synchronizing in G Suite.
2. The One Identity Manager parts for managing G Suite systems are available if the configuration parameter "TargetSystem\GoogleApps" is set.
    - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as 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 G Suite on page 10
- Setting Up the Synchronization Server on page 12
- Creating a Synchronization Project for initial Synchronization of G Suite on page 16
- Deactivating Synchronization on page 34
- Customizing Synchronization Configuration on page 23
- Appendix: Configuration Parameter for Managing G Suite on page 75
- Appendix: Default Project Templates for G Suite on page 78
- Appendix: Editing System Objects on page 80

Users and Permissions for Synchronizing with G Suite

The following users are involved in synchronizing One Identity Manager with G Suite.

Table 2: Users for Synchronization

User	Permissions
User for accessing G Suite	You must provide at least one user with super user permissions and a service account for authentication for full synchronization of G Suite 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 G Suite 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 the following API scopes in the Google Admin console: `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 more information, see Setting up Required Permissions for Accessing G Suite on page 11.

User	Permissions
One Identity Manager Service user account	The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited). The user account must belong to the group "Domain Users". The user account must have the extended access right "Log on as a service". The user account requires access rights to the internal web service. NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights 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 the One Identity Manager. In the default installation the 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 default system user "Synchronization" is available to run synchronization over an application server.

Setting up Required Permissions for Accessing G Suite

To provide the G Suite 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 G Suite super admin.
3. Select a project or create a new one.
4. Enabled 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	
Furnish a new private key	Enabled
Key type	JSON
Enable G Suite Domain-wide 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 G Suite Admin console (https://admin.google.com).
2. Log in as the G Suite 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 G Suite on page 10.

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 G Suite at least once and accept the terms of use.

Setting Up the Synchronization Server

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

- Windows operating system version 8.1. or later
- Windows Server

  Following versions are supported:

  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

- Microsoft .NET Framework Version 4.5.2 or later

  NOTE: Microsoft .NET Framework version 4.6 is not supported.

  NOTE: Take the target system manufacturer's recommendations into account.

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

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

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

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

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

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

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

1. Start the program Server Installer on your administrative workstation.
2. Enter valid data for connecting to One Identity Manager on the **Database connection** page and click **Next**.
3. Specify on which server you want to install the One Identity Manager Service on the **Server properties** page.
   a. Select a job server in the **Server** menu.

      - OR -

Click **Add** to add a new job server.

b. Enter the following data for the Job server.

Table 4: Job Servers Properties

Property	Description
Server	Name of the Job servers.
Queue	Name of queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Full server name	Full name of the server in DNS syntax. Example: `<name of server>.<fully qualified domain name>`

NOTE: Use the **Advanced** option to edit other Job server properties. You can use the Designer to change properties at a later date.

4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.
   - G Suite
5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

   The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.
   - G Suite connector
6. Check the One Identity Manager Service configuration on the **Service settings** page.

   NOTE: The initial service configuration is already predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more detailed information about configuring the service, see One Identity Manager Configuration Guide.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on the **Select installation source** page.
10. Select the file with the private key on the page **Select private key file**.

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

11. Enter the service's installation data on the **Service access** page.

Table 5: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server*** • Enter the server name. - OR - • Select a entry from the list.
Service account	One Identity Manager Service user account data. ***To enter a user account for the One Identity Manager Service*** • Set the option **Local system account**. This starts the One Identity Manager Service under the account "NT AUTHORITY\SYSTEM". - OR - • Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** **Enable** Advanced • . • Enable the option **Current user**. This uses the user account of the current user. - OR - • Enter user account, password and password confirmation.

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

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

    NOTE: The is entered with the name "One Identity Manager Service" in the server's service administration.

Creating a Synchronization Project for initial Synchronization of G Suite

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and G Suite. The following describes the steps for initial configuration of a synchronization project. For more detailed 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.

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

Table 6: Information Required for Setting up a Synchronization Project

Data	Explanation
Primary domain	Name of this G Suite'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 using to synchronize G Suite. 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 G Suite on page 10.
Synchronization server for G Suite	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database, are processed by the synchronization server. The One Identity Manager Service with the G Suite connector must be installed on the synchronization server. **Table 7: Additional Properties for the Job Server** **Property** / **Value** Server Function / G Suite connector Machine role / Server/Job server/G Suite For more information, see Setting Up the Synchronization Server on page 12.

Data	Explanation
One Identity Manager Database Connection Data	SQL Server: • Database server • Database • Database user and password • Specifies whether Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication. Oracle: • Species whether access is direct or through the Oracle client Which connection data is required, depends on how this option is set. • Database server • Oracle instance port • Service name • Oracle database user and password • Data source (TNS alias name from `TNSNames.ora`)
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • `RemoteConnectPlugin` is installed • G Suite connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

Data	Explanation
	TIP: The remote connection server requires the same configuration (with respect to the installed software) as the synchronization server. Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well. For more detailed information about setting up a remote connection, see the One Identity Manager Target System Synchronization Reference Guide.

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

- In default mode
- Started from the launchpad

Additional settings can be made if the project wizard is run in expert mode or is started directly from the Synchronization Editor. Follow the project wizard instructions through these steps.

To set up an initial synchronization project for G Suite

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

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

2. Select the entry **G Suite target system type**. Click **Run**.

   This starts the Synchronization Editor's project wizard.

3. Specify how the One Identity Manager can access the target system on the **System access** page.
   - If you have access from the workstation from which you started the Synchronization Editor, do not set anything.
   - If you do not have access from the workstation from which you started the Synchronization Editor, you can set up a remote connection.

     In this case, set the option **Connect using remote connection server** and select, under **Job server**, the server you want to use for the connection.

4. Enter the G Suite account's primary domain on the page **Primary domain and service account** as well as the service account's key file.

Table 8: Login Data for Connecting to G Suite

Property	Description
Primary domain	Name of the G Suite 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. - OR - • Click **Open key file** and select the path to the key file.

5. On the **G Suite Administrators** page, enter the email addresses of all the super administrators who can use the G Suite 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.

6. Specify, on the **Local cache** page, whether the G Suite connector's local cache should be used. This minimizes the number of times G Suite 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.

7. You can save the connection data on the last page of the system connection wizard.

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

8. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.

   NOTE: Reenter all the connection data if you are not working with an encrypted One Identity Manager database and no synchronization project has been saved yet in the database. This page is not shown if a synchronization project already exists.

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

10. Specify how system access should work on the page **Restrict target system access**. You have the following options:

Table 9: Specifying Target System Access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow should be set up to initially load 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 in synchronization direction "One Identity Manager".
Changes are also made to the target system.	Specifies whether a provisioning workflow should be set up in addition to the synchronization workflow to initially load the target system. The provisioning workflow displays the following characteristics: • Synchronization in the direction of the "target system" • Processing methods are only defined in the synchronization steps in synchronization direction "target system". • Synchronization steps are only created for such schema classes whose schema types have write access.

11. Select the synchronization server to execute synchronization on the **Synchronization server** page.

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

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

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

      NOTE: Ensure that this server is set up as the synchronization server after saving the synchronization project.

12. Click **Finish** to complete the project wizard.

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

    The synchronization project is created, saved and enabled immediately.

NOTE: If the synchronization project is not going to be executed immediately, disable the option **Activate and save the new synchronization project automatically**.

In this case, save the synchronization project manually before closing the Synchronization Editor.

NOTE: The target system connection data is saved in a variable set, which you can change in the Synchronization Editor under **Configuration | Variables** if necessary.

To configure the content of the synchronization log

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

   NOTE: Certain content create a lot of log data.

   The synchronization log should only contain the data necessary for error analysis and other evaluations.
6. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

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

NOTE: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the customer environment at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the customer environment.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
    a. Select the category **G Suite | User accounts | Linked but not configured | <Domain>**.
    b. Select the task **Assign account definition to linked accounts**.

Related Topics

- Setting Up the Synchronization Server on page 12
- Users and Permissions for Synchronizing with G Suite on page 10
- Show Synchronization Results on page 22
- Customizing Synchronization Configuration on page 23
- Target System Connection Advanced Settings on page 27
- Appendix: Default Project Templates for G Suite on page 78

Show 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. Select the category **Logs**.
2. Click ▶ in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.
3. Select a log by double-clicking on it.

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

To display a provisioning log.

1. Select the category **Logs**.
2. Click in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.
3. Select a log by double-clicking on it.

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

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

Synchronization logs are stored for a fixed length of time. The retention period is set in the configuration parameter "DPR\Journal\LifeTime" and its sub parameters.

To modify the retention period for synchronization logs

- Set the configuration parameter "Common\Journal\LifeTime" in the Designer and enter the maximum retention time for entries in the database journal. Use the configuration sub parameters to specify the retention period for each warning level.
- If there is a large amount of data, you can specify the number of objects to delete per DBQueue Processor operation and run in order to improve performance. Use the configuration parameters "Common\Journal\Delete\BulkCount" and "Common\Journal\Delete\TotalCount" to do this.
- Configure and set the schedule "Delete journal" in the Designer.

Customizing Synchronization Configuration

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

You must customize the synchronization configuration in order to compare the database with the G Suite regularly and to synchronize changes.

- Create a workflow with the direction of synchronization "target system" to use One Identity Manager as the master system for synchronization.
- To specify which G Suite objects and database object 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 which contain the necessary information about the synchronization objects when

synchronization starts. Variables can be implemented in base objects, schema classes or processing methods, for example.

- Use variables to set up a synchronization project which can be used for several different customers. Store a connection parameter as a variable for logging in to the respective G Suite 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.
- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema.

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

- The moment another synchronization is started with the same start up configuration, the running synchronization process is stopped and given the status, "Frozen". An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration. Group start up configurations with the same start up behavior.

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

Detailed information about this topic

- Configuring Synchronization in G Suite on page 24
- Configuring Synchronization of Customer Environments on page 25
- Updating Schemas on page 26
- Target System Connection Advanced Settings on page 27

Configuring Synchronization in G Suite

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). You also require a workflow with synchronization in the direction of the "target system" to use One Identity Manager as the master system for synchronization.

To create a synchronization configuration for synchronizing G Suite

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This adds a workflow for synchronizing in the direction of the target system.
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 Customer Environments on page 25

Configuring Synchronization of Customer Environments

The following prerequisites must be fulfilled for all customers that are to be synchronized with the same synchronization project.

Prerequisites

- The customer target systems schema are identical.
- All virtual schema properties used in the mapping must exist in the customer's extended schemas.

To customize a synchronization project for synchronizing another customer

1. Supply a user in the customer with sufficient permissions for accessing the G Suite.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other customers. Use the wizards to attach a base object.
   - Select the G Suite connector in the wizard and enter the connection parameters. The connection parameters are saved in a special variable set.

     A start up configuration is created, which uses the new 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 in G Suite on page 24

Updating Schemas

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

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

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

- A schema was changed by:
  - Changes to a target system schema
  - Customizations to the One Identity Manager schema
  - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
  - Activating the synchronization project
  - Synchronization project initial save
  - Compressing a schema

To update a system connection schema

1. Select the category **Configuration | Target system**.

   - OR -
   Select the category

   Configuration | One Identity Manager connection.
2. Select the view **General** and click **Update schema**.
3. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Mappings**.

3. Select a mapping in the navigation view.

   Opens the Mapping Editor. For more detailed information about editing mappings, see 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.

Target System Connection Advanced Settings

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.

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

   For more information, see Editing Connection Parameters in Variable Sets on page 29.

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. However the default values get overwritten and you cannot reset them.

   For more information, see Editing Target System Connection Properties on page 30.

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 10: Target System Connection Advanced Settings

Property	Description
Use the local cache	Specifies whether the G Suite connector's local cache is used. Local cache is used to prevent the API contingent from being exceeded through synchronization. Accesses to G Suite 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 detailed information, see the One Identity Manager Target System

Property	Description
	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 G Suite 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.

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 G Suite connector. If Google changes this list, you can enter an XML file here, which overwrites the list in the G Suite connector.
	Example:
	`<products>`
	`<product name="G Suite" id="Google-Apps">`
	`<sku id="Google-Apps-Unlimited" name="G Suite Business"/>`
	`<sku id="Google-Apps-For-Business" name="G Suite Basic" />`
	`<sku id="Google-Apps-Lite" name="G Suite 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>`

Editing Connection Parameters in Variable Sets

The connection parameters for advanced settings were saved as variables 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 user 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 for synchronization use different customers.

To modify advanced settings in a specialized variable set

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target systems**.
3. Open the **Connection parameters** view.
4. Select one of the following parameters and click **Convert**.

Table 11: Variables for Advanced System Connection Settings

Parameter	Description
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.
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.
Cache	Specifies whether the local G Suite cache is used.

For more information, see Target System Connection Advanced Settings on page 27.

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

   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 a variable set, mark the variable and click in the variable set view's toolbar. Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the category **Configuration | Start up configurations**.
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 category **Configuration | Base objects**.
13. Select the base object and click .

    - OR -

    Click to add a new base object.
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

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

Editing Target System Connection Properties

You can also change the target system connection's advanced properties with the system connection wizard. In the process, the values you set here are transferred to the default variable set. The original default values cannot, therefore, be restored again.

To edit advanced settings with the system connection wizard

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target systems**.
3. Click **Edit connection...**.

   This starts the system connection wizard.
4. Enable **Show advanced settings** on the system connection wizard's start page.
5. Customize the properties as required on the **Advanced settings** page.

   For more information, see Target System Connection Advanced Settings on page 27.
6. Save the changes.

Speeding Up Synchronization with Revision Filtering

Synchronization with G Suite does not support revision filtering.

Post-Processing Outstanding Objects

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

Objects marked as outstanding:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Must be post-processed separately in One Identity Manager.

Start target system synchronization to do this.

To post-process outstanding objects

1. Select the category **G Suite | Target system synchronization: G Suite**.

   All tables assigned to the target system type G Suite as synchronization tables are displayed in the navigation view.
2. Select the table whose outstanding objects you want to edit in the navigation view.

   This opens the target system synchronization form. All objects are shown here that are marked as outstanding.

   TIP:

   To display object properties of an outstanding object

   a. Select the object on the target system synchronization form.

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

Table 12: Methods for handling outstanding objects

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

Icon	Method	Description
		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 from the object.

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

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

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

To disable bulk processing

- Deactivate in the form toolbar.

You must customize synchronization to synchronize custom tables.

To add tables to the target system synchronization.

1. Select the category **G Suite | Basic configuration data | Target system types**.
2. Select the target system type G Suite in the result list.
3. Select **Assign synchronization tables** in the task view.
4. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
5. Save the changes.
6. Select **Configure tables for publishing**.
7. Select custom tables whose outstanding objects can be published in the target system and set the option **Publishable**.
8. Save the changes.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the option **Connection is read only** must no be set for the target system connection.

Configuring Memberships Provisioning

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

- Memberships are saved in the target system as an object property in list form (Example: List of users accounts in the property `Members` of a `group`).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; previously deleted memberships are added again.

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

To allow separate provisioning of memberships

1. Start the Manager.
2. Select the category **G Suite | Basic configuration data | Target system types**.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - The option can only be set for assignment tables whose base table has a `XDateSubItem` or a `CCC_XDateSubItem` .
    - Assignment tables, which are grouped together in a virtual schema property in the mapping, must be labeled identically.
5. Click **Enable merging**.
6. Save the changes.

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

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

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

Help for Analyzing Synchronization Issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance. The report contains information such as:

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

To generate a synchronization analysis report

1. Select the menu **Help | Generate synchronization analysis report** and answer the security prompt with **Yes**.

   The report may take a few minutes to generate. It is displayed in a separate window.
2. Print the report or save it in one of the available output formats.

Deactivating Synchronization

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

To prevent regular synchronization

- 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 loaded synchronization project

1. Select **General** on the start page.
2. Click **Deactivate project**.

Related Topics

- Creating a Synchronization Project for initial Synchronization of G Suite on page 16

3

Base Data for Managing G Suite

To manage G Suite in One Identity Manager, the following data is relevant.

- Configuration parameter

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

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

  For more information, see Appendix: Configuration Parameter for Managing G Suite on page 75.

- Account definitions

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

  For more information, see Setting Up Account Definitions on page 36.

- Password policies

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' 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 user or customize if required. You can also define your own password policies.

  For more information, see Password Policies on page 54.

- Initial Password for New User Accounts

  You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used or a randomly generated initial password can be issued.

  For more information, see Initial Password for New G Suite User Accounts on page 63.

- Email notifications about login data

  When a new user account is created, the login data are send to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.

  For more information, see Email Notifications about Login Data on page 64.

- Target system types

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

  For more information, see Post-Processing Outstanding Objects on page 31.

- Server

  In order to handle G Suite specific processes in One Identity Manager, the synchronization server and its server functionality must be declared.

  For more information, see Editing a Server on page 66.

- Target system managers

  A default application role exists for the target system manager in the One Identity Manager. Assign this application to employees who are authorized to edit the G Suite object in One Identity Manager.

  Define other application roles, if you want to limit target system managers' access permissions to individual customer environments. The application roles must be added under the default application role.

  For more information, see Target System Managers on page 70.

Setting Up Account Definitions

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

The data for the user accounts in the respective target system comes from the basic employee data. The assignment of the IT operating data to the employee’s user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role (template processing). Processing is done through

templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

For more details about the basics, see the One Identity Manager Target System Base Module Administration Guide.

The following steps are required to implement an account definition:

- Creating an Account Definition on page 37
- Setting Up Manage Levels on page 39
- Creating a Formatting Rule for IT Operating Data on page 42
- Determining IT Operating Data on page 43
- Assigning Account Definitions to Employees on page 46
- Assigning Account Definitions to a Target System on page 51

Creating an Account Definition

To create a new account definition

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- Master Data for an Account Definition on page 37

Master Data for an Account Definition

Enter the following data for an account definition:

Table 13: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.

Property	Description
User account table	Table in the One Identity Manager schema which maps user accounts.
Target System	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between . When this is requested or assigned, the required is automatically requested or assigned with it. Leave empty for G Suite.
Description	Spare text box 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 account definition assignments to employees. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can still be directly assigned to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account

Property	Description
	definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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 disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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 employees posing a security risk . Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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.

Setting Up Manage Levels

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

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

The One Identity Manager supplies a default configuration for manage levels:

- Unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.

- Full managed

  User accounts with a manage level of "Full managed" inherit specific properties from the assigned employee.

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

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

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

- Employee user accounts can be locked when they are disabled, deleted or rated as a security risk so that permissions are immediately withdrawn. If the employee is reinstated at a later date, the user accounts are also reactivated.
- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee’s user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted!

To assign manage levels to an account definition

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level** in the task view.
4. Assign manage levels in **Add assignments**.

   - OR -

   Remove assignments to manage levels in **Remove assignments**.
5. Save the changes.

IMPORTANT: The manage level "Unmanaged" is assigned automatically when an account definition is assigned and cannot be removed.

To edit a manage level

1. Select the category **G Suite | Basic configuration data | Account definitions | Manage levels**.
2. Select the manage level in the result list. Select **Change master data**.

   - OR -

   Click in the result list toolbar.
3. Edit the manage level's master data.
4. Save the changes.

Related Topics

- Master Data for a Manage Level on page 41

Master Data for a Manage Level

Enter the following data for a manage level.

Table 14: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.
Description	Spare text box 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 always: Data is always updated Only initially: Data is only initially determined.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.

Property	Description
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether locked user accounts retain their group memberships.

Creating a Formatting Rule for IT Operating Data

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

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

- G Suite Organization
- Groups can be inherited
- Identity
- Privileged user account
- Change password the next time you log in

To create a mapping rule for IT operating data

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Edit IT operating data mapping** in the task view and enter the following data.

Table 15: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
Source	Specifies which roles to use in order to find the user account properties.

Property	Description
	You have the following options: • Primary department • Primary location • Primary cost center • Primary business roles NOTE: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\GoogleApps\Accounts\MailTemplateDefaultValues".

4. Save the changes.

Related Topics

- Determining IT Operating Data on page 43

Determining IT Operating Data

In order for an employee to create user accounts with the manage level "Full managed", the necessary IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example:

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

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

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

To specify IT operating data

1. Select the role in the category **Organizations** or **Business roles**.
2. Select **Edit IT operating data** in the task view and enter the following data.

Table 16: IT Operating Data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. ***To specify an application scope*** a. Click → next to the text box. b. Select the table under **Table**, which maps the target system or the table `TSBAccountDef` for an account definition. c. Select the concrete target system or concrete account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. Columns using the script template `TSB_ITDataFromOrg` in their template are listed. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
Value	Concrete value which is assigned to the user account property.

3. Save the changes.

Related Topics

- Creating a Formatting Rule for IT Operating Data on page 42

Modifying IT Operating Data

If IT operating data changes, you must transfer these 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 the effect of a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the database in the case of each affected column in each affected database.

Prerequisites

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

  - OR -

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

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

To execute the template

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

Old value	Current value of the object property.
New value	Value applied to the object property after modifying the IT operating data.
Selection	Specifies whether the modification is applied to the user account.

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

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

Assigning Account Definitions to Employees

Account definitions are assigned to company employees. Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations or roles. The employees are categorized into these departments, cost centers, locations or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees. You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

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

NOTE: If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (department, cost center, location or business role).

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

Detailed information about this topic

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

   Remove the organizations from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Account Definitions to Business Roles on page 47
- Assigning Account Definitions to all Employees on page 48
- Assigning Account Definitions Directly to Employees on page 49
- Assigning Account Definitions to System Roles on page 49
- Adding Account Definitions in the IT Shop on page 50

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

   Remove business roles in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 47
- Assigning Account Definitions to all Employees on page 48
- Assigning Account Definitions Directly to Employees on page 49
- Assigning Account Definitions to System Roles on page 49
- Adding Account Definitions in the IT Shop on page 50

Assigning Account Definitions to all Employees

To assign an account definition to all employees

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Automatic assignment to employees** on the **General** tab.

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

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

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 47
- Assigning Account Definitions to Business Roles on page 47
- Assigning Account Definitions Directly to Employees on page 49
- Assigning Account Definitions to System Roles on page 49
- Adding Account Definitions in the IT Shop on page 50

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees** in the task view.
4. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 47
- Assigning Account Definitions to Business Roles on page 47
- Assigning Account Definitions to all Employees on page 48
- Assigning Account Definitions to System Roles on page 49
- Adding Account Definitions in the IT Shop on page 50

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

1. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove assignments to system roles in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 47
- Assigning Account Definitions to Business Roles on page 47
- Assigning Account Definitions to all Employees on page 48
- Assigning Account Definitions Directly to Employees on page 49
- Adding Account Definitions in the IT Shop on page 50

Adding Account Definitions in the IT Shop

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

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

To add an account definition to the IT Shop

1. Select the category **G Suite | Basic configuration data | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the account definition to the IT Shop shelf in **Add assignments**
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. Select the category **G Suite | Basic configuration data | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.

4. Remove the account definition from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

1. Select the category **G Suite | Basic configuration data | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

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

Related Topics

- Master Data for an Account Definition on page 37
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 47
- Assigning Account Definitions to Business Roles on page 47
- Assigning Account Definitions Directly to Employees on page 49
- Assigning Account Definitions to System Roles on page 49

Assigning Account Definitions to a Target System

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

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

User accounts are only linked to the employee (state "Linked") 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. Select the customer in the category **G Suite | Customers**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

Related Topics

- Assigning Account Definitions to Employees on page 46

Deleting an Account Definition

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

NOTE: If an account definition is deleted, the user accounts arising from this account definition are deleted.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Change master data** in the task view.
    d. Disable the option **Automatic assignment** to employees on the **General** tab.
    e. Save the changes.
2. Remove direct assignments of the account definition to employees.
    a. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign to employees** in the task view.
    d. Remove employees from **Remove assignments**.
    e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
    a. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.

c. Select **Assign organizations**.

d. Remove the account definition's assignments to departments, cost centers and locations in **Remove assignments**.

e. Save the changes.

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

a. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

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

Remove business roles from **Remove assignments**.

d. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves. For more detailed information, see the One Identity Manager IT Shop Administration Guide.

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

a. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Change master data** in the task view.

d. Remove the account definition from the **Required account definition** menu.

e. Save the changes.

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

a. Select the customer in the category **G Suite | Customers**.

b. Select **Change master data** in the task view.

c. Remove the assigned account definitions on the **General tab**.

d. Save the changes.

8. Delete the account definition.

a. Select the category **G Suite | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Click , to delete the account definition.

Password Policies

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' 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 user or customize if required. You can also define your own password policies.

Detailed information about this topic

Predefined Password Policies

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

Password for logging into One Identity Manager

The password policy "One Identity Manager password policy" is used for logging into One Identity Manager. This password policy defined the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the access code for a one off log in on the Web Portal (`Person.Passcode`).

The password policy "One Identity Manager password policy" is also labeled as the default and is used when no other password policy is found.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The password policy "Employee central password policy" defines the settings for the central password (`Person.CentralPassword`).

IMPORTANT: Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.

Password policies for target systems

A predefined password policy that you can apply to the user account password columns, is provided for every target system.

IMPORTANT: If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

The password policy "G Suite password policy" id 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.

Editing Password Policies

To edit a password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
2. Select the password policy in the result list and select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

- General Master Data for a Password Policy on page 55
- Policy Settings on page 56
- Character Sets for Passwords on page 57
- Custom Scripts for Password Requirements on page 57

General Master Data for a Password Policy

Enter the following master data for a password policy.

Table 17: Master Data for a Password Policy

Property	Meaning
Display name	Password policy name. Translate the given text using the

Property	Meaning
	button.
Description	Spare text box for additional explanation. Translate the given text using the button.
Error Message	Custom error message outputted 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. NOTE: The password policy "One Identity Manager password policy" is marked as the default policy. This password policy is applied if no other password policies can be found.

Policy Settings

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

Table 18: Policy Settings

Property	Meaning
Initial password	Initial password for new user accounts. If no password is given when the user account is added or a random password is generated, the initial password is used.
Password confirmation	Reconfirm password.
Min. Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If the value '5' is entered, for example, the last 5 passwords of the user are saved.
Min. password strength	Specifies how secure the password must be. The higher the

Property	Meaning
	password strength, the more secure it is. The password strength is not tested if the value is '0'. The values '1', '2', '3' and '4' gauge the required complexity of the password. The value '1' demands the least complex password. The value '4' demands the highest complexity.
Name properties denied	Specifies whether name properties are permitted in the password.

Character Sets for Passwords

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

Table 19: Character Classes for Passwords

Property	Meaning
Min. letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lower case	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 characters.
Denied special characters	List of characters, which are not permitted.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Maximum number of identical character that can be repeated after each other.

Custom Scripts for Password Requirements

You can implement custom scripts for testing and generating password 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

- Script for Checking a Password on page 58
- Script for Generating a Password on page 59

Script for Checking a Password

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

Syntax for 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 test

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

Example for a script for testing a password

A password cannot have '?' or '!' at the beginning. 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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
    b. Select the password policy in the result list.
    c. Select **Change master data** in the task view.
    d. Enter the name of the script to test the password in **Check script** on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for Generating a Password on page 59

Script for Generating a Password

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 property `Entity` of the `PasswordPolicy` class.

Example for a script to generate a password

The script replaces the invalid characters '?' and '!' in random passwords.

```
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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
    b. Select the password policy in the result list.
    c. Select **Change master data** in the task view.
    d. Enter the name of the script to generate a password in **Generation script** on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for Checking a Password on page 58

Restricted 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. Select the category **Base Data | Security Settings | Restricted passwords** in the Designer.
2. Create a new entry with the menu item **Object | New** an enter the term to excluded to the list.
3. Save the changes.

Testing a Password

When you test a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To test whether a password conforms to the password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
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 Generating a Password

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. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Assigning a Password Policy

The password policy "G Suite password policy" id 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.

IMPORTANT: If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

To reassign a password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
2. Select the password policy in the result list.
3. Select **Assign objects** in the task view.
4. Click **Add** in the **Assignments** section and enter the following data.

Table 20: Assigning a Password Policy

Property	Description
Apply to	Application scope of the password policy. ***To specify an application scope*** a. Click → next to the text box. b. Select the table which contains the password column under **Table**. c. Select the specific target system under **Apply to**. d. Click **OK**.
Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

5. Save the changes.

To change a password policy's assignment

1. Select the category **Manager | Basic configuration data | Password policies** in the G Suite.
2. Select the password policy in the result list.
3. Select **Assign objects** in the task view.
4. Select the assignment you want to change in **Assignments**.
5. Select the new password policy to apply from the **Password Policies** menu.
6. Save the changes.

Initial Password for New G Suite User Accounts

Table 21: Configuration Parameters for Formatting Initial Passwords for User Accounts

Configuration parameter	Meaning
QER\Person\UseCentralPassword	This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated.
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permanently stored. If the parameter is not set, the central password is only used for publishing to existing target system specific user accounts and is subsequently deleted from the One Identity Manager database.
TargetSystem\GoogleApps\Accounts\ InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.

You have the following possible options for issuing an initial password for a new user account.

- User the employee's central password. The employee's central password is mapped to the user account password.
  - Set the configuration parameter "QER\Person\UseCentralPassword" in the Designer.

    If the configuration parameter "QER\Person\UseCentralPassword" is set, the employee's central password is automatically mapped to an employee's user

account in each of the target systems. This excludes privileged user accounts, which are not updated.

- Use the configuration parameter "QER\Person\UseCentralPassword\PermanentStore" in the Designer to specify whether an employee's central password is permanently saved in the One Identity Manager database or only until the password has been published in the target system.

The password policy "Employee central password policy" is used to format the central password.

IMPORTANT: Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.

- Create user accounts manually and enter a password in their master data.
- Specify an initial password to be used when user accounts are created automatically.
  - Apply the target system specific password policies and enter an initial password in the password policies.
- Assign a randomly generated initial password to enter when you create user accounts.
  - Set the configuration parameter "TargetSystem\GoogleApps\Accounts\InitialRandomPassword" in the Designer.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.

Related Topics

- Password Policies on page 54
- Email Notifications about Login Data on page 64

Email Notifications about Login Data

Table 22: Configuration Parameters for Notifications about Actions in the Target System

Configuration parameter	Meaning
TargetSys-tem\GoogleApps\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem\GoogleApps\Accounts InitialRandomPassword\SendTo	This configuration parameter specifies to

Configuration parameter	Meaning
	which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee's manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\GoogleApps\DefaultAddress".
TargetSystem\GoogleApps\Accounts InitialRandomPassword\SendTo\ MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".
TargetSystem\GoogleApps\Accounts InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".

You can configure the login information 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, which 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.

To use email notifications about login data

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Configuration Guide.
2. Enable the configuration parameter "Common\MailNotification\DefaultSender" in the Designer and enter the email address for sending the notification.
3. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.
4. Ensure that a language culture can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed 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 person.

To send initial login data by email

1. Set the configuration parameter "TargetSystem\GoogleApps\Accounts\InitialRandomPassword" in the Designer.
2. Set the configuration parameter "TargetSystem\GoogleApps\Accounts\InitialRandomPassword\SendTo" in the Designer and enter the message recipient as value.
3. Set the configuration parameter "TargetSystem\GoogleApps\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in the Designer.

   By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.
4. Set the configuration parameter "TargetSystem\GoogleApps\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in the Designer.

   By default, the message sent uses the mail template "Employee - initial password for new user account". The message contains the initial password for the user account.

TIP: Change the value of the configuration parameter in order to use custom mail templates for these mails.

Editing a Server

In order to handle G Suite 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:

- Create an entry for the Job server in the category **Base Data | Installation | Job server** in the Designer. For detailed information, see the One Identity Manager Configuration Guide.
- Select an entry for the Job server in the category **Manager | Basic configuration data | Server** in the G Suite and edit the Job server master data.

  Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

NOTE: One Identity Manager must be installed, configured and started in order for a server to execute its function in the One Identity Manager Service network. Proceed as follows in the One Identity Manager Installation Guide.

To edit a Job server and its functions

1. Select the category **G Suite | Basic configuration data | Server** in the Manager.
2. Select the Job server entry in the result list.
3. Select **Change master data** in the task view.

4. Edit the Job server's master data.
5. Select **Assign server functions** in the task view and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master Data for a Job Server on page 67
- Specifying Server Functions on page 69

Related Topics

- Setting Up the Synchronization Server on page 12

Master Data for a Job Server

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Installation | Job server**.

Table 23: Job Server Properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of servers>.<Fully qualified domain name>`
Target System	Computer account target system.
Language culture	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 properties **Server is cluster** and **Server belongs to cluster** are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP	Internet protocol version 4 (IPv4) server address.

Property	Meaning
address (IPv4)	
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. Only the methods "Robocopy" and "Rsync" are currently supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication then takes place between servers with a Windows operating system using "Robocopy" and between servers with the Linux operating system using "rsync". 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 One Identity Manager Service is automatically updated. If the server is handling several queues the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. Permitted values are "Win32", "Windows", "Linux" and "Unix". If the input is empty, "Win32" is assumed.
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.

Property	Meaning
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure QBM_PJobQueueLoad 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 program "Job Queue Info".
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 being executed.
Server Function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying Server Functions on page 69

Specifying Server Functions

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Installation | Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.

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

Table 24: Permitted Server Functions

Server Function	Remark
Update Server	This server executes automatic software updating of all other servers. The

Server Function	Remark
	server requires a direct connection to the database server that the One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can process SQL tasks. 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.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which the One Identity Manager Service sends email notifications. Prerequisite for sending mails using the One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
G Suite connector	Server on which the G Suite connector is installed. This server executes synchronization with the target system G Suite.
SharePoint Online connector	Server on which the SharePoint Online connector is installed. This server executes synchronization with the target system SharePoint Online.

Related Topics

- Master Data for a Job Server on page 67

Target System Managers

For more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

Implementing Application Roles for Target System Managers

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

   The default application role target system managers are entitled to edit all customers in One Identity Manager.
3. Target system managers can authorize more employees as target system managers, within their scope of responsibilities and create other child application roles and assign individual customers.

Table 25: Default Application Roles for Target System Managers

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | G Suite** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare system entitlements for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

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

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

1. Log yourself into the Manager as target system administrator (application role **Target systems | Administrator**).
2. Select the category **One Identity Manager Administration | Target systems | G Suite**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

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

1. Login to the Manager as target system manager.
2. Select the application role in the category **G Suite | Basic configuration data | Target system managers**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To define target system managers for individual customers.

1. Login to the Manager as target system manager.
2. Select the category **G Suite | Customers**.
3. Select the customer in the result list.
4. Select **Change master data** in the task view.
5. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

   Click next to the **Target system manager** menu to create a new application role.
   - Enter the application role name and assign the parent application role **Target system | G Suite**.
   - Click **OK** to add the new application role.
6. Save the changes.
7. Assign the application role to employees, who are authorized to edit the customer in One Identity Manager.

Related Topics

- One Identity Manager Users for Managing G Suite on page 7

4

Troubleshooting

Newly Added User Accounts are Marked as Outstanding

If G Suite is synchronized with the One Identity Manager database shortly after provisioning new user accounts, these user accounts might be marked as outstanding in the 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 G Suite 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, which 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 31.

   a. Select the object that have been wrongly marked as outstanding.

   b. Apply the method "Reset".

      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.

Appendix: Configuration Parameter for Managing G Suite

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 26: Configuration Parameters for Synchronizing G Suite

Configuration Parameter	Meaning if Set
TargetSystem\GoogleApps	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system G Suite. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\GoogleApps\Accounts	Parameter for configuring G Suite user account data.
TargetSystem\GoogleApps\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued 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 employee the email with the random generated password should be sent (manager cost center/department/location/role, employee's manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\GoogleApps\DefaultAddress".
TargetSystem\GoogleApps\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".

Configuration Parameter	Meaning if Set
TargetSystem\GoogleApps\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\GoogleApps\Accounts\MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. Use the mail template "Employee - new user account with default properties created".
TargetSystem\GoogleApps\Accounts\PrivilegedAccount	This configuration parameter allows configuration of settings for privileged user accounts.
TargetSystem\GoogleApps\Accounts\TransferJPegPhoto	This configuration parameter specifies whether changes to the employee's picture are published in existing G Suite user accounts. The picture is not part of default synchronization. It is only published when employee data is changed.
TargetSystem\GoogleApps\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem\GoogleApps\MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. 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	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\GoogleApps\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem\GoogleApps\PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\GoogleApps\	List of all user accounts for which automatic

Configuration Parameter	Meaning if Set
PersonExcludeList	employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern.

Appendix: Default Project Templates for G Suite

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

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the .Synchronization Editor

The template uses mappings for the following schema types.

Table 27: Mapping G Suite schema types to tables in the One Identity Manager schema.

Schema Type in G Suite	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 G Suite	Table in the One Identity Manager Schema
UserExternalId	GAPUserExternalId
UserIm	GAPUserIM
UserOrganization	GAPUserOrganization
UserPhone	GAPUserPhone
UserRelation	GAPUserRelation
UserWebsite	GAPUserWebSite

Appendix: Editing System Objects

The following table describes permitted editing methods for G Suite schema types.

Table 28: Methods Available for Editing Schema Types

Schema type	Read	Paste	Delete	Refresh
G Suite 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
Admin roles assignments (`AdminRoleAssignment`)	Yes	Yes	Yes	Yes

About us

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

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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

N

O

P

R

S

T

U

V