Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

⚠️ WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

ℹ️ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Administration Guide for Connecting to G Suite
Updated - August 2019
Version - 8.1.1
# Contents

**Mapping G Suite in One Identity Manager** ................................................................. 9
- Architecture overview ......................................................................................... 9
- One Identity Manager users for managing G Suite ........................................ 10
- Configuration parameter .................................................................................. 12

**Synchronizing G Suite** ...................................................................................... 13
- Setting up the initial synchronization of G Suite ............................................ 13
  - Users and permissions for synchronizing with G Suite .......................... 14
  - Setting up required permissions for accessing G Suite ......................... 16
- Setting up the G Suite synchronization server ........................................... 17
  - System requirements for the G Suite synchronization server ............... 17
- Installing the One Identity Manager Service ............................................... 18
- Creating a synchronization project for initial synchronization of G Suite .... 20
  - Information required for setting up a synchronization project ............... 21
- Creating an initial synchronization project for G Suite ............................... 22
- Configuring the synchronization log ............................................................... 26

- Adjusting the synchronization configuration for G Suite environments .... 26
  - Configuring synchronization in G Suite .................................................... 27
  - Configuring synchronization of different customers ............................... 28
- Updating schemas ........................................................................................... 29
- Speeding up synchronization with revision filtering .................................... 30
  - Advanced settings for system connection to G Suite ............................ 30
    - Editing connection parameters in the variable set .............................. 33
    - Editing target system connection properties ...................................... 34
- Configuring the provisioning of memberships ............................................ 35
  - Configuring single object synchronization ............................................. 36

- Executing a synchronization ............................................................................ 37
  - Starting synchronization ............................................................................. 37
  - Displaying synchronization results ............................................................ 38
  - Deactivating synchronization ..................................................................... 39
  - Synchronizing single objects ...................................................................... 39
- Tasks after a synchronization ........................................................................ 40
Post-processing outstanding objects ..................................................40
Adding custom tables to the target system synchronization ..................43
Managing user accounts through account definitions ..........................43
Troubleshooting .............................................................................43

Managing G Suite user accounts and employees ...............................45
Account definitions for G Suite user accounts ....................................46
  Creating account definitions ..........................................................47
  Editing account definitions ..........................................................47
  Master data for account definitions ..............................................47
  Creating manage levels ..................................................................49
  Master data for manage levels ......................................................50
  Creating mapping rules for IT operating data .................................52
  Entering IT operating data ............................................................53
  Modify IT operating data ..............................................................55
  Assigning account definitions to employees ....................................56
    Assigning account definitions to departments, cost centers, and locations ....57
    Assigning account definitions to business roles ............................57
    Assigning account definitions to all employees .............................58
    Assigning account definitions directly to employees .....................59
    Assigning account definitions to system roles ..............................59
    Adding account definitions in the IT Shop ....................................60
  Assigning account definitions to target systems ..............................61
  Deleting account definitions .........................................................62
Automatic assignment of employees to G Suite user accounts ..............64
  Editing search criteria for automatic employee assignment ...............65
    Finding employees and directly assigning them to user accounts ........66
  Changing the manage level in G Suite user accounts .......................68
  Assigning account definitions to linked user accounts ....................69
Manually linking employees to G Suite user accounts .........................69
Supported user account types ..........................................................70
  Default user accounts .................................................................71
  Administrative user accounts .......................................................72
    Providing administrative user accounts for one employee ...............73
    Providing administrative user accounts for several employees ...........74
Privileged user accounts ............................................................... 75

Provision of login information for G Suite user accounts .......... 77
Password policies for G Suite user accounts ................................ 77
Predefined password policies ..................................................... 78
Applying password policies ..................................................... 79
Editing password policies .......................................................... 81
Creating password policies ....................................................... 81
General master data for password policies ................................. 81
Policy settings ............................................................................. 82
Character classes for passwords .................................................. 83
Custom scripts for password requirements ................................... 84
  Script for checking passwords .................................................. 84
  Script for generating a password .............................................. 86
Editing the excluded list for passwords ....................................... 87
Checking passwords .................................................................... 87
Testing the generation of passwords .......................................... 88
Initial password for new G Suite user accounts ......................... 88
Email notifications about login data ........................................... 89

Managing G Suite entitlement assignments .............................. 90
Assigning G Suite entitlements to user accounts in One Identity Manager ...... 90
  Assigning G Suite entitlements to departments, cost centers, and locations .......... 92
Assigning G Suite entitlements to business roles .......................... 93
Adding G Suite entitlements to system roles .................................. 94
Adding G Suite entitlements to the IT Shop .................................. 94
Assigning G Suite user accounts directly to an entitlement .......... 96
Assigning G Suite entitlements directly to a user account ............. 97
Assigning G Suite groups directly to a customer ......................... 97
Assigning G Suite customers directly to a group ......................... 98
Effectiveness of G Suite entitlement assignments ....................... 98
Inheritance of G Suite entitlements based on categories ................ 101
Overview of all assignments ...................................................... 103

Mapping of G Suite objects in One Identity Manager ................. 105
G Suite customers ....................................................................... 105
  Creating G Suite customers ................................................... 105
Editing master data for G Suite customers ................................................................. 106
General master data for G Suite customers .............................................................. 106
G Suite customer address data .................................................................................. 108
Defining categories for the inheritance of G Suite entitlements ................................. 108
Additional tasks for managing G Suite entitlements ................................................. 108
  Overview of a G Suite customer ............................................................................. 109
  Editing the synchronization project for a G Suite customer ................................... 109
G Suite user accounts ................................................................................................. 110
Creating G Suite user accounts .................................................................................. 111
Editing master data for G Suite user accounts ......................................................... 112
General master data for G Suite user accounts ....................................................... 113
Password data for G Suite user accounts ................................................................ 117
Phone numbers for G Suite user accounts ............................................................... 117
Addresses for G Suite user accounts ...................................................................... 118
E-mail addresses for G Suite user accounts ............................................................. 118
External IDs for G Suite user accounts ................................................................... 119
Instant messenger data for G Suite user accounts ................................................... 119
User details for G Suite user accounts .................................................................... 120
Relationships of G Suite user accounts ................................................................... 121
Websites of G Suite user accounts .......................................................................... 121
Additional tasks for managing G Suite user accounts .............................................. 122
  Overview of G Suite user accounts ....................................................................... 122
  Assigning extended properties to a G Suite user account ................................. 123
  Moving G Suite user accounts to a different organization .................................... 123
Locking G Suite user accounts ................................................................................ 123
Deleting and restoring G Suite user accounts ........................................................... 125
Transferring user data to a different G Suite user account ....................................... 126
G Suite groups ........................................................................................................... 127
Creating G Suite groups ......................................................................................... 127
Entering master data for G Suite groups .................................................................. 127
General master data for G Suite groups .................................................................. 128
Additional settings for G Suite groups ..................................................................... 129
Additional tasks for managing G Suite groups ......................................................... 130
  Overview of G Suite groups .................................................................................. 131
  Assigning extended properties to a G Suite group .............................................. 131
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning group managers</td>
<td>132</td>
</tr>
<tr>
<td>Assigning group owners</td>
<td>133</td>
</tr>
<tr>
<td>Assigning G Suite groups to G Suite groups</td>
<td>134</td>
</tr>
<tr>
<td>Deleting G Suite groups</td>
<td>135</td>
</tr>
<tr>
<td>G Suite products and SKUs</td>
<td>135</td>
</tr>
<tr>
<td>Editing master data for G Suite products and SKUs</td>
<td>136</td>
</tr>
<tr>
<td>General master data for G Suite products and SKUs</td>
<td>136</td>
</tr>
<tr>
<td>Additional tasks for managing G Suite products and SKUs</td>
<td>137</td>
</tr>
<tr>
<td>Overview of G Suite products and SKUs</td>
<td>138</td>
</tr>
<tr>
<td>Assigning extended properties to G Suite products and SKUs</td>
<td>138</td>
</tr>
<tr>
<td>G Suite organizations</td>
<td>138</td>
</tr>
<tr>
<td>Creating G Suite organizations</td>
<td>139</td>
</tr>
<tr>
<td>Editing master data for G Suite organizations</td>
<td>139</td>
</tr>
<tr>
<td>General master data for G Suite organizations</td>
<td>139</td>
</tr>
<tr>
<td>Additional tasks for managing G Suite organizations</td>
<td>140</td>
</tr>
<tr>
<td>Overview of G Suite organizations</td>
<td>140</td>
</tr>
<tr>
<td>Moving G Suite organizations</td>
<td>140</td>
</tr>
<tr>
<td>Deleting G Suite organizations</td>
<td>141</td>
</tr>
<tr>
<td>G Suite domains</td>
<td>141</td>
</tr>
<tr>
<td>G Suite domain aliases</td>
<td>142</td>
</tr>
<tr>
<td>G Suite admin roles</td>
<td>142</td>
</tr>
<tr>
<td>Creating G Suite admin roles</td>
<td>142</td>
</tr>
<tr>
<td>Editing master data for G Suite admin roles</td>
<td>143</td>
</tr>
<tr>
<td>General master data for G Suite admin roles</td>
<td>143</td>
</tr>
<tr>
<td>Additional tasks for managing G Suite admin roles</td>
<td>144</td>
</tr>
<tr>
<td>Overview of G Suite admin roles</td>
<td>144</td>
</tr>
<tr>
<td>Assigning admin privileges to G Suite admin roles</td>
<td>144</td>
</tr>
<tr>
<td>Deleting G Suite admin roles</td>
<td>145</td>
</tr>
<tr>
<td>G Suite admin privileges</td>
<td>145</td>
</tr>
<tr>
<td>Display master data for G Suite admin privileges</td>
<td>146</td>
</tr>
<tr>
<td>Additional tasks for managing G Suite admin privileges</td>
<td>146</td>
</tr>
<tr>
<td>Overview of G Suite admin privileges</td>
<td>146</td>
</tr>
<tr>
<td>Assigning G Suite admin privileges to admin roles</td>
<td>147</td>
</tr>
<tr>
<td>G Suite admin role assignments</td>
<td>147</td>
</tr>
<tr>
<td>Creating G Suite admin role designations</td>
<td>147</td>
</tr>
</tbody>
</table>
Mapping G Suite in One Identity Manager

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 Google Inc. REST APIs. The synchronization server ensures data is compared between the One Identity Manager database and G Suite.
One Identity Manager users for managing G Suite

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

Table 1: User

<table>
<thead>
<tr>
<th>User</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target system admin-</td>
<td>Target system administrators must be assigned to the **Target systems</td>
</tr>
<tr>
<td>istrators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Administrate application roles for individual target systems types.</td>
</tr>
<tr>
<td></td>
<td>• Specify the target system manager.</td>
</tr>
<tr>
<td></td>
<td>• Set up other application roles for target system managers if required.</td>
</tr>
<tr>
<td></td>
<td>• Specify which application roles for target system managers are mutually exclusive.</td>
</tr>
<tr>
<td>User</td>
<td>Tasks</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>• Authorize other employee to be target system administrators.</td>
</tr>
<tr>
<td></td>
<td>• Do not assume any administrative tasks within the target system.</td>
</tr>
</tbody>
</table>
| Target system managers | Target system managers must be assigned to **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 entitlements for adding to the IT Shop. |
|      | • Can add employees, who have an other identity than the **Primary identity**. |
|      | • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. |
|      | • Edit the synchronization's target system types and outstanding objects. |
|      | • Authorize other employees within their area of responsibility as target system managers and create child application roles if required. |
| One Identity Manager administrators | • Create customized permissions groups for application roles for role-based login to administration tools in Designer as required. |
|      | • Create system users and permissions groups for non-role-based login to administration tools in Designer as required. |
|      | • Enable or disable additional configuration parameters in Designer as required. |
|      | • Create custom processes in Designer as required. |
|      | • Create and configures schedules as required. |
|      | • Create and configure password policies as required. |
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 Base data | General | Configuration parameters in Designer.

For more information, see Appendix: Configuration parameters for managing G Suite on page 163.
Synchronizing G Suite

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.

This sections explains:

- how to set up synchronization to import initial data from G Suite to the One Identity Manager database,
- how to adjust a synchronization configuration, for example, to synchronize different customers with the same synchronization project,
- how to start and deactivate the synchronization,
- how to evaluate the synchronization results.

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

Detailed information about this topic

- Setting up the initial synchronization of G Suite on page 13
- Adjusting the synchronization configuration for G Suite environments on page 26
- Executing a synchronization on page 37
- Troubleshooting on page 43
- Appendix: Editing G Suite system objects on page 169

Setting up the initial synchronization of G Suite

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

**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 components for managing G Suite environments 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 14
- [System requirements for the G Suite synchronization server](#) on page 17
- [Creating a synchronization project for initial synchronization of G Suite](#) on page 20
- [Appendix: Configuration parameters for managing G Suite](#) on page 163
- [Appendix: Default project templates for G Suite](#) on page 165

**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**

<table>
<thead>
<tr>
<th>User</th>
<th>Permissions</th>
</tr>
</thead>
</table>
| User for accessing the target system (synchronization user) | You must provide at least one user with super-user permissions and a service account for authentication for full synchronization of 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 |
<table>
<thead>
<tr>
<th>User</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User for accessing the One Identity Manager database</td>
<td>The <strong>Synchronization</strong> default system user is provided for executing synchronization with an application server.</td>
</tr>
</tbody>
</table>
| One Identity Manager Service user account | The user account for One Identity Manager Service requires rights to carry out operations at file level, for example, assigning user rights and creating and editing directories and files.  
The user account must belong to the **Domain users** group.  
The user account must have the **Login as a service** extended user right  
The user account requires access rights to the internal web service.  

**NOTE:** If 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:  
```plaintext  
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 Permissions  
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 various API scopes in the Google Admin console: A list of API scopes is available on the One Identity Manager installation medium. You can use this list as a copy template.  
Directory: Modules\GAP\dvd\AddOn\ApiAccess  
File: GSuiteRequiredAPIAccess.txt
Related topics
- Appendix: API scopes for the service account on page 167
- Advanced settings for system connection to G Suite on page 30

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
2. Log in as the G Suite super admin.
3. Select a project or create a new one.
4. Enable the APIs Admin SDK, Enterprise License Manager API and Groups Settings API.
5. Create a service account.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td></td>
</tr>
<tr>
<td>Provide new private key</td>
<td>Enabled</td>
</tr>
<tr>
<td>Key type</td>
<td>JSON</td>
</tr>
<tr>
<td>Activate cross-domain G Suite delegation</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

6. Note the service account's client ID.
   You will need it for setting up the API privileges.
7. Save the key file locally.
   You will need it for creating the synchronization project.

To enable API access and authorize the service account's client ID for the required API scopes
1. Open the Google Admin console (https://admin.google.com).
2. Log in as the 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 the target system (synchronization user) on page 14.

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 G Suite synchronization server

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

The One Identity Manager Service with the G Suite connector must be installed on the synchronization server.

Detailed information about this topic

- System requirements for the G Suite synchronization server on page 17
- Installing the One Identity Manager Service on page 18

System requirements for the G Suite 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
  Following versions are supported:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- Microsoft .NET Framework Version 4.7.2 or later

NOTE: Take the target system manufacturer’s recommendations into account.
Installing the One Identity Manager Service

The One Identity Manager Service with the G Suite connector must be installed on the synchronization server. The synchronization server must be known as a Job server in the One Identity Manager.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server function</td>
<td>G Suite connector</td>
</tr>
<tr>
<td>Machine role</td>
<td>Server</td>
</tr>
</tbody>
</table>

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

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

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

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

For remote installation of One Identity Manager Service, you require an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

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

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the Database connection page.
3. Specify the server on which you want to install One Identity Manager Service on the Server properties page.
a. Select a Job server from the **Server** menu.
   - OR -
   To create a new Job server, click **Add**.

b. Enter the following data for the Job server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</td>
</tr>
<tr>
<td>Queue</td>
<td>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.</td>
</tr>
<tr>
<td>Full server name</td>
<td>Full server name in accordance with DNS syntax. Example: &lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</td>
</tr>
</tbody>
</table>

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

4. Select **G Suite** on the **Machine roles** page.

5. Select **G Suite connector** on the **Server functions** page.

6. Check the One Identity Manager Service configuration on the **Service settings** page.

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

7. To configure remote installations, click **Next**.

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

9. Select the directory with the install files on **Select installation source**.

10. Select the file with the private key on the page **Select private key file**.

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

11. Enter the service's installation data on the **Service access** page.
<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Server on which to install and start the service from.</td>
</tr>
<tr>
<td>To select a server</td>
<td>• Enter a name for the server.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>• Select a entry from the list.</td>
</tr>
<tr>
<td>Service account</td>
<td>User account data for the One Identity Manager Service.</td>
</tr>
<tr>
<td>To enter a user account for the One Identity Manager Service</td>
<td>• Set the option Local system account.</td>
</tr>
<tr>
<td></td>
<td>This starts the One Identity Manager Service under the NT AUTHORITY\SYSTEM account.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>• Enter user account, password and password confirmation.</td>
</tr>
<tr>
<td>Installation account</td>
<td>Data for the administrative user account to install the service.</td>
</tr>
<tr>
<td>To enter an administrative user account for installation</td>
<td>• Enable Advanced.</td>
</tr>
<tr>
<td></td>
<td>• Enable Current user.</td>
</tr>
<tr>
<td></td>
<td>This uses the user account of the current user.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>• Enter user account, password and password confirmation.</td>
</tr>
</tbody>
</table>

12. Click **Next** to start installing the service. Installation of the service occurs automatically and may take some time.

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

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

**Creating a synchronization project for initial synchronization of 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.

Information required for setting up a synchronization project

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

Table 7: Information required for setting up a synchronization project

<table>
<thead>
<tr>
<th>Data</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary domain</td>
<td>Name of this G Suite's primary domain.</td>
</tr>
<tr>
<td>Service account’s key file</td>
<td>JSON key file that was saved when the service account was set up.</td>
</tr>
<tr>
<td>Super admin email addresses for logging in</td>
<td>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 14.</td>
</tr>
<tr>
<td>Synchronization server for G Suite</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 8: Additional properties for the Job server

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server function</td>
<td>G Suite connector</td>
</tr>
<tr>
<td>Machine role</td>
<td>Server/Job server/G Suite</td>
</tr>
</tbody>
</table>

For more information, see System requirements for the G Suite synchronization server on page 17.
### Creating an initial synchronization project for G Suite

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

- executed In default mode, and
- started from the launchpad

If you execute the project wizard in expert mode or directly from Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.
To set up 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 Target system type G Suite and click Start.
   This starts the Synchronization Editor’s project wizard.

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

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

4. On the Primary domain and service account page, enter the primary domain of the G Suite account and the key file for the service account.

   Table 9: Login information for connection to G Suite

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary domain</td>
<td>Name of this G Suite's primary domain.</td>
</tr>
<tr>
<td>Service account's key file</td>
<td>JSON key file saved when the service account was set up.</td>
</tr>
<tr>
<td></td>
<td>- Drag and drop the key on the field to load it.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Click Open key file and select the path to the key file.</td>
</tr>
</tbody>
</table>

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 and a check is run on whether the correct API scopes are authorized.

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

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

   **NOTE:** If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not shown if a synchronization project already exists.

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

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

    **Table 10: Specify target system access**

    | Option                          | Meaning                                                                 |
    |---------------------------------|-------------------------------------------------------------------------|
    | Read-only access to target system. | Specifies whether a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics:  
      - Synchronization is in the direction of **One Identity Manager**.  
      - Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**. |
    | Read/write access to target system. Provisioning available. | Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics:  
      - Synchronization is in the direction of the **Target system**.  
      - Processing methods are only defined in the synchronization steps for synchronization in the direction of the **Target system**. |
11. Select the synchronization server to execute synchronization on the Synchronization server page.

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

a. Click  to add a new Job server.

b. Enter a name for the Job server and the full server name conforming to DNS syntax.

c. Click OK.

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

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

12. To close the project wizard, click Finish.

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

The synchronization project is created, saved and enabled immediately.

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

**NOTE:** The connection data for the target system is saved in a variable set and can be modified under Configuration | Variables in Synchronization Editor.

### Related topics

- Configuring the synchronization log on page 26
- Adjusting the synchronization configuration for G Suite environments on page 26
- Appendix: Default project templates for G Suite on page 165
- Appendix: API scopes for the service account on page 167
Configuring the synchronization log

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

To configure the content of the synchronization log

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

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

5. Click OK.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- Displaying synchronization results on page 38

Adjusting the synchronization configuration for G Suite environments

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.

NOTE: If you want to change the configuration of existing synchronization projects, check the possible effects of these changes on the data that has already been synchronized.
You must customize the synchronization configuration in order to compare the database with the G Suite regularly and to synchronize changes.

- To use One Identity Manager as the master system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- 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 that 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 for synchronizing 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.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.
- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema. Include the schema extensions in the mapping.

For more 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 27
- Configuring synchronization of different customers on page 28
- Updating schemas on page 29
- Advanced settings for system connection to G Suite on page 30

**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). To use One Identity Manager as the master system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.
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. Creates a workflow with **Target system** as its synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related topics
- Configuring synchronization of different customers on page 28

Configuring synchronization of different customers

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

**Prerequisites**
- The customer target systems schema are identical.
- All virtual schema properties used in the mapping must exist in the customer’s extended schemas.
- The connection parameters to the target system are defined as variables.

To customize a synchronization project for synchronizing another customer

1. Supply a user in the customer with sufficient permissions for accessing the G Suite.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other customer. Use the wizards to attach a base object.
   - In the wizard, select the G Suite connector and declare the connection parameters. The connection parameters are saved in a special variable set.
   - A start up configuration is created, which uses the newly created variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.
Updating schemas

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

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

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

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

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select Configuration | Target system.
   - OR -
   Select Configuration | One Identity Manager Connection.
3. Select the view General and click Update schema.
4. Confirm the security prompt with Yes.
   This reloads the schema data.
To edit a mapping

1. Select the category Mappings.
2. Select a mapping in the navigation view.

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

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

Speeding up synchronization with revision filtering

Synchronization with G Suite does not support revision filtering.

Advanced settings for system connection to G Suite

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 the variable set on page 33.

b. Edit the target system connection with the system connection wizard and change the effected values.
   The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.
   For more information, see Editing target system connection properties on page 34.

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 11: Target system connection advanced settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only API access</td>
<td>Specifies if the API scopes were only entered for read-only access in the G Suite Admin Console. Enable this option if no write access to the target system may be assigned. The connector only has read access to the target system.</td>
</tr>
<tr>
<td></td>
<td>- The service account's client ID must be authorized for various API scopes in the Google Admin console. A list of API scopes is available on the One Identity Manager installation medium. You can use this list as a copy template.</td>
</tr>
<tr>
<td></td>
<td>Directory: Modules\GAP\dvd\AddOn\ApiAccess</td>
</tr>
<tr>
<td></td>
<td>File: GSuiteRequiredAPIAccessReadOnly.txt</td>
</tr>
<tr>
<td></td>
<td>If this option is disabled, read-write access is possible. Other API scopes must be authorized for this.</td>
</tr>
<tr>
<td>Use the local cache</td>
<td>Specifies whether the G Suite connector's local cache is used.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This option is set by default and can be disabled for troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>For detailed information, see One Identity Manager Target System Synchronization Reference Guide.</td>
</tr>
<tr>
<td>Polling count</td>
<td>Specifies how many attempts are made to load a new value into the target system during provisioning or synchronization before an error occurs.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Batch retry count</td>
<td>Specifies the number of retries allowed for failed batch operations in the target system, for example, when synchronizing group memberships.</td>
</tr>
<tr>
<td>Batch timeout</td>
<td>Timeout between retries of failed batch operations.</td>
</tr>
<tr>
<td>Transfer user data before delete</td>
<td>Specifies whether user data is transferred to a different user account before user accounts are deleted.</td>
</tr>
<tr>
<td></td>
<td>User data such as Google Drive data, Google+ pages, and Google calendar, can be transferred to a different user account before final deletion.</td>
</tr>
<tr>
<td></td>
<td>Variable: CP_TransferUserDataBeforeDelete</td>
</tr>
<tr>
<td>Default email</td>
<td>Default email address of the destination user account for the transfer of user data when a user account is deleted. The email address of the destination</td>
</tr>
</tbody>
</table>
### Property Description

**address for data transfer**
- User account belongs to the primary domain of the customer to which the deleted user account belongs.
- This email address is used if no email address can be determined via the manager of the deleted user account.
- Variable: CP_DefaultDataTransferTargetEmail

**Products and SKUs XML**
- Product IDs and Stock keeping unit IDs as XML file.
- The list of available products and SKUs is defined by Google and therefore fixed in the 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:
    ```xml
    <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>
    ```

### Related topics
- Transferring user data to a different G Suite user account on page 126
- Appendix: API scopes for the service account on page 167
- Users and permissions for synchronizing with G Suite on page 14
Editing connection parameters in the variable set

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 your 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 Configuration | Target system.
3. Open the Connection parameters view.
   Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select one of the following parameters and click Convert.
   - Polling count
   - Batch retry count
   - Batch timeout
   - Use the local cache
   - Read-only API access

   For more information, see Advanced settings for system connection to G Suite on page 30.
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 $\rightarrow$ in the variable set view's toolbar.
   - To rename the variable set, select the variable set and click the variable set view in the toolbar $\rightarrow$. 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 $\rightarrow$.
   - 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 variable sets, or restoring default values and adding base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

**Editing target system connection properties**

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

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

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

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

**To edit advanced settings with the system connection wizard**

1. Open the synchronization project in the Synchronization Editor.

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

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

3. Select **Configuration | Target system**.

4. Click **Edit connection**.

   This starts the system connection wizard.

5. Enable **Show advanced options** on the system connection wizard’s start page.

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

   - When you test the connection, a check is carried out to verify if the appropriate API scopes are authorized.
   - For more information, see Advanced settings for system connection to G Suite on page 30.

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

   - For more information, see Advanced settings for system connection to G Suite on page 30.
8. Customize the properties as required on the **Advanced settings** page.
   For more information, see Advanced settings for system connection to G Suite on page 30.

9. Save the changes.

### Configuring the provisioning of memberships

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

- Memberships are saved in the target system as an object property in list form (Example: List of user accounts in the Members property of 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. In Manager, select **G Suite | Basic configuration data | Target system types**.
2. Select **G Suite** in the result list.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
   - This option can only be enabled for assignment tables that have a base table with XDateSubItem or CCC_XDateSubItem column.
   - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Enable merging**.
6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and the members list does not get entirely overwritten.
NOTE: The complete members list is updated by synchronization. During this process, objects with changes but incomplete provisioning are not handled. These objects are logged in the synchronization log.

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

Configuring single object synchronization

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

Prerequisites

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

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

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

1. In Manager, select G Suite | Basic configuration data | Target system types.
2. In the result list, select the target system type G Suite.
3. Select Assign synchronization tables.
4. In Add assignments, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select Configure tables for publishing.
7. Select the custom table and enter the Root object path.
   Enter the path to the base object in the ObjectWalker notation of the VI.DB.
   Example: FK(UID_GAPCustomer).XObjectKey
8. Save the changes.
Executing a synchronization

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

Starting synchronization

When setting up the initial synchronization project using the Launchpad, a default schedule for regular synchronizations is created and assigned. To execute regular synchronizations, activate this schedule.

To synchronize on a regular basis

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

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

To start initial synchronization manually

1. Open the synchronization project in the Synchronization Editor.
2. Select the category Configuration | Start up configurations.
3. Select a startup configuration in the document view and click **Execute**.
4. Confirm the security prompt with **Yes**.

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

- If another synchronization is started with the same startup configuration, this process is stop and is assigned the **Frozen** execution status. An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another startup 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 startup configuration.
  - Use the schedule to ensure that the startup configurations are executed in sequence.
  - Group startup configurations with the same startup behavior.

### Displaying synchronization results

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

**To display a synchronization log**

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

**To display a provisioning log.**

1. Open the synchronization project in the Synchronization Editor.
2. Select **Logs**.
3. Click ⚡ in the navigation view toolbar.
   - Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking 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.

Related topics
- Configuring the synchronization log on page 26
- Troubleshooting on page 43

Deactivating synchronization

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

To prevent regular synchronization
1. Open the synchronization project in the Synchronization Editor.
2. Select the start up configuration and deactivate the configured schedule.
   Now you can only start synchronization manually.

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

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

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

Synchronizing single objects

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

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

1. In Manager, select the G Suite category.
2. Select the object type in the navigation view.
3. In the result list, select the object that you want to synchronize.
4. Select Synchronize this object.
   A process for reading this object is entered in the job queue.

**NOTE:** The Synchronize this object task is executed for the object selected in the results list. If you want to synchronize changes to memberships, execute the single object synchronization on the base object of the assignment.

Example:
An admin role was assigned to a user in the target system. To synchronize this assignment, in Manager select the admin role assignment to which the user account was assigned, and execute single object synchronization. When you do this, all memberships for this admin role assignment are synchronized. If single object synchronization is executed in the user account, no memberships are synchronized, as the GAPUser table does not represent the base table of the assignment.

The base table of an assignment contains an XDateSubItem column containing information about the last change to the memberships.

Detailed information about this topic

- Configuring single object synchronization on page 36

Tasks after a synchronization

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

- Post-processing outstanding objects on page 40
- Managing user accounts through account definitions on page 43

Post-processing outstanding objects

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

Outstanding objects
• Cannot be edited in One Identity Manager.
• Are ignored by subsequent synchronization.
• Are ignored by inheritance calculations.

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

Start target system synchronization to do this.

**To post-process outstanding objects**

1. In Manager, select the **G Suite | Target system synchronization: G Suite** category.
   
   All tables assigned to the target system type **G Suite** as synchronization tables are displayed in the navigation view.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.
   
   All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was executed. The **No log available** entry can mean the following:
   
   - The synchronization log has already been deleted.
   - OR -
   - An assignment from a member list has been deleted in the target system.
   
   The base object of the assignment has been updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

   - An object that contains a member list has been deleted in the target system.
   
   During synchronization, the object and all corresponding entries in assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.

   **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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🗑️</td>
<td>Delete</td>
<td>The object is immediately deleted in the One Identity Manager database. Deferred deletion is not taken into account. The Outstanding label is removed for the object. Indirect memberships cannot be deleted.</td>
</tr>
</tbody>
</table>
| 📢 | Publish | The object is added in the target system. The Outstanding label is removed for the object. The method triggers the HandleOutstanding event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites:  
  - The table containing the object can be published.  
  - The target system connector has write access to the target system. |
| 🔄 | Reset | The Outstanding label is removed for the object. |

5. Confirm the security prompt with Yes.

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

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

**To disable bulk processing**

- Deactivate 🗑️ in the form toolbar.

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

 Related topics

- Adding custom tables to the target system synchronization on page 43
- Advanced settings for system connection to G Suite on page 30
Adding custom tables to the target system synchronization

You must customize synchronization to synchronize custom tables.

To add tables to the target system synchronization

1. In Manager, select G Suite | Basic configuration data | Target system types.
2. In the result list, select the target system type G Suite.
3. Select Assign synchronization tables.
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 Publishable.
8. Save the changes.

Related topics

- Post-processing outstanding objects on page 40

Managing user accounts through account definitions

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

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

Detailed information about this topic

- Assigning account definitions to linked user accounts on page 69

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.
Simulating synchronization
The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.

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

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

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

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

Related topics
- Displaying synchronization results on page 38
Managing G Suite user accounts and employees

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employee in all of the connected target systems. One Identity Manager provides the possibility to manage user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

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

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a customer, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

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

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

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

For more detailed information about employee handling and administration, see the One Identity Manager Target System Base Module Administration Guide.
Related topics

- Account definitions for G Suite user accounts on page 46
- Automatic assignment of employees to G Suite user accounts on page 64
- Editing master data for G Suite user accounts on page 112

Account definitions for G Suite user accounts

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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

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.

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

The following steps are required to implement an account definition:

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

Detailed information about this topic

- Creating account definitions on page 47
- Editing manage levels on page 49
- Creating mapping rules for IT operating data on page 52
- Entering IT operating data on page 53
- Assigning account definitions to employees on page 56
- Assigning account definitions to target systems on page 61
Creating account definitions

To create a new account definition

1. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.
2. Click in the result list.
3. On the master data form, enter the master data for the account definition.
4. Save the changes.

Related topics

- Master data for account definitions on page 47
- Editing account definitions on page 47

Editing account definitions

To edit an account definition

1. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Change master data.
4. Enter the account definition's master data.
5. Save the changes.

Related topics

- Master data for account definitions on page 47
- Creating account definitions on page 47

Master data for account definitions

Enter the following data for an account definition:

Table 13: Master data for an account definition

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Account definition name.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>definition</td>
<td>Table in the One Identity Manager schema that maps user accounts.</td>
</tr>
<tr>
<td>User account table</td>
<td>Target system to which the account definition applies.</td>
</tr>
<tr>
<td>Target system</td>
<td>Required account definition. Define the dependencies between . When this is requested or assigned, the required is automatically requested or assigned with it. Leave empty for G Suite.</td>
</tr>
<tr>
<td>Required account definition</td>
<td>Description Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Manage level (initial)</td>
<td>Manage level to use by default when you add new user accounts.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the configuration parameter QER</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>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 also be assigned directly to employees and roles outside of IT Shop.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>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.</td>
</tr>
<tr>
<td>Automatic assignment to employees</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable this option to remove automatic assignment of the account</td>
<td>Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</td>
</tr>
<tr>
<td>definition to all employees.</td>
<td></td>
</tr>
<tr>
<td>Disable this option to remove automatic assignment of the account</td>
<td>Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</td>
</tr>
<tr>
<td>definition to all employees.</td>
<td></td>
</tr>
<tr>
<td>Disable this option to remove automatic assignment of the account</td>
<td>Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.</td>
</tr>
<tr>
<td>definition to all employees.</td>
<td></td>
</tr>
<tr>
<td>Retain account definition if permanently disabled</td>
<td>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.</td>
</tr>
<tr>
<td>Retain account definition if temporarily disabled</td>
<td>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.</td>
</tr>
<tr>
<td>Retain account definition on deferred deletion</td>
<td>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.</td>
</tr>
<tr>
<td>Retain account definition on security risk</td>
<td>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.</td>
</tr>
<tr>
<td>Resource type</td>
<td>Resource type for grouping account definitions.</td>
</tr>
<tr>
<td>Spare field 01 - spare field 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

**Editing manage levels**

One Identity Manager supplies a default configuration for manage levels:
- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the employee but they do no inherit any further 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 the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee’s properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

**To edit a manage level**

1. In Manager, select **G Suite | Basic configuration data | Account definitions | Manage levels**.
2. Select the manage level in the result list.
3. Select **Change master data**.
4. Edit the manage level’s master data.
5. Save the changes.

**Related topics**

- Master data for manage levels on page 51
- Creating manage levels on page 50

**Creating manage levels**

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

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

**To create a manage level**

1. In Manager, select **G Suite | Basic configuration data | Account definitions | Manage levels**.
2. Click 📝 in the result list.
3. On the master data form, edit the master data for the manage level.
4. Save the changes.
Related topics

- Master data for manage levels on page 51
- Editing manage levels on page 49

Master data for manage levels

Enter the following data for a manage level.

Table 14: Master data for manage levels

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage level</td>
<td>Name of the manage level.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>IT operating data overwrites</td>
<td>Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Never</strong>: Data is not updated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Always</strong>: Data is always updated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Only initially</strong>: The data is only determined at the start.</td>
</tr>
<tr>
<td>Retain groups if temporarily disabled</td>
<td>Specifies whether user accounts of temporarily disabled employees retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if temporarily disabled</td>
<td>Specifies whether user accounts of temporarily disabled employees are locked.</td>
</tr>
<tr>
<td>Retain groups if permanently disabled</td>
<td>Specifies whether user accounts of permanently disabled employees retain group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if permanently disabled</td>
<td>Specifies whether user accounts of permanently disabled employees are locked.</td>
</tr>
<tr>
<td>Retain groups on deferred deletion</td>
<td>Specifies whether user accounts of employees marked for deletion retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if deletion is deferred</td>
<td>Specifies whether user accounts of employees marked for deletion are locked.</td>
</tr>
<tr>
<td>Retain groups on security risk</td>
<td>Specifies whether user accounts of employees posing a security risk retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if security is at risk</td>
<td>Specifies whether user accounts of employees posing a security risk are locked.</td>
</tr>
<tr>
<td>Retain groups if user account disabled</td>
<td>Specifies whether locked user accounts retain their group memberships.</td>
</tr>
</tbody>
</table>
Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the 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 at next login

To create a mapping rule for IT operating data

1. In Manager, select 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** and enter the following data.

**Table 15: Mapping rule for IT operating data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the <em>One Identity Manager Target System Base Module Administration Guide</em>.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies which roles to use in order to find the user account properties. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>- Primary department</td>
</tr>
<tr>
<td></td>
<td>- Primary location</td>
</tr>
<tr>
<td></td>
<td>- Primary cost center</td>
</tr>
<tr>
<td></td>
<td>- Primary business roles</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only use the primary business role if the Business Roles Module is installed.</td>
</tr>
<tr>
<td></td>
<td>- Empty</td>
</tr>
<tr>
<td></td>
<td>If you select a role, you must specify a default value and set the option <strong>Always use default value</strong>.</td>
</tr>
<tr>
<td>Default value</td>
<td>Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.</td>
</tr>
<tr>
<td>Always use default value</td>
<td>Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.</td>
</tr>
<tr>
<td>Notify when applying the standard</td>
<td>Specifies whether email notification to a defined mailbox is sent when the default value is used. The <strong>Employee - new user account with default properties created</strong> mail template is used. To change the mail template, adjust the **TargetSystem</td>
</tr>
</tbody>
</table>

4. Save the changes.

**Entering IT operating data**

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

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

**Example**

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

Create an account definition A for the default user account of the customer A and an account definition B for the administrative user account of customer A. 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 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 define IT operating data**

1. In Manager, select the role in the Organizations or Business roles category.
2. Select the Edit IT operating data task.
3. Click **Add** and enter the following data.

**Table 16: IT operating data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects on</td>
<td>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.</td>
</tr>
<tr>
<td>To specify an</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td></td>
</tr>
<tr>
<td>scope</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>Click ➔ next to the text box.</td>
</tr>
<tr>
<td>b.</td>
<td>Under <strong>Table</strong>, select the table that maps the target system for select the TSBAccountDef table for an account definition.</td>
</tr>
<tr>
<td>c.</td>
<td>Select the specific target system or account definition under <strong>Effects on</strong>.</td>
</tr>
<tr>
<td>d.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>User account property for which the value is set.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the menu,</td>
<td>you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the One Identity Manager Target System Base Module Administration Guide.</td>
</tr>
<tr>
<td>Value</td>
<td>Concrete value which is assigned to the user account property.</td>
</tr>
</tbody>
</table>

4. Save the changes.

**Related topics**

- Creating mapping rules for IT operating data on page 52

**Modify 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 effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

**Prerequisites**

- The IT operating data of a department, 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. In Manager, select 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 that the object property would have following modification of the IT operating data.

   Selection: Specifies whether the modification shall be adopted for 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).

NOTE: As long as an account definition for an employee is valid, the employee retains
the user account that was created by it. If the assignment of an account definition is
removed, the user account that was created from this account definition is deleted.

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

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In Manager, select 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 centers tab.
   TIP: In the Remove assignments area, you can remove the assignment of
   organizations.
   To remove an assignment
   - Select the organization and double click ✓.
5. Save the changes.

Assigning account definitions to business roles

Installed modules: Business Roles Module
To add account definitions to hierarchical roles

1. In Manager, select 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.
   
   **TIP:** In the Remove assignments area, you can remove the assignment of business roles.
   
   **To remove an assignment**
   - Select the business role and double click 🗑️.
5. Save the changes.

Assigning account definitions to all employees

To assign an account definition to all employees

1. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Change master data.
4. Set Automatic assignment to employees on General.
   
   **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 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.
Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In Manager, select 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.
   
   TIP: In the Remove assignments area, you can remove the assignment of employees.
   
   To remove an assignment
   - Select the employee and double-click ✓.
5. Save the changes.

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

1. In Manager, select 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.
   
   TIP: In the Remove assignments area, you can remove the assignment of system roles.
   
   To remove an assignment
   - Select the system role and double click ✓.
5. Save the changes.
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.

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

- If the account definition is only assigned to employees using IT Shop assignments, you must also set 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. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions (non-role-based login).
   - OR -
   In Manager, select Entitlements | Account definitions (role-based login).
2. Select an account definition in the result list.
3. Select Add to IT Shop.
4. Assign the account definitions to the IT Shop shelves in Add assignments.
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions (non-role-based login).
   - OR -
   In Manager, select Entitlements | Account definitions (role-based login).
2. Select an account definition in the result list.
3. Select Add to IT Shop.
4. Remove the account definitions from the IT Shop shelves in Remove assignments.
5. Save the changes.
To remove an account definition from all IT Shop shelves

1. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions (non-role-based login).
   - OR -
   In Manager, select Entitlements | Account definitions (role-based login).
2. Select an account definition in the result list.
3. Select Remove from all shelves (IT Shop).
4. Confirm the security prompt with Yes.
5. Click OK.

The account definition is removed from all shelves by 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 account definitions on page 47

Assigning account definitions to target systems

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 (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. In Manager, select the customer in G Suite | Customers.
2. Select Change master data.
3. Select the account definition for user accounts from Account definition (initial).
4. Save the changes.

Related topics
- Automatic assignment of employees to G Suite user accounts on page 64
Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
   a. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Change master data.
   d. Disable Automatic assignment to employees on the General tab.
   e. Save the changes.

2. Remove direct assignments of the account definition to employees.
   a. In Manager, select 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. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Assign organizations.
   d. In Remove assignments, remove the relevant departments, cost centers, and locations.
   e. Save the changes.

4. Remove the account definition’s assignments to business roles.
   a. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Assign business roles.
      Remove the business roles in 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 about unsubscribing requests, see the One Identity Manager Web Portal User Guide.

To remove an account definition from all IT Shop shelves

a. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions (non-role-based login).

   - OR -

   In Manager, select Entitlements | Account definitions (role-based login).

b. Select an account definition in the result list.

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

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

e. Click **OK**.

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

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. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.

   b. Select an account definition in the result list.

   c. Select **Change master data**.

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

   e. Save the changes.

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

   a. In Manager, select the customer in G Suite | Customers.

   b. Select **Change master data**.

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

   d. Save the changes.

8. Delete the account definition.

   a. In Manager, select G Suite | Basic configuration data | Account definitions | Account definitions.

   b. Select an account definition in the result list.

   c. Click to delete an account definition.
Automatic assignment of employees to G Suite user accounts

When you add a user account, an existing employee can be assigned automatically. This mechanism can follow on after a new user account has been created manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account’s target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

NOTE: It is not recommended to assign employees using automatic employee assignment in the case of administrative user accounts. Use Change master data to assign employees to administrative user account for the respective user account.

Run the following tasks to assign employees automatically.

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

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

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

Example:

ADMINISTRATOR*

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

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

- Define the search criteria for employee assignment to this customer.
NOTE:
The following applies for synchronization:
- Automatic employee assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:
- Automatic employee assignment takes effect if user accounts are added.

NOTE:
Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the customer is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

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

For more information, see Managing user accounts through account definitions on page 43.

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

Related topics
- Creating account definitions on page 47
- Assigning account definitions to target systems on page 61
- Changing the manage level in G Suite user accounts on page 68
- Editing search criteria for automatic employee assignment on page 65

### Editing search criteria for automatic employee assignment

The criteria for employee assignment are defined for the customer. In this case, you specify which user account properties must match the employee’s properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (AccountToPersonMatchingRule) in the GAPCustomer table.

Search criteria are evaluated when employees are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly.
NOTE: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account’s target system. You can customize user account properties depending on how the behavior of the manage level is defined.

It is not recommended to make assignment to administrative user accounts based on search criteria. Use Change master data to assign employees to administrative user account for the respective user account.

To specify criteria for employee assignment

1. In Manager, select G Suite | G Suite customers.
2. Select the customer in the result list.
3. Select Define search criteria for employee assignment in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 17: Standard search criteria for user accounts

<table>
<thead>
<tr>
<th>Apply to</th>
<th>Column for employee</th>
<th>Column for user account</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite user accounts</td>
<td>Default email address</td>
<td>Primary email address</td>
</tr>
<tr>
<td></td>
<td>(DefaultEmailAddress)</td>
<td>(PrimaryEmail)</td>
</tr>
</tbody>
</table>

5. Save the changes.

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

Related topics

- Automatic assignment of employees to G Suite user accounts on page 64
- Finding employees and directly assigning them to user accounts on page 66

Finding employees and directly assigning them to user accounts

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

Table 18: Manual Assignment View

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suggested</td>
<td>This view lists all user accounts to which One Identity Manager can assign</td>
</tr>
<tr>
<td>View</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>assignments</td>
<td>an employee. All employees are shown who were found using the search criteria and can be assigned.</td>
</tr>
<tr>
<td>Assigned user accounts</td>
<td>This view lists all user accounts to which an employee is assigned.</td>
</tr>
<tr>
<td>Without employee assignment</td>
<td>This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.</td>
</tr>
</tbody>
</table>

**To apply search criteria to user accounts**

1. In Manager, select **G Suite | G SuiteCustomers**.
2. In the result list, select the customer.
3. Select **Define search criteria for employee assignment** in the task view.
4. At the bottom of the form, click **Reload**.
   All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

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

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

**To assign employees directly over a suggestion list**

- Click **Suggested assignments**.
  1. Click **Selection** for all user accounts to which you want to assign the suggested employees. Multi-select is possible.
  2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
  3. Click **Assign selected**.
  4. Confirm the security prompt with **Yes**.
     The employees determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

- OR -

- Click **No employee assignment**.
  1. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.
2. Click **Selection** for all user accounts to which you want to assign the selected employees. Multi-select is possible.

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

4. Click **Assign selected**.

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

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

**To remove assignments**

- Click **Assigned user accounts**.
  1. Click **Selection** for all user accounts for which you want to delete the employee assignment. Multi-select is possible.
  2. Click **Remove selected**.
  3. Confirm the security prompt with **Yes**.

The assigned employees are removed from the selected user accounts.

**Changing the manage level in G Suite user accounts**

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

**To change the manage level for a user account**

1. In Manager, select **G Suite | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. On the **General** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

**Related topics**

- [General master data for G Suite user accounts](#) on page 113
Assigning account definitions to linked user accounts

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

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

**To select user accounts through account definitions**

1. Create an account definition.
2. Assign an account definition to the customer.
3. Assign the account definition and manage level to user accounts in **linked** status.
   a. In Manager, select **G Suite | User accounts | Linked but not configured | <Customer>**.
   b. Select **Assign account definition to linked accounts**.

**Detailed information about this topic**

- Account definitions for G Suite user accounts on page 46
- Assigning account definitions to target systems on page 61

Manually linking employees to G Suite user accounts

An employee can be linked to multiple G Suite user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One employee can also use default user accounts with different types.

**NOTE:** To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

**To manually assign user accounts to an employee**

1. In Manager, select **Employees | Employees**.
2. Select the employee in the result list and run **G SuiteAssign user accounts** from the task view.
3. Assign the user accounts.
4. Save the changes.

Related topics

- Supported user account types on page 70

Supported user account types

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

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

- Identity

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

<table>
<thead>
<tr>
<th>Identity</th>
<th>Description</th>
<th>Value of the IdentityType column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary identity</td>
<td>Employee's default user account.</td>
<td>Primary</td>
</tr>
<tr>
<td>Organizational identity</td>
<td>Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</td>
<td>Organizational</td>
</tr>
<tr>
<td>Personalized admin identity</td>
<td>User account with administrative permissions, used by one employee.</td>
<td>Admin</td>
</tr>
<tr>
<td>Sponsored identity</td>
<td>User account that is used for training purposes, for example.</td>
<td>Sponsored</td>
</tr>
<tr>
<td>Shared identity</td>
<td>User account with administrative permissions, used by several employees.</td>
<td>Shared</td>
</tr>
<tr>
<td>Service identity</td>
<td>Service account.</td>
<td>Service</td>
</tr>
</tbody>
</table>

**NOTE:** To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.
The primary identity, the organizational identity, and the personal admin identity are used for different user accounts, which can be used by the same actual employee to execute their different tasks within the company.

To provide user accounts with a personal admin identity or an organizational identity for an employee, you create subidentities for the employee. These subidentities are then linked to user accounts, enabling you to assign the required Entitlements to the different user accounts.

User accounts with a sponsored identity, group identity, or service identity are linked to dummy employees that do not refer to a real person. These dummy employees are needed so that Entitlements can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether dummy employees need to be considered separately.

For detailed information about mapping employee identities, see the One Identity Manager Identity Management Base Module Administration Guide.

- Privileged user account
  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column IsPrivilegedAccount).

**Detailed information about this topic**

- Default user accounts on page 71
- Administrative user accounts on page 72
- Providing administrative user accounts for one employee on page 73
- Providing administrative user accounts for several employees on page 74
- Privileged user accounts on page 75

**Default user accounts**

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

**To create default user accounts through account definitions**

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify 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.
3. Create a formatting rule for IT operating data.
   You use the mapping rule to define which rules are used to map the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined via a person's primary roles.

   Which IT operating data is required depends on the target system. The following setting are recommended for default user accounts:
   - In the mapping rule for the IsGroupAccount column, use the default value 1 and enable **Always use default value**.
   - In the mapping rule for the IdentityType column, use the default value **Primary** and enable **Always use default value**.

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.
   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

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

Related topics
- Account definitions for G Suite user accounts on page 46

Administrative user accounts

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

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

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

Related topics
- Providing administrative user accounts for one employee on page 73
- Providing administrative user accounts for several employees on page 74
Providing administrative user accounts for one employee

Prerequisites

- The user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be linked to a main identity.

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
   a. In Manager, select **G Suite | User accounts**.
   b. Select the user account in the result list.
   c. Select **Change master data**.
   d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.

2. Link the user account to the employee who will be using this administrative user account.
   a. In Manager, select **G Suite | User accounts**.
   b. Select the user account in the result list.
   c. Select **Change master data**.
   d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

   🔄 **TIP:** If you are the target system manager, you can choose 🕒 to create a new person.

Related topics

- Providing administrative user accounts for several employees on page 74
- For detailed information about mapping employee identities, see the One Identity Manager Identity Management Base Module Administration Guide.
Providing administrative user accounts for several employees

Prerequisite

- The user account must be labeled as a shared identity.
- A dummy employee must exist. The dummy employee must be labeled as a shared identity and must have a manager.
- The employees who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.
   a. In Manager, select G Suite | User accounts.
   b. Select the user account in the result list.
   c. Select Change master data.

2. Link the user account to a dummy employee.
   a. In Manager, select G Suite | User accounts.
   b. Select the user account in the result list.
   c. Select Change master data.
   d. On the General tab, select the dummy employee from the Employee selection list.

   TIP: If you are the target system manager, you can choose to create a new dummy employee.

3. Assign the employees who will use this administrative user account to the user account.
   a. In Manager, select G Suite | User accounts.
   b. Select the user account in the result list.
   c. Select the task Assign employees authorized to use.
   d. Assign employees in Add assignments.

   TIP: In the Remove assignments area, you can remove the assignment of employees.

To remove an assignment

- Select the employee and double-click.

TIP: One Identity Manager 8.1.1 Administration Guide for Connecting to G Suite
Managing G Suite user accounts and employees
Related topics

- Providing administrative user accounts for one employee
- For detailed information about mapping employee identities, see the One Identity Manager Identity Management Base Module Administration Guide.

Privileged user accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column IsPrivilegedAccount).

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

**To create privileged users through account definitions**

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

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

3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.

4. Create a formatting rule for IT operating data.

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

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

- In the mapping rule for the IsPrivilegedAccount column, use the default value **1** and enable **Always use default value**.
- You can also specify a mapping rule for the IdentityType column. The column owns different permitted values that represent user accounts.
- To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the IsGroupAccount column with a default value of **0** and enable **Always use default value**.
5. Enter the effective IT operating data for the target system.
   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

6. Assign the account definition directly to employees who work with privileged user accounts.
   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

   **TIP:** If customization requires that the primary email addresses of privileged user accounts follow a defined naming convention, create the template according to which the primary email addresses are formed.

**Related topics**

- Account definitions for G Suite user accounts on page 46
Provision of login information for G Suite user accounts

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

Detailed information about this topic

- Password policies for G Suite user accounts on page 77
- Initial password for new G Suite user accounts on page 88
- Email notifications about login data on page 89

Password policies for G Suite user accounts

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 policies apply not only when the user enters a password but also when random passwords are generated.

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

Detailed information about this topic

- Predefined password policies on page 78
- Applying password policies on page 79
- Creating password policies on page 81
- Custom scripts for password requirements on page 84
You can customize predefined password policies to meet your own requirements, if necessary.

**Password for logging in to One Identity Manager**

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy 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).

---

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

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

**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 **Employee central password policy** password policy defines the settings for the (Person.CentralPassword) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

---

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

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

**Password policies for user accounts**

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

---

**IMPORTANT:** If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** standard policy applies. In this case, ensure that the default policy does not violate the target systems requirements.
The **G Suite password policy** is predefined for the customer. You can apply this password policy to customer user accounts (GAPUser.Password).

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

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

### Applying password policies

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

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

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

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

1. Password policy of the account definition of the user account
2. Password policy of the manage level of the user account
3. Password policy for the G Suite customer of the user account
4. Password policy **One Identity Manager password policy** (default policy)

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

**To reassign a password policy**

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

**Table 20: Assigning a Password Policy**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply to</td>
<td>Application scope of the password policy.</td>
</tr>
</tbody>
</table>

**To specify an application scope**

a. Click ➔ next to the text box.

b. Select one of the following references under **Table**:
   - The table that contains the base objects of synchronization.
   - To apply the password policy based on the account definition, select the TSBAccountDef table.
   - Select the TSBBehavior table to apply the password policy based on the manage level.

c. Select the table that contains the base objects under **Apply to**.
   - If you have selected the table containing the base objects of synchronization, next select the specific target system.
   - If you have selected the TSBAccountDef table, next select the specific account definition.
   - If you have selected the TSBBehavior table, next select the specific manage level.

d. Click **OK**.

<table>
<thead>
<tr>
<th>Password column</th>
<th>The password column's identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password policy</td>
<td>The identifier of the password policy to be used.</td>
</tr>
</tbody>
</table>

5. Save the changes.

**To change a password policy's assignment**

1. In the Manager, select the **G Suite | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
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.
Editing password policies

To edit a password policy

1. In the Manager, select the **G Suite | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select **Change master data**.
4. Edit the password policy's master data.
5. Save the changes.

Detailed information about this topic

- **General master data for password policies** on page 81
- **Policy settings** on page 82
- **Character classes for passwords** on page 83
- **Custom scripts for password requirements** on page 84

Creating password policies

To create a password policy

1. In the Manager, select the **G Suite | Basic configuration data | Password policies** category.
2. Click 🗝️ in the result list.
3. On the master data form, enter the master data for the password policy.
4. Save the changes.

Detailed information about this topic

- **General master data for password policies** on page 81
- **Policy settings** on page 82
- **Character classes for passwords** on page 83
- **Custom scripts for password requirements** on page 84

General master data for password policies

Enter the following master data for a password policy.
Table 21: Master data for a password policy

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Password policy name. Translate the given text using the button.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation. Translate the given text using the button.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Custom error message outputted if the policy is not fulfilled. Translate the given text using the button.</td>
</tr>
<tr>
<td>Owner (Application Role)</td>
<td>Application roles whose members can configure the password policies.</td>
</tr>
<tr>
<td>Default policy</td>
<td>Mark as default policy for passwords.</td>
</tr>
</tbody>
</table>

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

Policy settings

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

Table 22: Policy settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial password</td>
<td>Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Minimum length of the password. Specify the number of characters a password must have.</td>
</tr>
<tr>
<td>Max. length</td>
<td>Maximum length of the password. Specify the number of characters a password can have.</td>
</tr>
<tr>
<td>Max. errors</td>
<td>Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has reached the number of</td>
</tr>
</tbody>
</table>
maximum failed logins, the employee or system user can no longer log in to One Identity Manager.

You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the One Identity Manager Web Portal User Guide.

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, for example, a value of 5 is entered, the user's last five passwords are stored.

Minimum password strength | Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1, 2, 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.

Name properties denied | Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the Contains name properties for password check option is set are taken into account. Adjust this option in the column definition in Designer. For more detailed information, see the One Identity Manager Configuration Guide.

Character classes for passwords

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

Table 23: Character classes for passwords

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. number letters</td>
<td>Specifies the minimum number of alphabetical characters the password must contain.</td>
</tr>
<tr>
<td>Min. number lowercase</td>
<td>Specifies the minimum number of lowercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number uppercase</td>
<td>Specifies the minimum number of uppercase letters the password must contain.</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Min. number digits</td>
<td>Specifies the minimum number of digits the password must contain.</td>
</tr>
<tr>
<td>Min. number special characters</td>
<td>Specifies the minimum number of special characters the password must contain.</td>
</tr>
<tr>
<td>Permitted special characters</td>
<td>List of permitted characters.</td>
</tr>
<tr>
<td>Max. identical characters in total</td>
<td>Maximum number of identical characters that can be present in the password in total.</td>
</tr>
<tr>
<td>Max. identical characters in succession</td>
<td>Maximum number of identical character that can be repeated after each other.</td>
</tr>
<tr>
<td>Denied special characters</td>
<td>List of characters, which are not permitted.</td>
</tr>
<tr>
<td>Lowercase not allowed</td>
<td>Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Uppercase not allowed</td>
<td>Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Digits not allowed</td>
<td>Specifies whether the password can contain digits. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Special characters not allowed</td>
<td>Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.</td>
</tr>
</tbody>
</table>

**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 passwords](#) on page 84
- [Script for generating a password](#) on page 86

**Script for checking passwords**

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 start with ? or !. 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. In the Manager, select the G Suite | Basic configuration data | Password policies category.
   b. Select the password policy in the result list.
   c. Select Change master data.
   d. Enter the name of the script to be used to check a password in the Check script input field on the Scripts tab.
   e. Save the changes.
Related topics

- Script for generating a password on page 86

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

In random passwords, the script replaces the ? and ! characters, which are not permitted.

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. In the Manager, select the G Suite | Basic configuration data | Password policies category.
   b. Select the password policy in the result list.
   c. Select Change master data.
d. Enter the name of the script to be used to generate a password in the Generating script input field on the Scripts tab.
e. Save the changes.

Related topics
- Script for checking passwords on page 84

Editing the excluded list for passwords

You can add words to a list of restricted terms to prohibit them from being used in passwords.

NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

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

Checking passwords

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. In the Manager, select the G Suite | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
4. Select the Test tab.
5. Select the table and object to be tested in Base object for test.
6. Enter a password in Enter password to test.
   A display next to the password shows whether it is valid or not.
Testing the generation of passwords

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

To generate a password that conforms to the password policy

1. In the Manager, select the G Suite | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
4. Select the Test tab.
5. Click Generate.
   
   This generates and displays a password.

Initial password for new G Suite user accounts

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

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - Enable the TargetSystem | GoogleApps | Accounts | InitialRandomPassword configuration parameter in 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.
- User the employee's central password. The employee’s central password is mapped to the user account password. For detailed information about an employee’s central password, see One Identity Manager Identity Management Base Module Administration Guide.

Related topics

- Password policies for G Suite user accounts on page 77
- Email notifications about login data on page 89
Email notifications about login data

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.

The following prerequisites must be fulfilled in order to use notifications:

- Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Installation Guide.
- In Designer, enable the Common | MailNotification | DefaultSender configuration parameter and enter the sender address for sending the email notifications.
- 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.
- Ensure that a language 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. Enable the TargetSystem | GoogleApps | Accounts | InitialRandomPassword configuration parameter in Designer.
2. In Designer, set the configuration parameter TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo and enter the notification recipient as a value.
   
   If no recipient can be found, the email is sent to the address stored in the configuration parameter TargetSystem | GoogleApps | DefaultAddress.
3. In Designer, set the configuration parameter TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName.
   
   By default, the message sent uses the mail template Employee - new user account created. The message contains the name of the user account.
4. In Designer, set the configuration parameter TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword.
   
   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.
Managing G Suite entitlement assignments

In G Suite, the users can have different entitlements, which are mapped in One Identity Manager as follows:

- Entitlement for logging on to G Suite
  Table: **G Suite Products and SKUs** (GAPPaSku)
- Administrative entitlements
  Table: **G Suite Admin role designations** (GAPOrgAdminRole)
- Entitlement for the use of G Suite groups
  Table: **G Suite Groups** (GAPGroup)

Entitlement assignments refer to the assignment of the various entitlements to user accounts. These include:

- G Suite user accounts: assignments to products and SKUs (GAPUserInPaSku table)
- G Suite user accounts: assignments to groups (GAPUserInGroup table)
- G Suite groups: assignments to customers (GAPCustomerInGroup table)

Assigning G Suite entitlements to user accounts in One Identity Manager

In One Identity Manager, G Suite entitlements can be assigned directly or indirectly to employees.

In the case of indirect assignment, employees and entitlements are organized in hierarchical roles. The number of entitlements assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If the employee has a G Suite user account, the entitlements are assigned to this user account.

Entitlements can also be assigned to employees via IT Shop requests. To enable the assignment of entitlements via IT Shop requests, employees are added as customers in a
shop. All entitlements assigned to this shop as products can be requested by the customers. After approval is granted, requested entitlements are assigned to the employees.

You can use system roles to group entitlements together and assign them to employees as a package. You can create system roles that contain only G Suite entitlements. System entitlements from different target systems can also be grouped together in a system role.

To react quickly to special requests, you can also assign the entitlements directly to user accounts.

**Prerequisites**

- For departments, cost centers, locations, or business roles, the assignment of persons, G Suite products and SKUs and G Suite groups is permitted.
- The **Entitlements can be inherited** option is selected for the user accounts.
- The user accounts are linked with an employee via the `UID_Person` (`Person`) column.
- User accounts and entitlements belong to the same customer.

For detailed information see the following guides:

<table>
<thead>
<tr>
<th>Theme</th>
<th>Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inheritance of company resources</td>
<td><em>One Identity Manager Identity Management Base Module Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td><em>One Identity Manager Business Roles Administration Guide</em></td>
</tr>
<tr>
<td>Assigning company resources via</td>
<td><em>One Identity Manager IT Shop Administration Guide</em></td>
</tr>
<tr>
<td>IT Shop requests</td>
<td></td>
</tr>
<tr>
<td>System roles</td>
<td><em>One Identity Manager System Roles Administration Guide</em></td>
</tr>
</tbody>
</table>

**Detailed information about this topic**

- Assigning G Suite entitlements to departments, cost centers, and locations on page 92
- Assigning G Suite entitlements to business roles on page 93
- Assigning G Suite user accounts directly to an entitlement on page 96
- Adding G Suite entitlements to system roles on page 94
- Adding G Suite entitlements to the IT Shop on page 94
- Assigning G Suite entitlements directly to a user account on page 97
- Assigning G Suite groups directly to a customer on page 97
- Assigning G Suite customers directly to a group on page 98
Assigning G Suite entitlements to departments, cost centers, and locations

Assign groups and products and SKUs to departments, cost centers, or locations in order to assign them to user accounts through these organizations.

To assign a permission to a department, cost center or location (non role-based login):

1. Select one of the following categories.
   - G Suite | Groups
   - G Suite | Products and SKUs
2. Select the entitlements 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 centers tab.
   
   TIP: In the Remove assignments area, you can remove the assignment of organizations.

To remove an assignment
- Select the organization and double click.

5. Save the changes.

To assign permissions to a department, cost center or location (role-based login)

1. Select Organizations | Departments.
   - OR -
   Select the category Organizations | Cost centers.
   - OR -
   Select the category Organizations | Locations.
2. Select the department, cost center or location in the result list.
3. Select one of the following tasks.
   - G Suite Assign groups
   - G Suite Assign products and SKUs
4. Assign the entitlements in the Add assignments area.
   - OR -
Remove the entitlements in the Remove assignments area.

5. Save the changes.

Related topics

- One Identity Manager users for managing G Suite on page 10

Assigning G Suite entitlements to business roles

Installed modules: Business Roles Module

You assign entitlements to business roles so that these entitlements are assigned to user accounts via these business roles.

**To assign an entitlement to business roles (non-role-based login):**

1. Select one of the following categories.
   - G Suite | Groups
   - G Suite | Products and SKUs
2. Select the entitlements in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of business roles.

   **To remove an assignment**
   - Select the business role and double click.

5. Save the changes.

**To assign entitlements to a business role (role-based login):**

1. Select the category Business roles | <Role class>.
2. Select the business role in the result list.
3. Select one of the following tasks.
   - G Suite Assign groups
   - G Suite Assign products and SKUs
4. Assign the entitlements in the Add assignments area.

   - OR -
Remove the entitlements in the **Remove assignments** area.

5. Save the changes.

**Related topics**

- One Identity Manager users for managing G Suite on page 10

---

**Adding G Suite entitlements to system roles**

**Installed modules:** System Roles Module

Use this task to add an entitlement to system roles. When you assign a system role to an employee, the entitlement is inherited by all user accounts of this employee.

**NOTE:** Groups with the option **Only use in IT Shop** can only be assigned to system roles that also have this option set. For detailed information, see the *One Identity Manager System Roles Administration Guide*.

**To assign a group to system roles:**

1. Select one of the following categories.
   - G Suite | Groups
   - G Suite | Products and SKUs
2. Select the entitlements in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.
   
   **TIP:** In the **Remove assignments** area, you can remove the assignment of system roles.

   **To remove an assignment**
   
   - Select the system role and double click ✅.

5. Save the changes.

---

**Adding G Suite entitlements to the IT Shop**

When you assign a permission to a IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- the permission must be marked with the **IT Shop** option.
- the permission must be assigned a service item.
TIP: In Web Portal, all products that can be requested are grouped together by service category. To make the permission easier to find in Web Portal, assign a service category to the service item.

- If you only want it to be possible for the permission to be assigned to employees through IT Shop requests, the permission must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

NOTE: With role-based login, the IT Shop administrators can assign permissions to IT Shop shelves. Target system administrators are not authorized to add permissions to IT Shop.

**To add a permission to IT Shop.**

1. In Manager, select one of the following categories (non-role-based login).
   - **G Suite | Groups**
   - **G Suite | Products and SKUs**
   - OR -
   2. In Manager select one of the following categories (role-based login).
   - **Entitlements | G Suite Groups**
   - **Entitlements | G Suite Products and SKUs**

2. In the result list, select the permission.
3. Select **Add to IT Shop**.
4. In **Add assignments**, the entitlement to the IT Shop shelves.
5. Save the changes.

**To remove, an entitlement from individual shelves of the IT Shop**

1. In Manager, select one of the following categories (non-role-based login).
   - **G Suite | Groups**
   - **G Suite | Products and SKUs**
   - OR -
   2. In Manager select one of the following categories (role-based login).
   - **Entitlements | G Suite Groups**
   - **Entitlements | G Suite Products and SKUs**

2. In the result list, select the permission.
3. Select **Add to IT Shop**.
4. In **Remove assignments**, the entitlement from the IT Shop shelves.
5. Save the changes.
To remove, an entitlement from all shelves of the IT Shop

1. In Manager, select one of the following categories (non-role-based login).
   - G Suite | Groups
   - G Suite | Products and SKUs
   - OR -
   In Manager select one of the following categories (role-based login).
   - Entitlements | G Suite Groups
   - Entitlements | G Suite Products and SKUs
2. In the result list, select the permission.
3. Select Remove from all shelves (IT Shop).
4. Confirm the security prompt with Yes.
5. Click OK.
   The entitlement is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this entitlement are canceled.

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

Related topics

- General master data for G Suite groups on page 128
- General master data for G Suite products and SKUs on page 136
- One Identity Manager users for managing G Suite on page 10

Assigning G Suite user accounts directly to an entitlement

To react quickly to special requests, you can assign the entitlements directly to user accounts.

To assign an entitlement directly to user accounts

1. Select one of the following categories.
   - G Suite | Groups
   - G Suite | Products and SKUs
2. Select the entitlements in the result list.
3. Select Assign members.
4. Select the User tab.
5. Assign user accounts in Add assignments.
- OR -
Remove user accounts from Remove assignments.

6. Save the changes.

**Assigning G Suite entitlements directly to a user account**

To enable a quick response to special requests, you can assign entitlements directly to a user account.

*To assign entitlements directly to a user account*

1. Select the category **G Suite | User accounts**.
2. Select the user account in the result list.
3. Select one of the following tasks.
   - assign group
   - Assign products and SKUs
   - Admin role designations
4. Assign the entitlements in the **Add assignments** area.
   - OR -
   Remove the entitlements in the **Remove assignments** area.
5. Save the changes.

**Assigning G Suite groups directly to a customer**

To add all user accounts of a customer as members in a G Suite group, assign the groups directly to the G Suite customer. In the calculation of inheritance, for all user accounts of the customer, an entry is made in the GAPUserInGroup table. The origin of the assignment is indicated in the XOrigin column with the value 16.

*To assign groups directly to a customer*

1. Select **G Suite | G Suite customers**.
2. Select the customer in the result list.
3. Select **Assign groups**.
4. Assign groups in **Add assignments**.
   - OR -
Remove groups from **Remove assignments**.
5. Save the changes.

**Related topics**
- Appendix: Special features in the assignment of G Suite groups on page 170

**Assigning G Suite customers directly to a group**

To add all user accounts of a customer as members in a G Suite group, assign the G Suite customers directly to the group. In the calculation of inheritance, for all user accounts of the customer, an entry is made in the GAPUserInGroup table. The origin of the assignment is indicated in the XOrigin column with the value **16**.

**To assign customers directly to a group**
1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **Assign G Suite customer as member**.
4. Assign the customers in the **Add assignments** view.
   - OR -
     - Remove the customers in **Remove assignments**.
5. Save the changes.

**Related topics**
- Appendix: Special features in the assignment of G Suite groups on page 170

**Effectiveness of G Suite entitlement assignments**

When groups are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually exclusive groups. To do this, you specify which of the two groups should apply to the user accounts if both are assigned.

It is possible to assign an excluded group directly, indirectly or by IT Shop request at any time. One Identity Manager determines whether the assignment is effective.
NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.
- One Identity Manager does not check whether membership of an excluded group is permitted in another group (table GAPGroupInGroup).

The effectiveness of the assignments is mapped in the GAPUserInGroup and GAPBaseTreeHasGroup via the column XIsInEffect.

Example of the effect of group memberships

- The groups A, B and C are defined in a customer.
- Group A is assigned through the department "Marketing", group B through "Finance" and group C through the business role "Control group".

Clara Harris has a user account in this customer. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B and C.

By using suitable controls, you want to prevent an employee from obtaining authorizations of groups A and group B at the same time. That means, groups A, B and C are mutually exclusive. A user, who is a member of group C cannot be a member of group B at the same time. That means, groups B and C are mutually exclusive.

Table 24: Specifying excluded groups (table AADGroupExclusionGAPGroupExclusion)

<table>
<thead>
<tr>
<th>Effective Group</th>
<th>Excluded Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td></td>
</tr>
<tr>
<td>Group B</td>
<td>Group A</td>
</tr>
<tr>
<td>Group C</td>
<td>Group B</td>
</tr>
</tbody>
</table>

Table 25: Effective Assignments

<table>
<thead>
<tr>
<th>Employee</th>
<th>Member in Role</th>
<th>Effective Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ben King</td>
<td>Marketing</td>
<td>Group A</td>
</tr>
<tr>
<td>Employee</td>
<td>Member in Role</td>
<td>Effective Group</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Jan Bloggs</td>
<td>Marketing, finance</td>
<td>Group B</td>
</tr>
<tr>
<td>Clara Harris</td>
<td>Marketing, finance, control group</td>
<td>Group C</td>
</tr>
<tr>
<td>Jenny Basset</td>
<td>Marketing, control group</td>
<td>Group A, Group C</td>
</tr>
</tbody>
</table>

Only the group C assignment is in effect for Clara Harris. It is published in the target system. If Clara Harris leaves the business role "control group" at a later date, group B also takes effect.

The groups A and C are in effect for Jenny Basset because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

**Table 26: Excluded groups and effective assignments**

<table>
<thead>
<tr>
<th>Employee</th>
<th>Member in Role</th>
<th>Assigned Group</th>
<th>Excluded Group</th>
<th>Effective Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jenny Basset</td>
<td>Marketing</td>
<td>Group A</td>
<td>Group B</td>
<td>Group C</td>
</tr>
<tr>
<td></td>
<td>Control group</td>
<td>Group C</td>
<td>Group A</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisites**

- The configuration parameter `QER | Structures | Inherit | GroupExclusion` is enabled.
- Mutually exclusive groups belong to the same customer.

**To exclude a group**

1. In the Manager, select the **G Suite | Groups** category.
2. Select a group in the result list.
3. Select **Exclude groups**.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.
   - OR -
   In **Remove assignments**, remove the groups that are not longer mutually exclusive.
5. Save the changes.
Inheritance of G Suite entitlements based on categories

In One Identity Manager, entitlements can be selectively inherited by user accounts. For this purpose, the entitlements and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables enter your categories for the permissions. Each table contains the category positions **Position 1 to Position 31**.

Every user account can be assigned to one or more categories. Each entitlement can also be assigned to one or more categories. If at least one of the category items between the user account and the assigned entitlement is the same, the entitlement is inherited by the user account. If the entitlement or the user account is not classified in a category, the entitlement is also inherited by the user account.

**NOTE:** Inheritance through categories is only taken into account when entitlements are assigned indirectly via hierarchical roles. Categories are not taken into account when entitlements are directly assigned to user accounts.

**Table 27: Category examples**

<table>
<thead>
<tr>
<th>Category Position</th>
<th>Categories for User Accounts</th>
<th>Categories for entitlements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default user</td>
<td>Default group</td>
</tr>
<tr>
<td>2</td>
<td>Administrator</td>
<td>Administrator group</td>
</tr>
</tbody>
</table>
**Figure 2: Example of inheriting through categories.**

<table>
<thead>
<tr>
<th>User Categories</th>
<th>Permissions Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>System administrator</td>
<td>Default permissions</td>
</tr>
<tr>
<td>System user</td>
<td>System user permissions</td>
</tr>
<tr>
<td>Default user</td>
<td>System administrator permissions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

**Resulting Group Memberships**

<table>
<thead>
<tr>
<th>Group A</th>
<th>Group B</th>
<th>Group C</th>
<th>Group D</th>
<th>Group E</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

**Key:**
- ![Icon] Inherits due to matching categories
- ![Icon] Inherits because user account is not categorized
- ![Icon] Inherits because group is not categorized
- ![Icon] Inherits because user account and group are not categorized

**To use inheritance through categories**

- Define the categories for the G Suite customer.
- Assign categories to user accounts through their master data.
- Assign categories to groups, products, and SKUs through their master data.
Related topics

- Defining categories for the inheritance of G Suite entitlements on page 108
- General master data for G Suite user accounts on page 113
- General master data for G Suite groups on page 128
- General master data for G Suite products and SKUs on page 136

Overview of all assignments

The **Overview of all assignments** report is displayed for some objects, such as authorizations, compliance rules, or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Examples

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees who violate this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.
  
  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the **i** icon in the report’s toolbar.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the **V** button in a role's control, you display all employees in the role with the base object.
• Use the small arrow next to to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 3: Toolbar of the Overview of all assignments report.

Table 28: Meaning of Icons in the Report Toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Show the legend with the meaning of the report control elements</td>
</tr>
<tr>
<td>📋</td>
<td>Saves the current report view as a graphic.</td>
</tr>
<tr>
<td>⚡</td>
<td>Selects the role class used to generate the report.</td>
</tr>
<tr>
<td>🔄</td>
<td>Displays all roles or only the affected roles.</td>
</tr>
</tbody>
</table>
Mapping of G Suite objects in One Identity Manager

You use One Identity Manager to manage all objects of the G Suite, that are required for the optimization of access control in the target system. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in Manager.

G Suite customers

The target system for the synchronization of G Suite is the primary domain of a G Suite customer. G Suite customers are created as base objects for the synchronization in One Identity Manager. They are used for the configuration of provisioning processes, the automatic assignment of employees to user accounts, and the passing on of G Suite entitlements to user accounts.

Creating G Suite customers

NOTE: G Suite sets up the One Identity Manager customer in the Synchronization Editor database. If necessary, customers can also be created in Manager.

To set up a customer

1. In Manager, select G Suite | G Suite customers.
2. Click in the result list.
3. On the master data form, edit the master data for the customer.
4. Save the changes.
Related topics

- General master data for G Suite customers on page 106
- G Suite customer address data on page 108
- Defining categories for the inheritance of G Suite entitlements on page 108
- Editing master data for G Suite customers on page 106

Editing master data for G Suite customers

To edit the master data for a customer

1. In Manager, select G Suite | G Suite customers.
2. Select the customer in the result list.
3. Select Change master data.
4. Edit the master data for the customer.
5. Save the changes.

Related topics

- General master data for G Suite customers on page 106
- G Suite customer address data on page 108
- Defining categories for the inheritance of G Suite entitlements on page 108
- Creating G Suite customers on page 105

General master data for G Suite customers

On the General tab, you enter the following master data:

Table 29: General master data for G Suite customers

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite customer</td>
<td>Unique ID of the G Suite customer.</td>
</tr>
<tr>
<td>Customer primary domain</td>
<td>Name of this customer’s primary domain.</td>
</tr>
<tr>
<td>Customer creation time</td>
<td>Time at which the customer was created.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alternative e-mail address</td>
<td>Second e-mail address for the customer. This e-mail address must not be in the customer's domain.</td>
</tr>
<tr>
<td>Phone</td>
<td>Customer's telephone number in E.164 format.</td>
</tr>
<tr>
<td>Country</td>
<td>Unique country ID.</td>
</tr>
<tr>
<td>Language</td>
<td>Name of the language.</td>
</tr>
<tr>
<td>Account definition (initial)</td>
<td>Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this customer and if user accounts are to be created that are already managed (Linked configured). The account definition's default manage level is applied. User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.</td>
</tr>
<tr>
<td>Target system managers</td>
<td>Application role in which the customer's target system managers are defined. Target system managers only edit objects from customers to whom they are assigned. A different target system manager can be assigned to each customer. Select the One Identity Manager application role whose members are responsible for the administration of this customer. Use the button to add a new application role.</td>
</tr>
<tr>
<td>Synchronized by</td>
<td>Type of synchronization through which data is exchanged between the customer and One Identity Manager. You can no longer change the synchronization type once objects for this customer are present in One Identity Manager. When you create a customer with the Synchronization Editor, One Identity Manager is used.</td>
</tr>
</tbody>
</table>

**Table 30: Permitted values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Synchronization by</th>
<th>Provisioned by</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Identity Manager</td>
<td>G Suite connector</td>
<td>G Suite connector</td>
</tr>
<tr>
<td>No synchronization</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**NOTE:** If you select No synchronization, you can define custom processes to exchange data between One Identity Manager and the target system.
Related topics

- Assigning account definitions to target systems on page 61
- Account definitions for G Suite user accounts on page 46
- Automatic assignment of employees to G Suite user accounts on page 64
- Target system managers for customers on page 158

G Suite customer address data

On the Postal address tab, enter the following master data:

Table 31: G Suite customer address data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization name</td>
<td>Name of the organization for the customer's postal address.</td>
</tr>
<tr>
<td>Name of contact person</td>
<td>Customer's contact person.</td>
</tr>
<tr>
<td>Address line 1-3</td>
<td>Customer's postal address.</td>
</tr>
<tr>
<td>Region</td>
<td>Region of the postal address</td>
</tr>
<tr>
<td>City</td>
<td>City of the postal address</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code of the postal address</td>
</tr>
</tbody>
</table>

Defining categories for the inheritance of G Suite entitlements

In One Identity Manager, entitlements can be selectively inherited by user accounts. For this purpose, the entitlements and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables enter your categories for the permissions. Each table contains the category positions **Position 1** to **Position 31**.

**To define a category**

1. In Manager, select the customer in G Suite | Customers.
2. Select Change master data.
3. Switch to the Mapping rule category tab.
4. Extend the relevant roots of a table.
5. Click 🗼 to enable category.

6. Enter a category name of your choice for user accounts and groups and products and SKUs in the login language used.

7. Save the changes.

Detailed information about this topic

- Inheritance of G Suite entitlements based on categories on page 101

Additional tasks for managing G Suite customers

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of G Suite customers assign group</td>
<td>Overview of a G Suite customer on page 109</td>
</tr>
<tr>
<td>Define Search Criteria for Employee Assignment</td>
<td>Assigning G Suite groups directly to a customer on page 97</td>
</tr>
<tr>
<td>How to Edit a Synchronization Project</td>
<td>Editing search criteria for automatic employee assignment on page 65</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Editing the synchronization project for a G Suite customer on page 109</td>
</tr>
<tr>
<td></td>
<td>Synchronizing single objects on page 39</td>
</tr>
</tbody>
</table>

Overview of a G Suite customer

To obtain an overview of a G Suite customer

1. In Manager, select G Suite | G Suite customers.
2. Select the customer in the result list.
3. Select customer overview G Suite

Editing the synchronization project for a G Suite customer

Synchronization projects in which a G Suite customer is already used as a base object can also be opened in Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full
functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

![NOTE: Manager is locked for editing throughout. To edit objects in Manager, close the Synchronization Editor.]

**To open an existing synchronization project in the Synchronization Editor:**

1. In Manager, select **G Suite | G Suite customers**.
2. Select the customer in the result list.
3. Select **Change master data**.
4. Select **Edit synchronization project**.

**Related topics**

- [Adjusting the synchronization configuration for G Suite environments](#) on page 26

**G Suite user accounts**

Use One Identity Manager to manage the users of G Suite. The user data for the registered users is represented in One Identity Manager as user accounts. You can use the user accounts to manage the user's permissions, for example, membership of G Suite groups or administrative permissions.

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

![NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.]

![NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location or a primary cost center.]

**Related topics**

- [Managing G Suite user accounts and employees](#) on page 45
- [Account definitions for G Suite user accounts](#) on page 46
- [Appendix: Default project templates for G Suite](#) on page 165
- [Editing master data for G Suite user accounts](#) on page 112
- [Managing G Suite entitlement assignments](#) on page 90
Creating G Suite user accounts

To create a user account

1. In Manager, select **G Suite | User accounts**.
2. Click in the result list.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

Various communication data and organizational data can be assigned to user accounts, such as e-mail addresses, website, information about the user’s organization or relationships to other users.

To assign communication data to a user account

1. Select the required tabs on the master data form.
2. Click **Add**.
   - This inserts a new row in the table.
3. Select this row and edit the master data.
4. Save the changes.

To edit communication data

1. Select the required tabs on the master data form.
2. In the table, select the row that you want to edit.
3. Edit the master data.
4. Save the changes.

To remove the assignment of communication data

1. Select the required tabs on the master data form.
2. In the table, select the row that you want to remove.
3. Click **Delete**.
4. Save the changes.

Detailed information about this topic

- General master data for G Suite user accounts on page 113
- Password data for G Suite user accounts on page 117
- Phone numbers for G Suite user accounts on page 117
- Addresses for G Suite user accounts on page 118
- E-mail addresses for G Suite user accounts on page 118
- External IDs for G Suite user accounts on page 119
Related topics

- Editing master data for G Suite user accounts
- Deleting and restoring G Suite user accounts

Editing master data for G Suite user accounts

To edit master data for a user account

1. In Manager, select G Suite | User accounts.
2. Select the user account in the result list and run Change master data.
3. Edit the user account's resource data.
4. Save the changes.

Various communication data and organizational data can be assigned to user accounts, such as e-mail addresses, website, information about the user's organization or relationships to other users.

To assign communication data to a user account

1. Select the required tabs on the master data form.
2. Click Add.
   This inserts a new row in the table.
3. Select this row and edit the master data.
4. Save the changes.

To edit communication data

1. Select the required tabs on the master data form.
2. In the table, select the row that you want to edit.
3. Edit the master data.
4. Save the changes.
To remove the assignment of communication data

1. Select the required tabs on the master data form.
2. In the table, select the row that you want to remove.
3. Click Delete.
4. Save the changes.

Detailed information about this topic

- General master data for G Suite user accounts on page 113
- Password data for G Suite user accounts on page 117
- Phone numbers for G Suite user accounts on page 117
- Addresses for G Suite user accounts on page 118
- E-mail addresses for G Suite user accounts on page 118
- External IDs for G Suite user accounts on page 119
- Instant messenger data for G Suite user accounts on page 119
- User details for G Suite user accounts on page 120
- Relationships of G Suite user accounts on page 121
- Websites of G Suite user accounts on page 121

Related topics

- Creating G Suite user accounts
- Deleting and restoring G Suite user accounts
- Locking G Suite user accounts

General master data for G Suite user accounts

On the General tab, you enter the following master data:

Table 32: Additional master data for a user account

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account.</td>
</tr>
</tbody>
</table>
For a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity** or **Service identity**, you can create a new employee. To do this, click next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.

**NOTE:** To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account definition</td>
<td>Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. <strong>NOTE:</strong> The account definition cannot be changed once the user account has been saved.</td>
</tr>
<tr>
<td>Manage level</td>
<td>Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.</td>
</tr>
<tr>
<td>G Suite customer</td>
<td>Customer to which the user account belongs.</td>
</tr>
<tr>
<td>Unique ID</td>
<td>G Suite internal ID of the user account.</td>
</tr>
<tr>
<td>First name</td>
<td>User's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>User's last name.</td>
</tr>
<tr>
<td>Primary email address</td>
<td>Primary email address for the user account.</td>
</tr>
<tr>
<td>G Suite Organization</td>
<td>G Suite organization to which the user account belongs.</td>
</tr>
<tr>
<td>Creation time</td>
<td>Time at which the user account was created.</td>
</tr>
<tr>
<td>Deletion time</td>
<td>Time at which the user account was deleted. The user account can be restored within five days.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Maximum risk index value of all assigned entitlements. The property is only visible if the QER</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk Assessment Administration Guide</td>
<td>Categories for the inheritance of G Suite permissions to the user account. User accounts can selectively inherit permissions. To do this, entitlements and user accounts are divided into categories. Select one or more categories from the menu.</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Notes content type</td>
<td>Format of notes.</td>
</tr>
<tr>
<td>Notes</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Specifies whether the user account is locked.</td>
</tr>
<tr>
<td>Suspension reason</td>
<td>Reason for the suspension of the user account.</td>
</tr>
<tr>
<td>Aliases</td>
<td>List of all alias e-mail addresses that are set up for this user account.</td>
</tr>
<tr>
<td>Non editable aliases</td>
<td>List of all e-mail addresses that cannot be changed. These e-mail addresses do not belong to the primary domain or its subdomains.</td>
</tr>
<tr>
<td>Identity</td>
<td>User account’s identity type Permitted values are:</td>
</tr>
<tr>
<td></td>
<td><strong>Primary identity</strong>: Employee’s default user account.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational identity</strong>: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</td>
</tr>
<tr>
<td></td>
<td><strong>Personalized administrator identity</strong>: User account with administrative entitlements, used by one employee.</td>
</tr>
<tr>
<td></td>
<td><strong>Sponsored identity</strong>: User account that is used for training purposes, for example.</td>
</tr>
<tr>
<td></td>
<td><strong>Shared identity</strong>: User account with administrative entitlements, used by several employees. Assign all employees show use the user account.</td>
</tr>
<tr>
<td></td>
<td><strong>Service identity</strong>: Service account.</td>
</tr>
<tr>
<td>Entitlements can be inherited</td>
<td>Specifies whether the user account may inherit G Suite permissions via the employee. If this option is set, the user account inherits permissions through hierarchical roles or IT Shop requests.</td>
</tr>
<tr>
<td></td>
<td>1. Example: An employee with a G Suite user account is a member of a department. A G Suite product and SKU are assigned to this department. If this option is set, the user account inherits this product and SKU.</td>
</tr>
<tr>
<td></td>
<td>2. Example: An employee with a G Suite user account requests a G Suite group in the IT Shop. The request is approved and assigned.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privileged user account</td>
<td>Specifies whether this is a privileged user account.</td>
</tr>
<tr>
<td>Include in global address list</td>
<td>Specifies whether the user account is displayed in the global address list.</td>
</tr>
<tr>
<td>Included in white list</td>
<td>Specifies whether the IP address for the user account is included in the white list for e-mails.</td>
</tr>
<tr>
<td>Is super admin</td>
<td>Specifies whether the user account has super admin permissions.</td>
</tr>
<tr>
<td>Delegated administrator</td>
<td>Specifies whether the user account has delegated admin permissions.</td>
</tr>
<tr>
<td>G Suite agreement accepted</td>
<td>Specifies whether the user has performed an initial logon to GSuite and has accepted the G Suite (online) agreement.</td>
</tr>
<tr>
<td>Google mailbox is created</td>
<td>Specifies whether a Google mailbox has been created for the user account.</td>
</tr>
<tr>
<td>2-step verification is enrolled</td>
<td>Specifies whether <strong>2-step verification</strong> for the user account is enrolled.</td>
</tr>
<tr>
<td>2-step verification enforced</td>
<td>Specifies whether <strong>2-step verification</strong> for the user account is enforced.</td>
</tr>
</tbody>
</table>

**Related topics**

- Managing G Suite user accounts and employees on page 45
- Account definitions for G Suite user accounts on page 46
- Automatic assignment of employees to G Suite user accounts on page 64
- Inheritance of G Suite entitlements based on categories on page 101
- Locking G Suite user accounts on page 123
- Supported user account types on page 70
- Providing administrative user accounts for one employee on page 73
- Providing administrative user accounts for several employees on page 74
- Moving G Suite user accounts to a different organization on page 123
Password data for G Suite user accounts

On the Password tab, enter the password for logging in to G Suite.

Table 33: User account password data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Password for the user account. The employee’s central password can be mapped to the user account password. For detailed information about an employee’s central password, see One Identity Manager Identity Management Base Module Administration Guide. If you use an initial password for the user accounts, it is automatically entered when a user account is created.</td>
</tr>
<tr>
<td>Confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Last login</td>
<td>Time of the last login to G Suite.</td>
</tr>
<tr>
<td>Change password at next login</td>
<td>Specifies whether the user has to change their password the next time they log in.</td>
</tr>
</tbody>
</table>

Related topics

- [Initial password for new G Suite user accounts](#) on page 88

Phone numbers for G Suite user accounts

You can edit user account email addresses in Phone numbers.

Table 34: Phone number properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the telephone number.</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the telephone number. If the Custom value is selected in the Type input field, you can enter your own phone number type here.</td>
</tr>
<tr>
<td>Phone</td>
<td>Telephone number in any format.</td>
</tr>
<tr>
<td>Primary phone number</td>
<td>Specifies whether this is the primary telephone number.</td>
</tr>
</tbody>
</table>
Related topics

- Editing master data for G Suite user accounts on page 112

Addresses for G Suite user accounts

On the Addresses tab, you can edit the addresses of the user account.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the address</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the address. If the Custom value is selected in the Type input field, you can enter your own address type here.</td>
</tr>
<tr>
<td>Extended address</td>
<td>Extended address, for example, for entering a specific region</td>
</tr>
<tr>
<td>Address</td>
<td>Full address.</td>
</tr>
<tr>
<td>Street</td>
<td>The street name of the address.</td>
</tr>
<tr>
<td>Zip code</td>
<td>The zip code of the address.</td>
</tr>
<tr>
<td>City</td>
<td>The city of the address.</td>
</tr>
<tr>
<td>Region</td>
<td>Region, if required</td>
</tr>
<tr>
<td>Mailbox</td>
<td>Mailbox, if applicable</td>
</tr>
<tr>
<td>Country ID</td>
<td>Unique country ID.</td>
</tr>
<tr>
<td>Primary address</td>
<td>Specifies whether this address is the user’s primary address.</td>
</tr>
<tr>
<td>Source is structured</td>
<td>Specifies whether the address is provided in a structured format.</td>
</tr>
</tbody>
</table>

E-mail addresses for G Suite user accounts

You can edit user account email addresses in Email addresses.
### Table 36: Properties of an e-mail address

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the e-mail address.</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the e-mail address. If the Custom value is selected in the Type input field, you can enter your own e-mail address type here.</td>
</tr>
<tr>
<td>Email address</td>
<td>Additional email addresses. This value can also be the user account's primary e-mail address or an alias.</td>
</tr>
</tbody>
</table>

**Related topics**
- [Editing master data for G Suite user accounts](#) on page 112

### External IDs for G Suite user accounts

On the External IDs tab, you can edit the external IDs of the user account.

### Table 37: Properties of an external ID

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the external ID.</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the external ID. If the Custom value is selected in the Type input field, you can enter your own ID type type here.</td>
</tr>
<tr>
<td>External ID</td>
<td>Value of the external ID.</td>
</tr>
</tbody>
</table>

**Related topics**
- [Editing master data for G Suite user accounts](#) on page 112

### Instant messenger data for G Suite user accounts

On the Instant Messenger tab, you can edit the Instant Messenger data for the user account.
Table 38: Instant messenger properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of Instant Messenger</td>
</tr>
<tr>
<td>Custom type</td>
<td>Type of Instant Messenger defined by the user If the Custom value is selected in the Type input field, you can enter your own Instant Messenger type here.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Network protocol of the Instant Messenger You can set a custom protocol or a standard protocol.</td>
</tr>
<tr>
<td>Custom protocol</td>
<td>If the Custom value is selected in the Protocol input field, you can enter your own protocol type here.</td>
</tr>
<tr>
<td>Primary Instant Messenger</td>
<td>Specifies whether this is the primary Instant Messenger.</td>
</tr>
</tbody>
</table>

Related topics

Editing master data for G Suite user accounts on page 112

User details for G Suite user accounts

On the Organizations tab, you can edit various organization data for the user account.

Table 39: Properties of user details

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the organization.</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the organization. If the Unknown value is selected in the Type input field, you can enter your own organization type here.</td>
</tr>
<tr>
<td>Organization name</td>
<td>Name of the organization for which the user details are being maintained.</td>
</tr>
<tr>
<td>Cost center</td>
<td>A cost center within the organization.</td>
</tr>
<tr>
<td>Department</td>
<td>A department within the organization.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the organization belongs.</td>
</tr>
<tr>
<td>location</td>
<td>Location of the organization.</td>
</tr>
<tr>
<td>Icon</td>
<td>Text symbol for the organization, for example GOOG for Google.</td>
</tr>
</tbody>
</table>
### Relationships of G Suite user accounts

On the **Relations** tab, you can edit the relationships of the user account.

**Table 40: Properties of a relationship**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the relationship.</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the relationship. If the <strong>Custom</strong> value is selected in the <strong>Type</strong> input field, you can enter your own relation type here.</td>
</tr>
<tr>
<td>Relation</td>
<td>Primary e-mail address of the user to whom the relationship exists.</td>
</tr>
</tbody>
</table>

**Related topics**

- [Editing master data for G Suite user accounts](#) on page 112

### Websites of G Suite user accounts

On the **Websites** tab, you can edit the websites of the user account.

**Table 41: Properties of a website**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type or purpose of the website.</td>
</tr>
<tr>
<td>Custom type</td>
<td>User-defined type of the website. If the <strong>Custom</strong> value is selected in the <strong>Type</strong> input field, you can enter your own website type here.</td>
</tr>
<tr>
<td>Website</td>
<td>URL of the website.</td>
</tr>
</tbody>
</table>
## Related topics

- [Editing master data for G Suite user accounts](#) on page 112

## Additional tasks for managing G Suite user accounts

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of G Suite user accounts</td>
<td><a href="#">Overview of G Suite user accounts</a> on page 122</td>
</tr>
<tr>
<td>assign group</td>
<td>Assigning G Suite entitlements directly to a user account on page 97</td>
</tr>
<tr>
<td>Assign products and SKUs</td>
<td>Assigning G Suite entitlements directly to a user account on page 97</td>
</tr>
<tr>
<td>Admin role designations</td>
<td>Assigning G Suite entitlements directly to a user account on page 97</td>
</tr>
<tr>
<td>Assigning extended properties</td>
<td>Assigning extended properties to a G Suite user account on page 123</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Synchronizing single objects on page 39</td>
</tr>
<tr>
<td>Change G Suite organization</td>
<td>Moving G Suite user accounts to a different organization on page 123</td>
</tr>
</tbody>
</table>

### Overview of G Suite user accounts

**To obtain an overview of a user account**

1. In Manager, select **G Suite | User accounts**.
2. Select the user account in the result list.
3. Select **G Suite user account overview**.
Assigning extended properties to a G Suite user account

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a user account

1. In Manager, select G Suite | User accounts.
2. Select the user account in the result list.
3. Select Assign extended properties.
4. Assign extended properties in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of extended properties.

   To remove an assignment
   - Select the extended property and double click 🌐.

5. Save the changes.

For detailed information about extended properties, see the One Identity Manager Identity Management Base Module Administration Guide.

Moving G Suite user accounts to a different organization

Within the organizational hierarchy of a G Suite customer, user accounts can be moved to a different organization.

To move a user account to another organization

1. In Manager, select G Suite | User accounts.
2. Select the user account in the result list and run Change master data.
3. Select Change G Suite organizational unit in the task view.
4. Confirm the security prompt with Yes.
5. Select the new organization from the G Suite organization unit menu on the General tab.
6. Save the changes.

Locking G Suite user accounts

The way you lock user accounts depends on how they are managed.
Scenario:
- The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the manage level Full managed manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the GAPUser.IsSuspended

Scenario:
- The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the QER | Person | TemporaryDeactivation configuration parameter
  - If the configuration parameter is set, the employee’s user accounts are locked if the employee is permanently or temporarily disabled.
  - If the configuration parameter is not set, the employee’s properties do not have any effect on the associated user accounts.

**To lock the user account when the configuration parameter is disabled.**
1. In Manager, select G Suite | User accounts.
2. Select the user account in the result list.
3. Select Change master data.
4. Set the option Locked on the General tab.
5. Save the changes.

Scenario:
- User accounts not linked to employees.

**To lock a user account that is no longer linked to an employee.**
1. In Manager, select G Suite | User accounts.
2. Select the user account in the result list.
3. Select Change master data.
4. Set the option Locked on the General tab.
5. Save the changes.

**To unlock a user account**
1. In Manager, select G Suite | User accounts.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Deactivate the **Locked** option on the **General** tab.
5. Save the changes.

For more detailed information about deactivating and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

**Related topics**

- Account definitions for G Suite user accounts on page 46
- Creating manage levels on page 50
- Deleting and restoring G Suite user accounts on page 125

**Deleting and restoring G Suite user accounts**

If a user account is deleted in One Identity Manager, it is initially marked for deletion. The user account is therefore locked. Depending on the deferred deletion setting, the user account is either deleted from the One Identity Manager database immediately, or at a later date.

**NOTE:** As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is deleted.

**To delete a user account that is not managed using an account definition**

1. In Manager, select **G Suite | User accounts**.
2. Select the user account in the result list.
3. Click 🗑 to delete the user account.
4. Confirm the security prompt with **Yes**.

**To restore a user account**

1. In Manager, select **G Suite | User accounts**.
2. Select the user account in the result list.
3. Click 💢 in the result list.

**Configuring deferred deletion**

By default, user accounts are finally deleted from the database after 30 days. The user accounts are initially locked. You can reenable the user accounts until deferred deletion is run. After deferred deletion is run, the user account are deleted from the database and cannot be restored anymore. You can configure an alternative deletion delay in Designer using the GAPUser table.
Transferring user data to a different G Suite user account

When a user account is deleted, various user data can be transferred to a different user account. After the deletion delay has expired, the data transfer is first initiated in the G Suite environment. As soon as the data transfer has been successfully completed in the target system, the user account is permanently deleted.

Prerequisites

- Data transfer is approved for the customer. To enable this, the Transfer user data before delete setting must be enabled, or the CP_TransferUserDataBeforeDelete variable is set to True.
- A manager has been assigned to the employee to whom the deleted user account is linked.
  - OR -
    The deleted user account has a relationship of the type Manager.
- The manager's email address belongs to the primary domain of the customer to which the deleted user account belongs.
- In the event that no valid email address can be determined in this way, a valid default email address is defined. This is specified in the target system connection using the Default email address for data transfer setting or in the CP_DefaultDataTransferTargetEmail variable.

Detailed information about this topic

- Advanced settings for system connection to G Suite on page 30
- General master data for G Suite user accounts on page 113
- Relationships of G Suite user accounts on page 121

Related topics

- Deleting and restoring G Suite user accounts on page 125
G Suite groups

Users of G Suite can use groups to exchange information or organize meetings. This information is only made available to the members of a group. In One Identity Manager, you can create and edit groups and manage group members.

Creating G Suite groups

To create a group

1. In the Manager, select the G Suite | Groups category.
2. Click in the result list.
3. On the master data form, edit the master data for the group.
4. Save the changes.

Detailed information about this topic

- General master data for G Suite groups on page 128
- Additional settings for G Suite groups on page 129

Related topics

- Entering master data for G Suite groups on page 127
- Deleting G Suite groups on page 135

Entering master data for G Suite groups

To edit group master data

1. In the Manager, select the G Suite | Groups category.
2. Select the group in the result list and run Change master data.
3. On the master data form, edit the master data for the group.
4. Save the changes.

Detailed information about this topic

- General master data for G Suite groups on page 128
- Additional settings for G Suite groups on page 129
General master data for G Suite groups

On the **General** tab, edit the following master data.

**Table 42: Entering master data for a group**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite customer</td>
<td>Customer to which the group belongs.</td>
</tr>
<tr>
<td>Group ID</td>
<td>Unique ID of the group.</td>
</tr>
<tr>
<td>Group name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Email address</td>
<td>Group’s email address</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item data for requesting the group through the IT Shop.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the configuration parameter QER</td>
</tr>
<tr>
<td>Category</td>
<td>Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is admin created</td>
<td>Specifies whether the group was created by an administrator. If this option is disable, the group was created by a user.</td>
</tr>
<tr>
<td>Aliases</td>
<td>List of additional e-mail addresses under which e-mails can be sent to the group.</td>
</tr>
<tr>
<td>Non editable aliases</td>
<td>List of all e-mail addresses that cannot be changed. These e-mail addresses do not belong to the primary domain or its subdomains.</td>
</tr>
</tbody>
</table>

### Related topics
- [Inheritance of G Suite entitlements based on categories](#) on page 101
- [Adding G Suite entitlements to the IT Shop](#) on page 94

### Additional settings for G Suite groups

On the **Settings** tab, edit the following master data.

#### Table 43: Additional settings for groups

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Name of the language, e.g. es-ES.</td>
</tr>
<tr>
<td>Allow external members</td>
<td>Specifies whether users from other domains are permitted as members. If this option is activated, in the <strong>Join the group</strong> input field, define which users are permitted to become members.</td>
</tr>
<tr>
<td>Join the group</td>
<td>Select which users are permitted to become members of the group. You can only select the <strong>Public</strong> value if the <strong>Allow external members</strong> option is set.</td>
</tr>
<tr>
<td>Spam messages</td>
<td>Select how suspected spam messages are handled. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Allow</strong>: Post in the group without moderation.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Moderate</strong>: Send to the moderation queue and send a message to the moderators.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Silently moderate</strong>: Send to the moderation queue, but do not send a message to the moderators.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reject</strong>: Reject immediately.</td>
</tr>
<tr>
<td>Post replies</td>
<td>Select who receives the replies to posts. If <strong>Use a custom address to send replies to</strong> is selected, a valid email address must be entered in the <strong>Post replies to</strong> input field.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Send replies to</td>
<td>E-mail address to which the replies to posts are sent. If <strong>Use a custom address to send replies to</strong> is selected in the <strong>Post replies</strong> input field, you must enter a valid e-mail address.</td>
</tr>
<tr>
<td>Notify authors when their messages are rejected</td>
<td>Specifies whether the author of a post is informed if their post is rejected by the moderators. If this option is activated, enter a notification text in the <strong>Rejected author notification</strong> input field.</td>
</tr>
<tr>
<td>Rejected author notification</td>
<td>Notification that is sent to authors if their post is rejected. The maximum text length is 10,000 characters. Notifications are only sent if the <strong>Notify authors when moderators reject their messages</strong> option is enabled.</td>
</tr>
<tr>
<td>Max message size</td>
<td>Maximum size of the messages that can be sent to this group in bytes.</td>
</tr>
<tr>
<td>Allow Google communication</td>
<td>Specifies whether Google is permitted to contact the group managers.</td>
</tr>
<tr>
<td>Allow web posting</td>
<td>Specifies whether users are permitted to post in the group via the web interface. If this option is disabled, the users can only use GMail for communication with the group.</td>
</tr>
<tr>
<td>Post as the group</td>
<td>Specifies whether group members are permitted to use the e-mail address of the group to post posts.</td>
</tr>
<tr>
<td>Archive messages to the group</td>
<td>Specifies whether messages sent to the group are archived.</td>
</tr>
<tr>
<td>Include in global address list</td>
<td>Specifies whether the group is displayed in the global address list.</td>
</tr>
<tr>
<td>List this group in the directory</td>
<td>Specifies whether the group is entered in the group directory.</td>
</tr>
</tbody>
</table>

### Additional tasks for managing G Suite groups

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of G Suite Groups</td>
<td><strong>Overview of G Suite groups</strong> on page 131</td>
</tr>
<tr>
<td>Task</td>
<td>Theme</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assigning extended properties</td>
<td>Assigning extended properties to a G Suite group on page 131</td>
</tr>
<tr>
<td>Assigning group managers</td>
<td>Assigning group managers on page 132</td>
</tr>
<tr>
<td>Assigning group owners</td>
<td>Assigning group owners</td>
</tr>
<tr>
<td>assign user accounts</td>
<td>Assigning G Suite user accounts directly to an entitlement on page 96</td>
</tr>
<tr>
<td>assign group</td>
<td>Assigning G Suite groups to G Suite groups on page 134</td>
</tr>
<tr>
<td>Assign customer as member</td>
<td>Assigning G Suite customers directly to a group</td>
</tr>
<tr>
<td>Exclude groups</td>
<td>Effectiveness of G Suite entitlement assignments on page 98</td>
</tr>
<tr>
<td>Assign system roles</td>
<td>Adding G Suite entitlements to system roles on page 94</td>
</tr>
<tr>
<td>Assign business roles</td>
<td>Assigning G Suite entitlements to business roles on page 93</td>
</tr>
<tr>
<td>Assign organizations</td>
<td>Assigning G Suite entitlements to departments, cost centers, and locations on page 92</td>
</tr>
<tr>
<td>Add to IT Shop</td>
<td>Adding G Suite entitlements to the IT Shop on page 94</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Synchronizing single objects on page 39</td>
</tr>
</tbody>
</table>

**Overview of G Suite groups**

Use this task to obtain an overview of the most important information about a group.

To obtain an overview of a group

1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **G Suite group overview** in the task view.

**Assigning extended properties to a G Suite group**

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.
**To specify extended properties for a group**

1. In the Manager, select the **G Suite | Groups** category.
2. Select the group in the result list.
3. Select **Assign extended properties**.
4. Assign extended properties in **Add assignments**.
   
   **TIP:** In the **Remove assignments** area, you can remove the assignment of extended properties.

   **To remove an assignment**
   - Select the extended property and double click 🆘.

5. Save the changes.

For more detailed information about setting up extended properties, see the **One Identity Manager Identity Management Base Module Administration Guide**.

**Assigning group managers**

Define the group managers for a group.

**To define the group managers for a group**

1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **Assign group managers**
4. In the **Table** menu, select the **G Suite user accounts** table.
5. Assign user accounts in **Add assignments**.
   - OR -
   - Remove user accounts from **Remove assignments**.
6. Save the changes.
NOTE: By default, G Suite customers and groups cannot be assigned as group managers. However, these assignments are possible in the Google admin console. If these assignments exist in the target system, they are imported into the One Identity Manager database during synchronization. Existing assignments can be displayed in Manager.

**To check whether groups are assigned to a group as the group manager**

1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **Assign group managers**
4. In the **Table** menu, select the **G Suite groups** table.
   
   In the **Remove assignments** area, all assigned groups are displayed.

**To check whether the customer is assigned to a group as the group manager**

1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **Assign group managers**
4. In the **Table** menu, select the **G Suite customers** table.
   
   In the **Remove assignments** area, the assigned customer is displayed.

In Manager, customers and groups cannot be assigned as group managers.

**Assigning group owners**

Define the group owners for a G Suite group.

**To define user accounts as group owners of a group**

1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **Assign group owners**.
4. In the **Table** menu, select the **G Suite user accounts** table.
5. Assign user accounts in **Add assignments**.
   
   - OR -
   
   Remove user accounts from **Remove assignments**.
6. Save the changes.
NOTE: By default, G Suite customers and groups cannot be assigned as group owners. However, these assignments are possible in the Google admin console. If these assignments exist in the target system, they are imported into the One Identity Manager database during synchronization. Existing assignments can be displayed in Manager.

To check whether groups are assigned to a group as the group owner
1. Select the category G Suite | Groups.
2. Select the group in the result list.
3. Select Assign group owners.
4. In the Table menu, select the G Suite groups table.
   In the Remove assignments area, all assigned groups are displayed.

To check whether the customer is assigned to a group as the group owner
1. Select the category G Suite | Groups.
2. Select the group in the result list.
3. Select Assign group owners.
4. In the Table menu, select the G Suite customers table.
   In the Remove assignments area, the assigned customer is displayed.

In Manager, customers and groups cannot be assigned as group owners.

Assigning G Suite groups to G Suite groups

G Suite groups can themselves be members of other G Suite groups. This means that the groups can be hierarchically structured.

To assign groups directly to a group as members
1. Select the category G Suite | Groups.
2. Select the group in the result list.
3. Select Assign groups.
4. Select the Has members tab.
5. Assign child groups in Add assignments.
   TIP: you can remove the assignment of groups in the Remove assignments area.

To remove an assignment
- Select the group and double click ✓.

6. Save the changes.
To add a group as a member of other groups

1. Select the category **G Suite | Groups**.
2. Select the group in the result list.
3. Select **Assign groups**.
4. Select the **Is member of** tab.
5. Assign parent groups in **Add assignments**.
   - **TIP:** you can remove the assignment of groups in the **Remove assignments** area.
   - **To remove an assignment**
     - Select the group and double click √.
6. Save the changes.

Related topics
- Assigning G Suite user accounts directly to an entitlement on page 96

Deleting G Suite groups

To delete a group

1. In the Manager, select the **G Suite | Groups** category.
2. Select the group in the result list.
3. Click DELETE.
4. Confirm the security prompt with Yes.

The group is deleted completely from the One Identity Manager database and from G Suite.

G Suite products and SKUs

Products and related services, as well as the licenses required for login, are represented in One Identity Manager as products and SKUs (Stock-Keeping-Units). To provide users with the required permissions to log on to G Suite, assign the product SKUs to the user accounts.
Editing master data for G Suite products and SKUs

To edit the master data of a product SKU

1. In Manager, select G Suite | Products and SKUs.
2. Select the product SKU in the result list.
3. Select Change master data.
4. Edit the master data for the product SKU.
5. Save the changes.

Detailed information about this topic

- General master data for G Suite products and SKUs on page 136

General master data for G Suite products and SKUs

For products and SKUs, edit the following master data.

Table 44: General master data of a product SKU

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite customer</td>
<td>Customer to which the product SKU belongs.</td>
</tr>
<tr>
<td>Product name</td>
<td>Display name of the product.</td>
</tr>
<tr>
<td>SKU name</td>
<td>Display name of the SKU.</td>
</tr>
<tr>
<td>Service item</td>
<td>Enter a service item for requesting the product SKU through the IT Shop.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the product SKU can only be requested through the IT Shop. The product SKU can be requested by employees through the Web Portal and distributed with a defined approval process. The product SKU can still be assigned directly to user accounts and hierarchical roles.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the product SKU can only be requested through the IT Shop. The product SKU can be requested by employees through the Web Portal and distributed with a defined approval process. Direct assignment of the product SKU to hierarchical roles or user accounts is not permitted.</td>
</tr>
</tbody>
</table>
### Property Description

**Risk index**
Value for evaluating the risk of assignments to the product SKU. Enter a value between 0 and 1. This input field is only visible if the configuration parameter `QER | CalculateRiskIndex` is activated. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.

**Category**
Categories for passing on the product SKU to user accounts. Product SKUs can be selectively passed on to user accounts. To do this, the product SKUs and user accounts are divided into categories. Select one or more categories from the menu.

### Related topics
- *Inheritance of G Suite entitlements based on categories* on page 101
- *Adding G Suite entitlements to the IT Shop* on page 94

### Additional tasks for managing G Suite products and SKUs

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of the G Suite product and the SKU</td>
<td>Overview of G Suite products and SKUs on page 138</td>
</tr>
<tr>
<td>Assigning extended properties</td>
<td>Assigning extended properties to G Suite products and SKUs on page 138</td>
</tr>
<tr>
<td>assign user accounts</td>
<td>Assigning G Suite user accounts directly to an entitlement on page 96</td>
</tr>
<tr>
<td>Assign system roles</td>
<td>Adding G Suite entitlements to system roles on page 94</td>
</tr>
<tr>
<td>Assign business roles</td>
<td>Assigning G Suite entitlements to business roles on page 93</td>
</tr>
<tr>
<td>Assign organizations</td>
<td>Assigning G Suite entitlements to departments, cost centers, and locations on page 92</td>
</tr>
<tr>
<td>Add to IT Shop</td>
<td>Adding G Suite entitlements to the IT Shop on page 94</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Synchronizing single objects on page 39</td>
</tr>
</tbody>
</table>
Overview of G Suite products and SKUs

You use this task to obtain an overview of the most important information for a product SKU.

To obtain an overview of a product SKU

1. Select G Suite | Products and SKUs.
2. Select the product SKU in the result list.
3. Select product and SKU overview.

Assigning extended properties to G Suite products and SKUs

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a product SKU

1. In Manager, select G Suite | Products and SKUs.
2. Select the product SKU in the result list.
3. Select Assign extended properties.
4. Assign extended properties in Add assignments.
5. Save the changes.

TIP: In the Remove assignments area, you can remove the assignment of extended properties.

To remove an assignment

- Select the extended property and double click.

G Suite organizations

Organizations are used to define the settings for the users of G Suite. Each customer has one parent organization. You can set up additional organizations below this organization and therefore create an organizational hierarchy. Child organizations inherit the settings of the relevant parent organization. User accounts are assigned to exactly one organization.
Creating G Suite organizations

To create an organization

1. In Manager, select G Suite | Organizations.
2. Click ➔ in the result list.
3. On the master data form, edit the master data for the organization.
4. Save the changes.

Related topics

- General master data for G Suite organizations on page 139
- Editing master data for G Suite organizations on page 139

Editing master data for G Suite organizations

To edit organization master data

1. In Manager, select G Suite | Organizations.
2. Select the organization from the result list.
3. Select Change master data.
4. Edit the master data for the organization.
5. Save the changes.

Related topics

- General master data for G Suite organizations on page 139
- Creating G Suite organizations on page 139

General master data for G Suite organizations

For organizations, edit the following master data:

Table 45: General master data for organizations

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite customer</td>
<td>Customer to which the organization belongs.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Organization ID</td>
<td>ID of the organization</td>
</tr>
<tr>
<td>Organization name</td>
<td>Display name of the organization</td>
</tr>
<tr>
<td>Full path</td>
<td>Full path of the organization.</td>
</tr>
<tr>
<td>Parent organization</td>
<td>The parent organization.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

**Additional tasks for managing G Suite organizations**

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of the G Suite organization</td>
<td><a href="#">Overview of G Suite organizations</a> on page 140</td>
</tr>
<tr>
<td>Synchronize object</td>
<td><a href="#">Synchronizing single objects</a> on page 39</td>
</tr>
<tr>
<td>Changing parent organizations</td>
<td><a href="#">Moving G Suite organizations</a> on page 140</td>
</tr>
</tbody>
</table>

**Overview of G Suite organizations**

Use this task to obtain an overview of the most important information about an organization.

To obtain an overview of an organization

1. Select G Suite | Organizations.
2. Select the organization from the result list.
3. Select organization overview | G Suite

**Moving G Suite organizations**

Child organizations can be moved within an organizational hierarchy. To move a child organization, assign a different parent organization to the child organization.
To move an organization

1. Select G Suite | Organizations.
2. Select the organization from the result list.
3. Select Change master data.
4. Select Change parent organizational unit in the task view.
5. Confirm the security prompt with Yes.
6. Select the new organization from the Parent organization menu.
7. Save the changes.

Deleting G Suite organizations

To delete an organization

1. In Manager, select G Suite | Organizations.
2. Select the organization from the result list.
3. Click 
4. Confirm the security prompt with Yes.

The organization is permanently deleted from the One Identity Manager database and from G Suite.

G Suite domains

In G Suite, the primary domain of a customer and additional Internet domains are mapped as One Identity Manager domains. Domains are imported into the One Identity Manager database during synchronization. You cannot edit their properties. Changes to the object properties of individual domains can be transferred via single object synchronization.

To display the properties of a domain:

1. In Manager, select G Suite | Domains.
2. Select the domain in the result list.
3. Select Change master data.

To obtain an overview of a domain

1. In Manager, select G Suite | Domains.
2. Select the domain in the result list.
3. Select domain overview.
G Suite domain aliases

Domain aliases provide the users of a primary domain with additional e-mail addresses. Domain aliases are imported into the One Identity Manager database during synchronization. You cannot edit their properties. Changes to the object properties of individual domain privileges can be transferred via single object synchronization.

To display the properties of a domain alias
1. In Manager, select G Suite | Domain aliases.
2. Select a domain alias in the result list.
3. Select Change master data.

To obtain an overview of a domain alias
1. In Manager, select G Suite | Domain aliases.
2. Select a domain alias in the result list.
3. Select domain alias overview.

G Suite admin roles

Admin roles are used to grant users administrative privileges in G Suite. Custom admin roles can be created in the One Identity Manager. To ensure that the users receive the privileges, assign the admin roles to user accounts.

Creating G Suite admin roles

To create an admin role
1. In Manager, select G Suite | Admin roles.
2. Click "+" in the result list.
3. On the master data form, edit the master data for the admin role.
4. Save the changes.

Related topics
- General master data for G Suite admin roles on page 143
- Editing master data for G Suite admin roles on page 143

Editing master data for G Suite admin roles

To edit the master data for an admin role
1. In Manager, select G Suite | Admin roles.
2. Select the admin role in the result list.
3. Select Change master data.
4. Edit the master data for the admin role.
5. Save the changes.

Related topics
- General master data for G Suite admin roles on page 143
- Creating G Suite admin roles on page 142

General master data for G Suite admin roles

For admin roles, edit the following master data:

Table 46: General master data for an admin role

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite customer</td>
<td>Customer to which the admin role belongs.</td>
</tr>
<tr>
<td>Role identifier</td>
<td>Unique ID of the role. For new admin roles, the ID is allocated in the target system.</td>
</tr>
<tr>
<td>Role name</td>
<td>Display name of the role</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Is super admin</td>
<td>Specifies whether the admin role is a super admin role.</td>
</tr>
<tr>
<td>Is system role</td>
<td>Specifies whether the admin role is a predefined admin role.</td>
</tr>
</tbody>
</table>
Additional tasks for managing G Suite admin roles

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite admin role overview</td>
<td>Overview of G Suite admin roles on page 144</td>
</tr>
<tr>
<td>Assign admin privileges</td>
<td>Assigning admin privileges to G Suite admin roles on page 144</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Synchronizing single objects on page 39</td>
</tr>
</tbody>
</table>

Overview of G Suite admin roles

You use this task to obtain an overview of the most important information for an admin role.

To obtain an overview of an admin role

1. Select G Suite | Admin roles.
2. Select the admin role in the result list.
3. Select admin role overview.

Assigning admin privileges to G Suite admin roles

Assign all the privileges to the custom admin roles that you want the user accounts to receive via this admin role.

To assign admin privileges to a custom admin role

1. In Manager, select G Suite | Admin roles.
2. Select the admin role in the result list.
3. Select Assign admin privileges.
4. Assign the admin privileges in the **Add assignments** area.
   
   **TIP:** you can remove the assignment of admin privileges in the **Remove assignments** area.

   **To remove an assignment**
   - Select the admin privilege and double click `✓`.

5. Save the changes.

**Related topics**
- [Assigning G Suite admin privileges to admin roles](#) on page 147

### Deleting G Suite admin roles

Custom admin roles can be deleted in the Manager. System roles cannot be deleted.

**To delete a custom admin role**

1. In Manager, select **G Suite | Admin roles**.
2. Select the admin role in the result list.
3. Click `Trash`.
4. Confirm the security prompt with **Yes**.

The admin role is permanently deleted from the One Identity Manager database and from G Suite.

### G Suite admin privileges

Admin privileges represent the administrative privileges that user accounts receive via the assigned admin roles. Admin privileges are imported into the One Identity Manager database during synchronization. You cannot edit their properties. Changes to the object properties of individual admin privileges can be transferred via single object synchronization.
Display master data for G Suite admin privileges

To display the master data for an admin privilege

1. In Manager, select G Suite | Admin privileges.
2. Select the admin privileges in the result list.
3. Select Change master data.

Related topics

- Overview of G Suite admin privileges on page 146

Additional tasks for managing G Suite admin privileges

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of G Suite admin</td>
<td>Overview of G Suite admin privileges on page 146</td>
</tr>
<tr>
<td>privileges</td>
<td></td>
</tr>
<tr>
<td>Admin role designations</td>
<td>Assigning G Suite admin privileges to admin roles on page 147</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Synchronizing single objects on page 39</td>
</tr>
</tbody>
</table>

Overview of G Suite admin privileges

You use this task to obtain an overview of the most important information for an admin privilege.

To obtain an overview of admin privileges

1. Select G Suite | Admin privileges.
2. Select the admin privileges in the result list.
3. Select admin privilege overview.G Suite
Assigning G Suite admin privileges to admin roles

You assign an admin privilege to various custom admin roles.

**To assign admin privileges to custom admin roles**

1. In Manager, select **G Suite | Admin privileges**.
2. Select the admin privileges in the result list.
3. Select **Assign admin role**.
4. Assign the admin roles in the **Add assignments** area.
   - **TIP:** you can remove the assignment of admin roles in the **Remove assignments** area.
   - **To remove an assignment**
     - Select the admin role and double click ✅.
5. Save the changes.

Related topics

- [Assigning admin privileges to G Suite admin roles](#) on page 144

G Suite admin role assignments

Administrative privileges can be limited to individual organizations. To enable this, assign the admin roles to organizations. User accounts that are assigned this type of admin role can use the related administrative privileges only in the assigned organization.

Creating G Suite admin role designations

**To assign an organization to an admin role**

1. In Manager, select **G Suite | Admin role designations**.
2. Click 🏛️ in the result list.
3. On the master data form, edit the designation.
   - Select the required admin role from the **Admin role** menu.
   - Select the required organization from the **G Suite Organization** menu.
4. Save the changes.
Related topics

- Assigning user accounts to G Suite admin role designations on page 148

Additional tasks for managing G Suite admin role assignments

After you have entered the master data, you can run the following tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite admin role assignment</td>
<td>Overview of G Suite admin role designations on page 148</td>
</tr>
<tr>
<td>assign user accounts</td>
<td>Assigning user accounts to G Suite admin role designations on page 148</td>
</tr>
<tr>
<td>Synchronize object</td>
<td>Synchronizing single objects on page 39</td>
</tr>
</tbody>
</table>

Overview of G Suite admin role designations

You use this task to obtain an overview of the most important information for an admin role designation.

**To obtain an overview of admin role designations**

1. Select G Suite | Admin role designations.
2. Select the admin role designation in the result list.
3. Select admin role assignment overview.G Suite

Assigning user accounts to G Suite admin role designations

Assign all user accounts that you want to receive the administrative privileges for the organization to the admin role designations.

**To assign user accounts to an admin role designation**

1. In Manager, select G Suite | Admin role designations.
2. Select the admin role designation in the result list.
3. Select Assign user accounts in the task view.
4. Assign user accounts in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of user accounts.

   **To remove an assignment**
   - Select the user accounts and double click ☑.

5. Save the changes.

### Deleting G Suite admin role designations

**To delete an admin role assignment**

1. In Manager, select **G Suite | Admin role designations**.
2. Select the admin role designation in the result list.
3. Click 🗑.
4. Confirm the security prompt with **Yes**.

The admin role is permanently deleted from the One Identity Manager database and from G Suite.

### Reports about G Suite objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for G Suite environments.

<table>
<thead>
<tr>
<th>Table 47: Reports for the target system</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>report</strong></td>
</tr>
<tr>
<td>Overview of all assignments (customer)</td>
</tr>
<tr>
<td>Overview of all assignments (group)</td>
</tr>
<tr>
<td>Overview of all assignments (product and SKU)</td>
</tr>
<tr>
<td>G Suite user</td>
</tr>
<tr>
<td>report</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>account and group administration</td>
</tr>
<tr>
<td>Show unused user accounts</td>
</tr>
<tr>
<td>Show entitlement drifts</td>
</tr>
<tr>
<td>Show user accounts with an above average number of system entitlements</td>
</tr>
<tr>
<td>Show orphaned user accounts</td>
</tr>
<tr>
<td>Data quality summary for G Suite user accounts</td>
</tr>
</tbody>
</table>
Handling of G Suite objects in Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal. The Web Portal supports the administration of G Suite for the following tasks:

- **Managing user accounts and employees**
  An account definition can be requested by shop customers in IT Shop when it is assigned to an Web Portal shelf. The request undergoes a defined approval procedure. The user account is not created until it has been agreed by an authorized person, such as a manager.

- **Managing entitlement assignments**
  When a G Suite entitlement is assigned to an IT Shop shelf, the entitlement can be requested by the shop customers in the Web Portal. The request undergoes a defined approval procedure. The entitlement is not assigned until it has been approved by an authorized person.
  
  In the Web Portal, managers and administrators of organizations can assign G Suite entitlements to the departments, cost centers, or locations for which they are responsible. The entitlements are inherited by all persons who are members of these departments, cost centers, or locations.
  
  If the Business Roles Module is available, managers and administrators of business roles in Web Portal can assign G Suite entitlements to the business roles for which they are responsible. The entitlements are inherited by all persons who are members of these business roles.
  
  If the System Roles Module is available, supervisors of system roles in Web Portal can assign G Suite entitlements to the system roles. The entitlements are inherited by all persons to whom these system roles are assigned.

- **Attestation**
  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in Manager. The attesters use the Web Portal to approve attestation cases.

- **Governance administration**
If the Compliance Rules Module is available, you can define rules that identify the invalid entitlement assignments and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in Manager. Supervisors use the Web Portal to check and resolve rule violations and to grant exception approvals.

If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment
  You can use the risk index of G Suite entitlements to evaluate the risk of entitlement assignments for the company. The One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics
  The Web Portal provides a range of reports and statistics about the employees, user accounts, and their entitlements and risks.

For more information about the named topics, see Assigning G Suite entitlements to user accounts in One Identity Manager on page 90 and refer to the following guides:

- One Identity Manager Web Portal User Guide
- One Identity Manager Attestation Administration Guide
- One Identity Manager Compliance Rules Administration Guide
- One Identity Manager Company Policies Administration Guide
- One Identity Manager Risk Assessment Administration Guide
Basic data for managing G Suite

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

- **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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.
  For more information, see Account definitions for G Suite user accounts on page 46.

- **Password policy**
  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 use or customize if required. You can also define your own password policies.
  For more information, see Password policies for G Suite user accounts on page 77.

- **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 40.

- **Server**
  In order to handle G Suite -specific processes in One Identity Manager, the synchronization server and its server functions must be declared.
  For more information, see Job server for G Suite-specific process handling on page 154.

- **Target system managers**
  A default application role exists for the target system manager in One Identity Manager. Assign the employees who are authorized to edit all G Suite objects in One Identity Manager to this application role.
ns for target system managers to individual farms. SharePoint Define additional application roles if you want to limit the edit permissions for target system managers to individual customers. The application roles must be added under the default application role.

For more information, see Target system managers for customers on page 158.

Job server for G Suite-specific process handling

In order to handle G Suite-specific processes in One Identity Manager, the synchronization server and its server functions must be declared. You have several options for defining a server's functionality:

- Create an entry for the Job server in Designer under Base Data | Installation | Job server. For detailed information, see One Identity Manager Configuration Guide.
- Select an entry for the Job server in Manager | Basic configuration data | Server in 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.

Related topics
- System requirements for the G Suite synchronization server on page 17

Editing G Suite Job servers

To edit a Job server and its functions

1. In Manager, select the category G Suite | Basic configuration data | Server.
2. Select the Job server entry in the result list.
3. Select Change master data.
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
- General master data for Job servers on page 155
- Specifying server functions on page 157
General master data for Job servers

**NOTE:** All editing options are also available in Designer under *Base Data | Installation | Job server.*

**NOTE:** More properties may be available depending on which modules are installed.

### Table 48: Job Server Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</td>
</tr>
<tr>
<td>Full server name</td>
<td>Full server name in accordance with DNS syntax.</td>
</tr>
<tr>
<td></td>
<td>Example: &lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</td>
</tr>
<tr>
<td>Target system</td>
<td>Computer account target system.</td>
</tr>
<tr>
<td>Language</td>
<td>Language of the server.</td>
</tr>
<tr>
<td>Server is cluster</td>
<td>Specifies whether the server maps a cluster.</td>
</tr>
<tr>
<td>Server belongs to cluster</td>
<td>Cluster to which the server belongs.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The properties <strong>Server is cluster</strong> and <strong>Server belongs to cluster</strong> are mutually exclusive.</td>
</tr>
<tr>
<td>IP address (IPv6)</td>
<td>Internet protocol version 6 (IPv6) server address.</td>
</tr>
<tr>
<td>IP address (IPv4)</td>
<td>Internet protocol version 4 (IPv4) server address.</td>
</tr>
<tr>
<td>Copy process (source server)</td>
<td>Permitted copying methods that can be used when this server is the source of a copy action.</td>
</tr>
<tr>
<td></td>
<td>At present, only copy methods that support the Robocopy and rsync programs are supported.</td>
</tr>
<tr>
<td></td>
<td>If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.</td>
</tr>
</tbody>
</table>
| Copy                            | Permitted copying methods that can be used when this server is the destin-
<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>process (target server)</td>
<td>action of a copy action.</td>
</tr>
<tr>
<td>Coding</td>
<td>Character set coding that is used to write files to the server.</td>
</tr>
<tr>
<td>Parent Job server</td>
<td>Name of the parent Job server.</td>
</tr>
<tr>
<td>Executing server</td>
<td>Name of the executing server. The name of the server that exists physically and where the processes are handled.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Queue</td>
<td>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.</td>
</tr>
<tr>
<td>Server operating system</td>
<td>Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values <strong>Win32</strong>, <strong>Windows</strong>, <strong>Linux</strong> and <strong>Unix</strong> are permitted. If no value is specified, <strong>Win32</strong> is used.</td>
</tr>
<tr>
<td>Service account data</td>
<td>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.</td>
</tr>
<tr>
<td>One Identity Manager Service installed</td>
<td>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.</td>
</tr>
<tr>
<td>Stop One Identity Manager Service</td>
<td>Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the program &quot;Job Queue Info&quot;. For more detailed information, see the One Identity Manager Process Monitoring and Troubleshooting Guide.</td>
</tr>
</tbody>
</table>
### Property | Meaning
--- | ---
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 157

### Specifying server functions

**NOTE:** All editing options are also available in Designer under **Base Data | Installation | Job server.**

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

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

#### Table 49: Permitted server functions

<table>
<thead>
<tr>
<th>Server function</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Server</td>
<td>This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that 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.</td>
</tr>
<tr>
<td>SQL processing server</td>
<td>The server can execute 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.</td>
</tr>
<tr>
<td>CSV script server</td>
<td>The server can process CSV files using the ScriptComponent process component.</td>
</tr>
<tr>
<td><strong>Server function</strong></td>
<td><strong>Remark</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>One Identity Manager Service installed</td>
<td>Server on which a One Identity Manager Service is installed.</td>
</tr>
<tr>
<td>SMTP host</td>
<td>Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.</td>
</tr>
<tr>
<td>Default report server</td>
<td>Server on which reports are generated.</td>
</tr>
<tr>
<td>G Suite connector</td>
<td>Server on which the G Suite connector is installed. This server executes synchronization with the target system G Suite.</td>
</tr>
</tbody>
</table>

**Related topics**

- General master data for Job servers on page 155

**Target system managers for customers**

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

ns for target system managers to individual farms. SharePoint Define additional application roles if you want to limit the edit permissions for target system managers to individual customers. The application roles must be added under the default application role.

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

**Implementing application roles for target system managers**

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

Table 50: Default Application Roles for Target System Managers

<table>
<thead>
<tr>
<th>User</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target system managers</td>
<td>Target system managers must be assigned to **Target systems</td>
</tr>
<tr>
<td></td>
<td>- Assume administrative tasks for the target system.</td>
</tr>
<tr>
<td></td>
<td>- Create, change or delete target system objects, like user accounts</td>
</tr>
<tr>
<td></td>
<td>or groups.</td>
</tr>
<tr>
<td></td>
<td>- Edit password policies for the target system.</td>
</tr>
<tr>
<td></td>
<td>- Prepare entitlements for adding to the IT Shop.</td>
</tr>
<tr>
<td></td>
<td>- Can add employees, who have an other identity than the <strong>Primary</strong></td>
</tr>
<tr>
<td></td>
<td>identity.</td>
</tr>
<tr>
<td></td>
<td>- Configure synchronization in the Synchronization Editor and defines</td>
</tr>
<tr>
<td></td>
<td>the mapping for comparing target systems and One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>- Edit the synchronization’s target system types and outstanding</td>
</tr>
<tr>
<td></td>
<td>objects.</td>
</tr>
<tr>
<td></td>
<td>- Authorize other employees within their area of responsibility as</td>
</tr>
<tr>
<td></td>
<td>target system managers and create child application roles if</td>
</tr>
<tr>
<td></td>
<td>required.</td>
</tr>
</tbody>
</table>

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

1. Log in to One Identity Manager as Manager administrator (**Base role | Administrators**)
2. Select **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees**.
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 Manager as target system administrator (**Target systems | Administrators**).
2. Select **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 Manager as target system manager.
2. Select the application role in G Suite | Basic configuration data | Target system managers.
3. Select Assign employees.
4. Assign the employees you want and save the changes.

To specify target system managers for individual customers

1. Log in to Manager as target system manager.
2. Select G Suite | Customers.
3. Select the customer in the result list.
4. Select Change master data.
5. On the General tab, select the application role in the Target system manager menu.
   - OR -
   Next to the Target system manager menu, click ⌁ to create a new application role.
   a. Enter the application role name and assign the Target systems | G Suite parent application role.
   b. Click OK to add the new application role.
6. Save the changes.
7. Assign employees to this application role who are permitted to edit the customer in One Identity Manager.

Related topics

- One Identity Manager users for managing G Suite on page 10
- General master data for G Suite customers on page 106
Troubleshooting the connection to a G Suite environment

Newly added G Suite 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 40.
   a. Select the object that have been wrongly marked as outstanding.
   b. Apply the Reset method.
      This removes the Outstanding mark. the next time synchronization is run, the error should not occur.
For more detailed information about defining a scope and specifying handling methods for synchronization steps, see the One Identity Manager Target System Synchronization Reference Guide.
Appendix: Configuration parameters for managing G Suite

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

**Table 51: Configuration parameters for synchronizing G Suite**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning if Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Meaning if Set</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>InitialRandomPassword</td>
<td>their initial password. The Employee - initial password for new user account mail template is used.</td>
</tr>
<tr>
<td>SendTo</td>
<td></td>
</tr>
<tr>
<td>MailTemplatePassword</td>
<td></td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>GoogleApps</td>
</tr>
</tbody>
</table>
Appendix: Default project templates for G Suite

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

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

The template uses mappings for the following schema types.

Table 52: Mapping G Suite schema types to tables in the One Identity Manager schema.

<table>
<thead>
<tr>
<th>Schema Type in G Suite</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminPrivilege</td>
<td>GAPPrivilege</td>
</tr>
<tr>
<td>AdminRole</td>
<td>GAPAdminRole</td>
</tr>
<tr>
<td>AdminRoleAssignment</td>
<td>GAPOrgAdminRole</td>
</tr>
<tr>
<td>Customer</td>
<td>GAPCustomer</td>
</tr>
<tr>
<td>Domain</td>
<td>GAPDomain</td>
</tr>
<tr>
<td>DomainAlias</td>
<td>GAPDomainAlias</td>
</tr>
<tr>
<td>Group</td>
<td>GAPGroup</td>
</tr>
<tr>
<td>OrgUnit</td>
<td>GAPOrgUnit</td>
</tr>
<tr>
<td>ProductAndSku</td>
<td>GAPPaSku</td>
</tr>
<tr>
<td>User</td>
<td>GAPUser</td>
</tr>
<tr>
<td>UserAddress</td>
<td>GAPUserAddress</td>
</tr>
<tr>
<td>UserEmail</td>
<td>GAPUserEmail</td>
</tr>
<tr>
<td>Schema Type in G Suite</td>
<td>Table in the One Identity Manager Schema</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>UserExternalId</td>
<td>GAPUserExternalId</td>
</tr>
<tr>
<td>UserIm</td>
<td>GAPUserIM</td>
</tr>
<tr>
<td>UserOrganization</td>
<td>GAPUserOrganization</td>
</tr>
<tr>
<td>UserPhone</td>
<td>GAPUserPhone</td>
</tr>
<tr>
<td>UserRelation</td>
<td>GAPUserRelation</td>
</tr>
<tr>
<td>UserWebsite</td>
<td>GAPUserWebSite</td>
</tr>
</tbody>
</table>
Appendix: API scopes for the service account

The service account’s client ID must be authorized for various API scopes in the Google Admin console:

For read and write access:

- https://www.googleapis.com/auth/admin.directory.customer,
- https://www.googleapis.com/auth/admin.directory.device.chromeos,
- https://www.googleapis.com/auth/admin.directory.device.mobile,
- https://www.googleapis.com/auth/admin.directory.device.chromeos.mobile.action,
- https://www.googleapis.com/auth/admin.directory.domain,
- https://www.googleapis.com/auth/admin.directory.group,
- https://www.googleapis.com/auth/admin.directory.group.member,
- https://www.googleapis.com/auth/admin.directory.notifications,
- https://www.googleapis.com/auth/admin.directory.orgunit,
- https://www.googleapis.com/auth/admin.directory.resource.calendar,
- https://www.googleapis.com/auth/admin.directory.rolemanagement,
- https://www.googleapis.com/auth/admin.directory.user,
- https://www.googleapis.com/auth/admin.directory.user.alias,
- https://www.googleapis.com/auth/admin.directory.user.security,
- https://www.googleapis.com/auth/admin.directory.userschema,
- https://www.googleapis.com/auth/apps.groups.settings,
- https://www.googleapis.com/auth/admin.datatransfer,
- https://www.googleapis.com/auth/apps.licensing

For read-only access:

- https://www.googleapis.com/auth/admin.directory.customer.readonly,
- https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly,
- https://www.googleapis.com/auth/admin.directory.device.mobile.readonly,
- https://www.googleapis.com/auth/admin.directory.domain.readonly,
- https://www.googleapis.com/auth/admin.directory.group.readonly,
- https://www.googleapis.com/auth/admin.directory.group.member.readonly,
- https://www.googleapis.com/auth/admin.directory.orgunit.readonly,
- https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly,
- https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
- https://www.googleapis.com/auth/admin.directory.user.readonly,
- https://www.googleapis.com/auth/admin.directory.user.alias.readonly,
https://www.googleapis.com/auth/admin.directory.userschema.readonly,
https://www.googleapis.com/auth/apps.groups.settings,
https://www.googleapis.com/auth/admin.datatransfer.readonly,
https://www.googleapis.com/auth/apps.licensing
The following table describes permitted editing methods for G Suite schema types.

### Table 53: Methods available for editing schema types

<table>
<thead>
<tr>
<th>Schema type</th>
<th>Read</th>
<th>Paste</th>
<th>Delete</th>
<th>Refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>G Suite customer (Customer)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Domain (Domain)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Domain alias (DomainAlias)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Organization (OrgUnit)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account (User)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group (Group)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Product and SKU (ProductAndSku)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: address (UserAddress)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: Email address (UserEmail)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: external ID (UserExternalId)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: instant messenger (UserIm)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: user details (UserOrganization)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: phone number (UserPhone)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: relation (UserRelation)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User account: website (UserWebsite)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin role (AdminRole)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin privilege (AdminPrivilege)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Admin roles assignments (AdminRoleAssignment)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Appendix: Special features in the assignment of G Suite groups

In One Identity Manager, entitlements can be assigned directly or indirectly to user accounts. The type of assignment is indicated in the XOrigin column in the assignment tables. In the GAPUserInPaSku and GAPUserInGroup assignment tables, XOrigin can have the default values 1 to 15 (bit 0 to 3).

Through the assignment of a G Suite groups to a G Suite customer, all the customer's user accounts can become members of the group. In the calculation of inheritance, an entry is made in the GAPUserInGroup table for each of the customer's user accounts. The origin of these assignments is indicated in GAPUserInGroup.XOrigin with the value 16 (bit 4).

Table 54: Origin of entitlement assignments

<table>
<thead>
<tr>
<th>Assignment table</th>
<th>Type of assignment</th>
<th>Origin (XOrigin column)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAPUserInPaSku</td>
<td>direct</td>
<td>1</td>
</tr>
<tr>
<td>GAPUserInPaSku</td>
<td>indirect</td>
<td>2</td>
</tr>
<tr>
<td>GAPUserInGroup</td>
<td>Dynamic</td>
<td>4</td>
</tr>
<tr>
<td>GAPUserInGroup</td>
<td>assignment request</td>
<td>8</td>
</tr>
<tr>
<td>GAPUserInGroup</td>
<td>via customers</td>
<td>16</td>
</tr>
</tbody>
</table>

For detailed information about the calculation of assignments in One Identity Manager, see the One Identity Manager Identity Management Base Module Administration Guide.

Related topics

- Assigning G Suite entitlements to user accounts in One Identity Manager on page 90
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

**A**
- account definition 46
  - add to IT Shop 60
- assign automatically 58
- assign to all employees 58
- assign to business role 57
- assign to cost center 57
- assign to customers 61
- assign to department 57
- assign to employee 56, 59
- assign to location 57
- assign to system roles 59
- assign to user account 69
- create 47
- creating manage level 50
- delete 62
- edit 47
- editing manage level 49
- IT operating data 52-53
- address 118
- admin privilege
  - admin role designations 147
  - display 146
  - overview 146
- admin role assignment
  - add 147
  - insert 147
- admin roles
  - add 142
  - assign admin privileges 144
  - assign to organisation 147
- assign user accounts 148
  - create 142
  - delete 145
  - edit 143
  - insert 142
  - overview 144
  - predefined 143
    - super admin 143
    - system role 143
- admin roles assignment
  - assign user accounts 148
  - create 147
  - delete 149
  - overview 148
- API scope 14, 30
- application roles for G Suite 10
- authorization assignment
  - direct 96-97

**B**
- base object 33, 36

**C**
- cache 33
- calculation schedule 37
  - disable 39
- category 108
- configuration parameter 12, 163
- convert connection parameter 33
customer
  account definition 106
  account definition (initial) 61
  add 105
  address 108
  alternative email address 106
  assign group 97, 170
  category 101
  contact person 108
  create 105
  domain 106
  edit 106
  insert 105
  organizations 108
  overview 109
  report 149
  synchronization type 106
  target system manager 10, 158

D
  data transfer 126
  default email address for data transfer 126
  default user accounts 71
  direction of synchronization
    direction target system 22, 27
    in Manager 22
  domain 141
    overview 141
    synchronizing 141
  domain alias 142
    overview 142
    synchronizing 142
  dummy employee 74

E
  email address 118
  email notification 89
  employee
    assign user account 69
    group identity 74
    main identity 73
    personalized admin identity 73
    primary identity 74
  employee assignment
    manual 66
    remove 66
    search criteria 65
  exclusion definition 98
  extended property
    G Suite group 131
    G Suite products and SKUs 138
    user account 123
  external ID 119

G
  G Suite
    troubleshooting 161
  G Suite customer 109
  group
    about IT Shop requests 128
    add to IT Shop 94
    additional settings 129
    Aliases 128
    assign business role 93
    assign category 128
    assign cost center 92
    assign customer 98
assign department 92
assign extended properties 131
assign group 134
assign location 92
assign system role 94
assign user account 90, 96
assigning through customers 170
category 101
create 127
delete 135
edit 127
effective 98
email address 128
exclusion 98
inheriting through roles 90
inheriting through system roles 94
language 129
manager 132
overview 131
overview of all assignments 103
owner 133
parent 134
risk index 128
spam message 129
subordinate 134
group identity 74
group manager 132
group owner 133

IT Shop shelf
assign account definition 60
assign group 94
assign products and SKUs 94

J
Job server 154
et 18, 154
properties 155

L
log file 43
login data 89

M
manage level
create 50
edit 49
membership
modify provisioning 35

N
NLog 43
notification 89

O
object
delete immediately 40
outstanding 40
publish 40
organization hierarchy
change 140

I
identity 70
inheritance
category 101
IT operating data
change 55
organizations 120
   add 139
   assign to admin role 147
change 123
   changing parent organizations 140
create 139
customer 139
delete 141
edit 139-140
insert 139
move 140
overview 140
parent 139
outstanding object 40

P
password
   initial 88-89
password policy 77
   assign 79
   character sets 83
   check password 87
   conversion script 84, 86
create 81
default policy 79, 81
display name 81
edit 81
error message 81
excluded list 87
failed logins 82
generate password 88
initial password 82
name components 82
new 81
password age 82
password cycle 82
password length 82
password strength 82
predefined 78
test script 84
permission
   add to IT Shop 94
   assign business role 93
   assign organizations 92
   assign system role 94
   assign user account 96
category 101
effective 98
exclusion 98
group 90
   inheriting through categories 108
   inheriting through system roles 94
overview of all assignments 103
product and SKU 90
personalized admin identity 73
phone 117
polling count 33
product and SKU
   about IT Shop requests 136
   add to IT Shop 94
   assign business role 93
   assign category 136
   assign cost center 92
   assign department 92
   assign extended properties 138
   assign location 92
   assign system role 94
   assign user account 90, 96
category 101
edit 136
inheriting through roles 90
inheriting through system roles 94
overview 138
overview of all assignments 103
risk index 136
project template 165
provisioning
members list 35

R
relation 121
reset revision 43
reset start up data 43
retries 33
revision filter 30
risk assessment
  group 128
  product and SKU 136
  user account 113

S
schema
  changes 29
  shrink 29
  update 29
scope 161
server 154
server function 157
single object synchronization 36, 39
site 121
start up configuration 33
synchronization
  accelerate 30
  API access 14
  authorizations 14
  base object
    create 28
  calculation schedule 37
  configure 22, 26
  connection parameter 22, 26, 28
different customers 22, 26, 28
extended schema 28
prerequisite 13
prevent 39
scope 26, 161
simulate 43
start 22, 37
synchronization project
  create 22
target system schema 28
user 14
variable 26
variable set 28
workflow 22, 27
synchronization analysis report 43
synchronization configuration
  customize 26-28
synchronization log 38, 43
  contents 26
  create 26
synchronization project
  create 22
disable 39
edit 109
  project template 165
synchronization server 17, 154
  configure 17
  edit 154
  install 18
Job server 18
server function 157
system requirements 17
synchronization workflow
create 22, 27
synchronize single object 39
system
employee assignment 65
specify category 108
system connection
advanced settings 30, 34
API access 30
cache 30
enabled variable set 34
polling count 30
retries 30
timeout 30

T
target system manager 158
specify 106
target system synchronization 40
template
IT operating data, modify 55
timeout 33

U
user account 110
address 118
admin role designations 97
administrative user account 72
apply template 55
assign employee 64
assign extended properties 123
assign group 97
assign permissions 97
assign products and SKUs 97
assigned employee 113
assigned permissions 149
assigning through customers 170
category 101
change organisation 123
connected 69
create 111
customer 113
data quality 149
default user accounts 71
deferred deletion 125
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
default user accounts 71
delete 125-126
edit 112, 123
email address 113, 118
template
IT operating data, modify 55
timeout 33
external ID 119
group identity 74
identity 70
instant messenger 119
lock 123, 125
move 123
organizations 113, 120
outstanding 161
overview 122
password 88, 117
notification 89
personalized admin identity 73
privileged user account 70, 72, 75
relations 121
restore 125
risk index 113
site 121
synchronization 161
telephone number 117
type 70-71, 75
unused 149
user details 120
user data
  transfer 126
user detail 120

V
variable set 33
  active 34

X
XOrigin
  bit 4 170