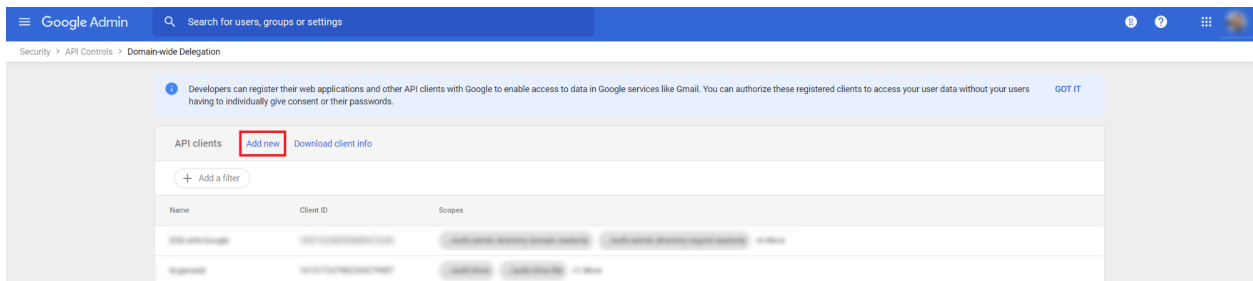# DSS-Support GoogleCDS

Foreword

Google Cloud Directory Sync enables administrators to synchronize users, groups, and other data from an Active Directory/LDAP service to their Google Cloud domain directory.
We're using Directory API Service for synchronization from Google to our LDAP app.
A service account that enables server-to-server authentication using a robot account for authorization between machines is required.. Customers will need to make some settings in the Google Admin Workspace account.

General Flow

1) Register the client id, which will be used to grant access to the directory in Google Admin:
   Go to **Security→API Controls→Domain-wide Delegation** and click on the button **Add New**.

2) Populate the fields with data:
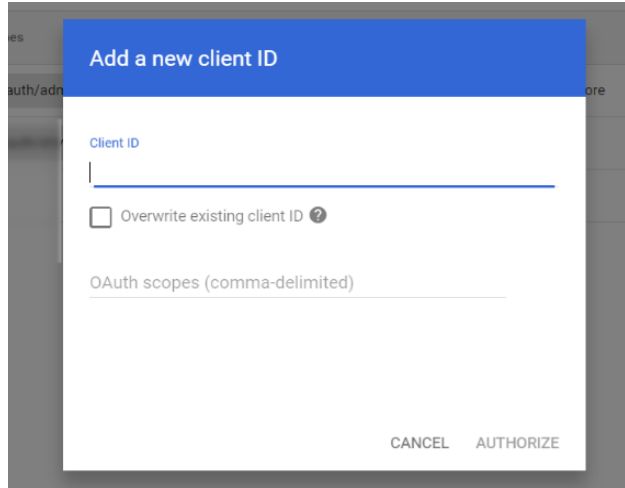   ➔ **Client ID:** 117731328853281683659
   ➔ **OAuth scopes:**
   https://www.googleapis.com/auth/admin.directory.domain.readonly
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly
   https://www.googleapis.com/auth/admin.directory.group.readonly
   https://www.googleapis.com/auth/admin.directory.group.member.readonly
   https://www.googleapis.com/auth/admin.directory.user.readonly

   All scopes are read-only, have access only to view, not to manage customer data.

Add a new client ID

Client ID

☐ Overwrite existing client ID ❓

OAuth scopes (comma-delimited)

CANCEL   AUTHORIZE

✕   DSS-with-Google

Client ID

109116248294689413242

Scopes

https://www.googleapis.com/auth/admin.directory.domain.readonly

https://www.googleapis.com/auth/admin.directory.orgunit.readonly

https://www.googleapis.com/auth/admin.directory.group.readonly

https://www.googleapis.com/auth/admin.directory.user.readonly

https://www.googleapis.com/auth/admin.directory.group.member.read
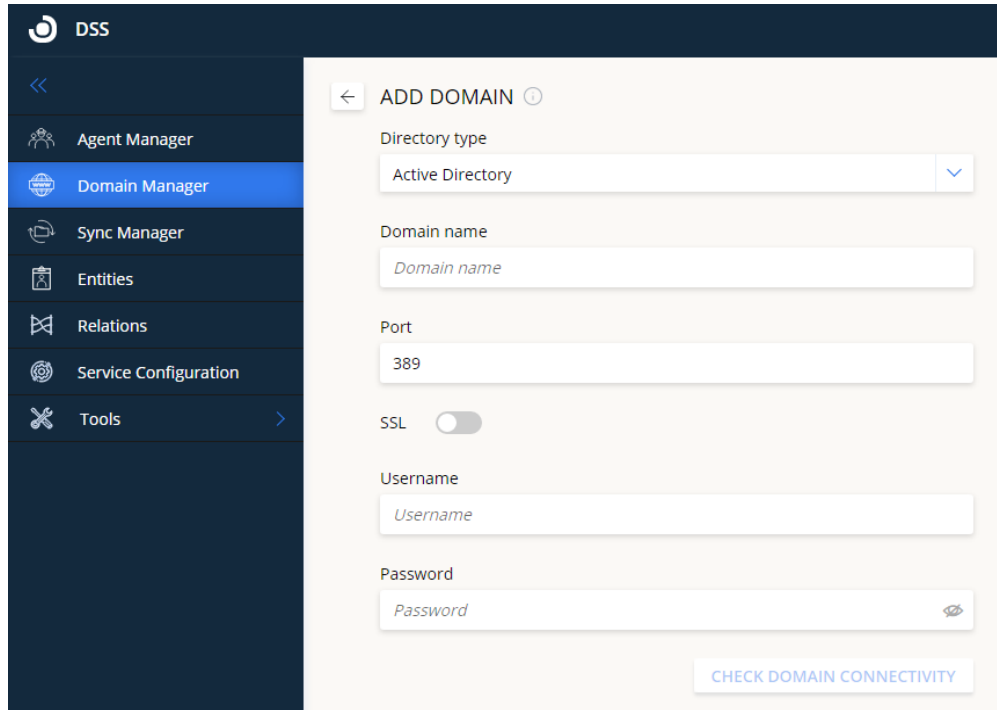
EDIT

Directory Synchronization Google CDS

Add to Domain manager screen a new directory type Google CDS.

When **selected** update the fields below accordingly
1. **Client ID - 117731328853281683659**
2. Domain Name
3. Username

The Client ID is a read-only field that the customer will need to use to approve our LDAP app in his domain via Google Admin.
The Username is the email of the admin account that will be used for the connection.

Sync Configuration

Destination & Time

Start node options:
LDAP Directory in the Google structure is different and user can:

1. Leave an empty value - the sync will go through all ous, groups and users.
2. Group=<group name> - enter the group he would like to start to synchronize from a specific group.
   Google Groups is a service that Google provides to create email-based groups similar to an email alias or list. These groups can be used as email lists, to assign specific permissions on Google Apps.
3. OU=<ou name> - enter the OU he would like the sync to start from a specific OU.

When the user will use a specific depth, will be scanned other ous/groups connected to the start ou/group according to the search depth value.

Update the below text in the Info icon of the destination & time
Start sync from:
Defines where the sync will start from.

- Leave empty to sync all the users and groups in the directory;
- OU=<ou name> - specify the ou you would like to start from.
- Group=<group name> - specify the group you would like to start from.

Once configured, click Test to make sure the domain is valid (it might take up to 2 minutes for the test to complete)

Inline text:

Leave empty to sync all directory, or enter ou=<ou name> // (only 1 ou allowed), or enter group=<group name> // (only 1 group allowed)

Object

Object Type

Object type "Computers" **is not supported**. Instead, Google CDS has [Mobile devices](#), [Chrome devices](#), and [Chrome browsers](#) (available only beta version). But we still have to investigate it. <u>Remove the computers option.</u>
Update the info text of the Object tab
Sync Objects: Configure which objects to sync by (currently only users object is supported)

Sync Attribute

The Google CDS doesn't have by default attribute value, for this, all queries are made by email.
Remove the CN, the samAccountName, the userPrincipalName from the Sync Attributes list.

Membership Filter:

When the Google CDS is selected update the DD list to show options
1. All Objects
2. Only members of OUS
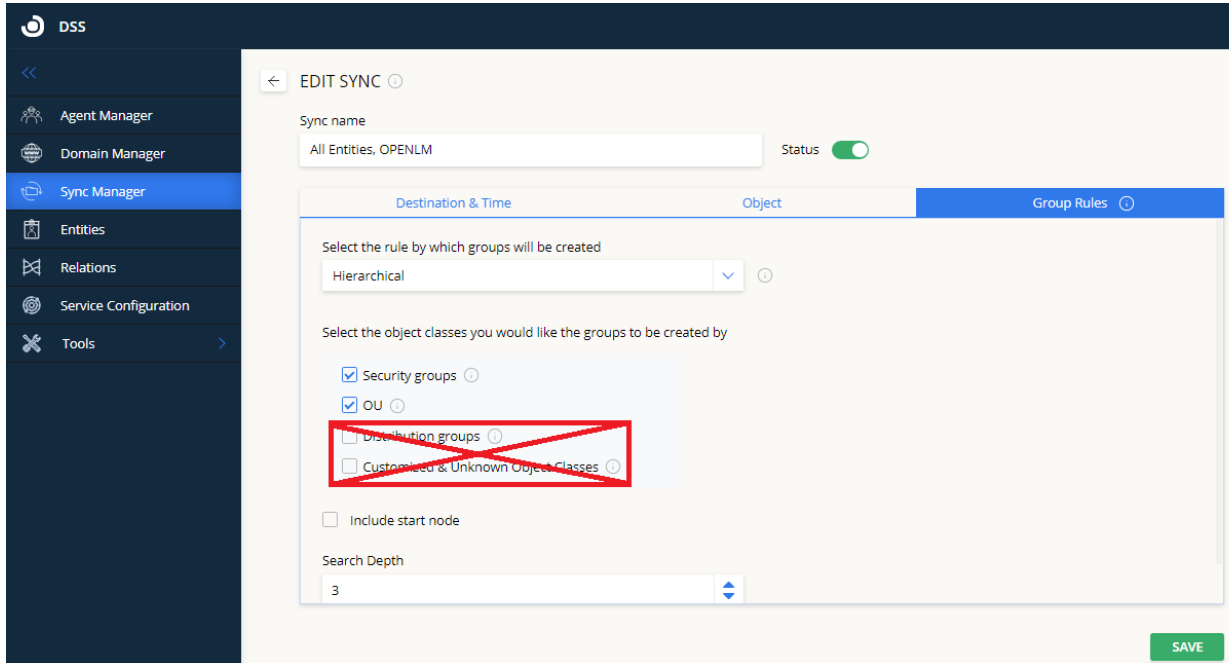3. Only members of Security Groups

Search depth

The Search depth is relevant in all cases for the group and the ou.

Group Rules

All group rules are supported, but the hierarchy synchronization supports only **groups** and **ous**.
Remove the rest options:
● Distribution group;
● Customize & unknown object classes;

Include start node is the same as in other syncs.

Search Depth - can't be higher than the Search depth was selected in the Object screen.

Set a default group-supported

Directory sample

The directory has OUS A-E

→ indicate pointer from one ou to another sub-OU

A → B
B → C
C → A
C → D
D

User list :

OU A - A3, A4
OU B - A1, A2
OU C - A5, A6
OU D - A7, A8

Hierarchical structure if the sync is configured to sync from OU=B with search depth of 3 in the group & rules

```
B--
        C--
                A--
        D--
```

U1
U2
  U5
  U6
    U3
    U4
  U7
  U8