

NetSpective Authentication Portal

Sign-In with Google and

Google Apps Directory Synchronization



Copyright © 2024 by Grom Educational Services, Inc. All rights reserved

Although the author and publisher have made every effort to ensure that the information in this document was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Printed in the United States of America

Grom Educational Services, Inc.
3280 Pointe Parkway, Suite 2500
Peachtree Corners, Georgia 30092
www.gromedu.com

© 2024 Google Inc., used with permission. Google and the Google logo are registered trademarks of Google Inc.

Table of Contents

Overview	4
Prerequisites	4
Sign-In with Google Integration	5
Sign out from Google Authentication	6
Sign-In with Google and traditional LDAP Directory sources	7
Google Apps Directory Integration	8
Sign-In with Google Authentication Sequence	10

Overview

Enabling Sign-In with Google will allow NetSpective's Authentication Portal to act like a Google enabled website. Once the user authorizes NetSpective to see their Google identity, they can log into the portal and gain Internet access with a single button press.

Enabling Google Apps Directory Synchronization will allow assignment of Google Apps groups and organizational units to NetSpective groups.

Prerequisites

There are several steps that should be performed prior to integration with Google. Please review the following:

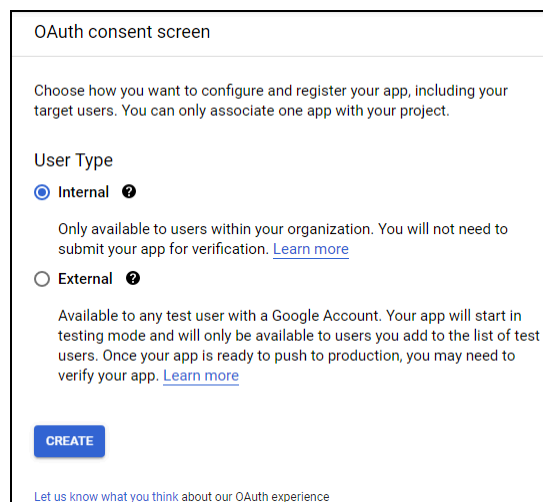
1. Assign a hostname to NetSpective in your DNS servers, e.g., webfilter.example.com. Google requires a valid Internet hostname so don't use .local domains.
2. Verify your firewall rules permit NetSpective to have HTTP, HTTPS, and NTP protocol access to the public Internet.
3. Verify that NetSpective has the correct time. In the Device Settings —> Advanced —> System Time section, set the local time zone, and then press *Test NTP Server* to assure your appliance has connectivity to a timeserver. A valid test will display "NTP Server Test OK". If you do not receive this message, consider changing the server IP address to a local NTP server or check your firewall rules.
4. Ensure that NetSpective has valid DNS server settings in Device Settings —> Network DNS server section.
5. Google's consoles work best with the Chrome web browser. You may download and install the Chrome web browser from <https://www.google.com/chrome/browser/desktop/index.html>.
6. Ensure that you have access to Google Apps Admin at <https://admin.google.com/> and the Google Cloud Platform at <https://console.cloud.google.com/>.

Sign-In with Google Integration

Enabling Sign-In with Google will configure NetSpective's Authentication Portal to behave like a Google enabled website. Once the user authorizes the NetSpective to see their Google identity, they can log into the portal and gain Internet access with a single button press. It will be necessary to use the Google Developers Console to create a project and a client ID that will be used to authenticate users.

Note: Google changes the Cloud Platform frequently; these steps may vary.

1. Using the Google Chrome web browser, log into the Google Developers console at <https://console.developers.google.com>.
2. Create a project associated with NetSpective. Click Select a project —> New Project... and provide a name.
3. Once in the project, under APIs & Services, click "OAuth consent screen". Create a new Internal consent screen.



The screenshot shows the 'OAuth consent screen' configuration page. At the top, it says 'OAuth consent screen'. Below that, a message states: 'Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.' Under the heading 'User Type', there are two radio button options. The first is 'Internal', which is selected and has a help icon. Its description is: 'Only available to users within your organization. You will not need to submit your app for verification. [Learn more](#)'. The second option is 'External', also with a help icon. Its description is: 'Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more](#)'. At the bottom left is a blue 'CREATE' button. At the bottom right is a link: 'Let us know what you think about our OAuth experience'.

- a. Set the App name that your users will recognize, e.g., “WebFilter at example.com”. This name will appear to users when they are asked to authorize NetSpective to see their identity. You are also required to provide a “User support email” and a Developer contact Email address. Once these three fields are filled out, click “Save and Continue” until you are brought back to the Dashboard.

Edit app registration

1 OAuth consent screen

2 Scopes

3 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *

Webfilter

The name of the app asking for consent

User support email *

webfilter@example.com

For users to contact you with questions about their consent

App logo

BROWSE

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

Authorized domains 2

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

+ ADD DOMAIN

Developer contact information

Email addresses *

helpdesk@example.com

These email addresses are for Google to notify you about any changes to your project.

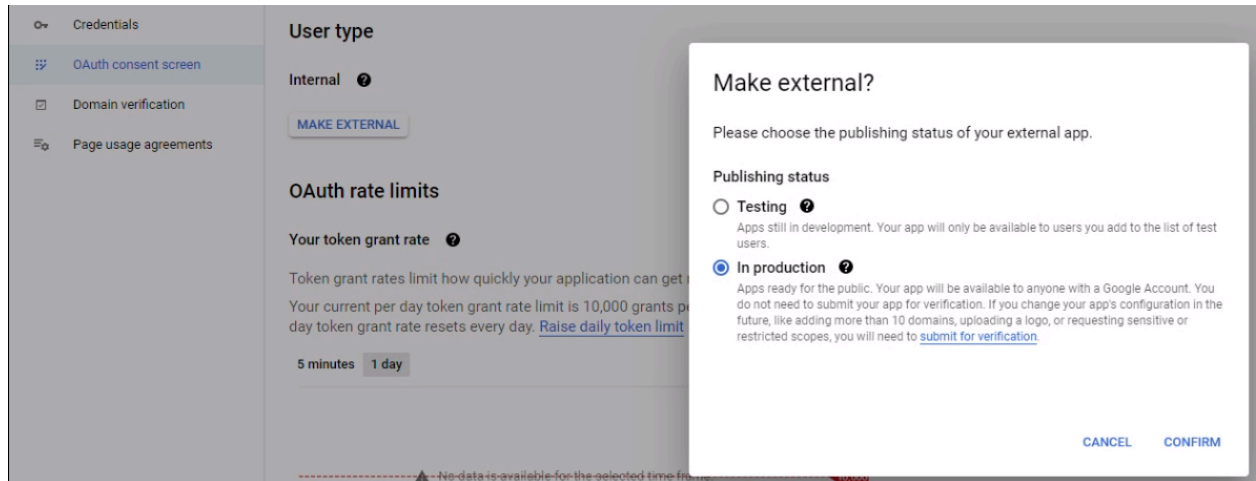
SAVE AND CONTINUE

CANCEL

b.

6

- c. Under your new “OAuth consent screen” under “User type” select the button “Make External”. On the next window, choose “In Production” so all users can use the consent screen. This is important if you want to limit users to only sign in using your domain, and not personal Google accounts.
- d. When you are finished, click Confirm.

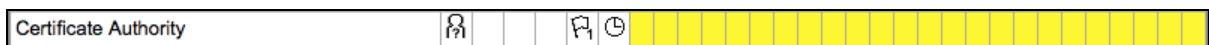


4. Under APIs & Services—> Credentials —> Create Credentials —> OAuth client ID.
5. You will be presented with a web form.
 - a. Select Web application from the drop down list.
 - b. Provide a name e.g. WebFilter at Example.
 - c. Authorized JavaScript origins should be the hostname you gave the appliance in the Prerequisites section e.g. <https://webfilter.example.com/>.
 - d. Authorized redirect URIs should be the hostname followed by /access/oauth2/callback e.g. <https://webfilter.example.com/access/oauth2/callback>.
 - e. Press the Create button.

6. Locate the newly created OAuth 2.0 client ID, and then press the download icon to save the client_secrets.json file.

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID				
<input type="checkbox"/>	WebFilter at Example	Jun 8, 2021	Web application	690768590874-vgpn...				

7. In NetSpective, select Authentication —> Google Sign-in—> Client Settings section, press the Upload button to upload the client_secrets.json to the appliance. When complete, the page will update with the Google client ID and appliance URLs.
8. You may want to limit which user domains are permitted to log into the appliance; Edit the list of Allowed Domains. If the allowed domains list is empty, it will accept all valid Google domains including gmail.com.
9. To enable Sign-In with Google on the authentication portal, select Authentication —> Authentication Rules, locate and click the Authentication Rule you wish to modify, and then add Google to Authentication Methods. Press the Save button.



There are several websites users should access without authentication to validate SSL certificates and allow Sign-In with Google to work properly. These websites were added to the Certificate Authority category. **NetSpective's Public Group Policy should permit unauthenticated access to the Certificate Authority category without SSL interception.**

Verify by selecting Management —> Groups—> Public —>. The Certificate Authority category should be permitted and the person icon indicates that unauthenticated access is allowed.

Test the Authentication Portal. Verify that the Sign-In with Google icon appears at the login screen and that Sign-In with Google works in NetSpective. Verify that your user ID appears in NetSpective's Users —> Currently Logged On group. If Sign-In with Google works properly but your email address isn't in NetSpective's directory, you will be signed in with an email address.

Sign out from Google Authentication

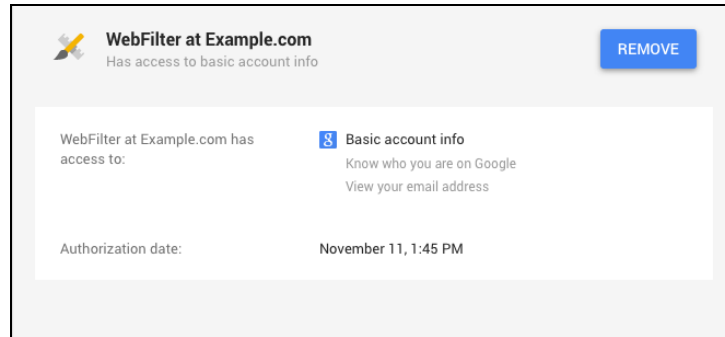
When a user authorizes NetSpective to see their identity, it updates their Google account so any device (including phones, tablets, Chromebooks, and laptops) logged into Google will also *Sign-In with Google* at NetSpective. **Users should use Sign-In with Google from the devices they own; however, this may not happen in practice, inform your users to logout of Google at public workstations.** Since there are times that logging out of NetSpective is necessary, you may want to make the following logout URLs available to your users via an internal website or browser bookmarks.

A user could choose to logout NetSpective's Authentication Portal and maintain connection with Google by visiting the following logout page e.g. <https://webfilter.example.com/access/logout>. This URL can be customized to redirect the user to a website upon successful logout by adding a CGI parameter e.g. https://webfilter.example.com/access/logout?u=http://target_website.com.

A user could deauthorize NetSpective from their Google account via one of two methods:

By visiting the appliance OAuth2 logout page e.g. <https://webfilter.example.com/access/oauth2/logout>. This URL can be customized to redirect the user to a website on successful logout by adding a CGI parameter e.g. https://webfilter.example.com/access/oauth2/logout?u=http://target_website.com.

By visiting <https://myaccount.google.com/security> —> Connected apps & sites —> Apps connected to your Account —> Manage Apps. Once they find NetSpective's web app, they can click to expand the option and then press the Remove button.



Sign-In with Google and traditional LDAP Directory sources

An LDAP Directory source may be Microsoft Active Directory, Apple's Open Directory, or Novell's eDirectory. These directories may have an email address for each user in the domain.

When NetSpective performs LDAP directory synchronization, it retrieves the email addresses of users for storage in NetSpective's directory. When the user signs in with Google, NetSpective will receive the email address of the user and then check the email address against the LDAP Directory user ID. If a user is found, it will authenticate the user using their LDAP directory user ID. For example, if you were using Active Directory and [username@example.com](#) signed in with Google the user will appear in Management —> Currently Logged On Users group as EXAMPLE\username.

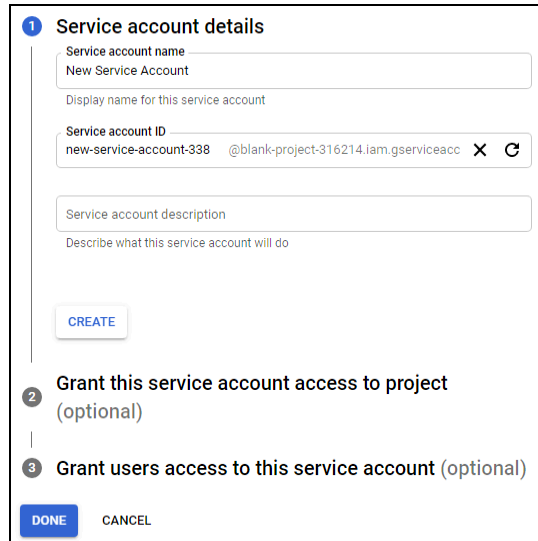
If you are already using an LDAP Directory source, Google Apps Directory Integration may not be needed.

Google Apps Directory Integration

NetSpective will query users with group and organizational unit assignments from the Google Apps Directory. Use the Google Developers Console to enable the Admin SDK, create a Google Apps service account client ID, and assign privileges to the account. The service account will be used to query the Google Apps Directory.

Note: You should only use Google Apps Directory Integration if you have users that are not in another directory source like Active Directory, Open Directory, or eDirectory.

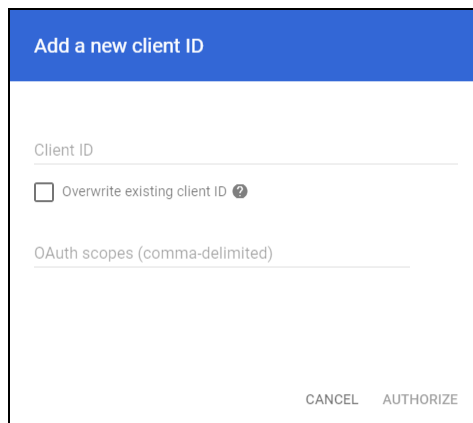
1. Using the Google Chrome web browser, log into Google Developers console at <https://console.cloud.google.com/>.
2. Select a project associated with NetSpective.
3. At the Project Dashboard, click Enable APIs, and then search for Admin SDK API. Once found, click Admin SDK API. In the following screen, press the Enable API button.
4. The Admin SDK is limited by free quota to 150,000 queries per day. NetSpective's API usage can be examined at the project's Usage and Quota tabs.
5. Select Credentials from the left sidebar, press the Create Credentials button and then select Service Account.



The screenshot shows the 'Service account details' form in the Google Developers Console. It includes fields for 'Service account name' (with a suggestion 'New Service Account'), 'Display name for this service account', 'Service account ID' (showing 'new-service-account-338' and '@blank-project-316214.iam.gserviceacc'), and 'Service account description'. A 'CREATE' button is visible. Below the form, there are two optional steps: 'Grant this service account access to project (optional)' and 'Grant users access to this service account (optional)'. At the bottom, there are 'DONE' and 'CANCEL' buttons.

6. You will be presented with a web form. Enter a name for the service account and click Create. For step 2, select Service Account Token Creator. Step 3 is also optional, so click Done.
 - a. From the Credentials screen, click to edit the Service Account you just created. From the top heading select Keys, and then "Add Key" and Create New Key. Select the JSON radio button and then press the Create button. The new service account key will be created and a service account JSON file will be downloaded. Verify that the service account JSON file is in your browser's downloads folder since it will be imported into NetSpective.

- b. While still editing the Service Account, click Details. Click Show Domain-wide Delegation, enable it, and then press Save. The Client ID at the bottom will be needed later, so copy and paste the new Client ID to a text file. This Client ID will be used to set permissions on the account.
7. Using the Google Chrome web browser, log into Google Apps Admin console at <http://admin.google.com/>. Click the Security icon. Click the API Controls section and ensure “trust internal, domain-owned apps” is checked.
8. Click Manage Domain Wide Delegation to reveal the API Clients section. Click the Add New button at the top.



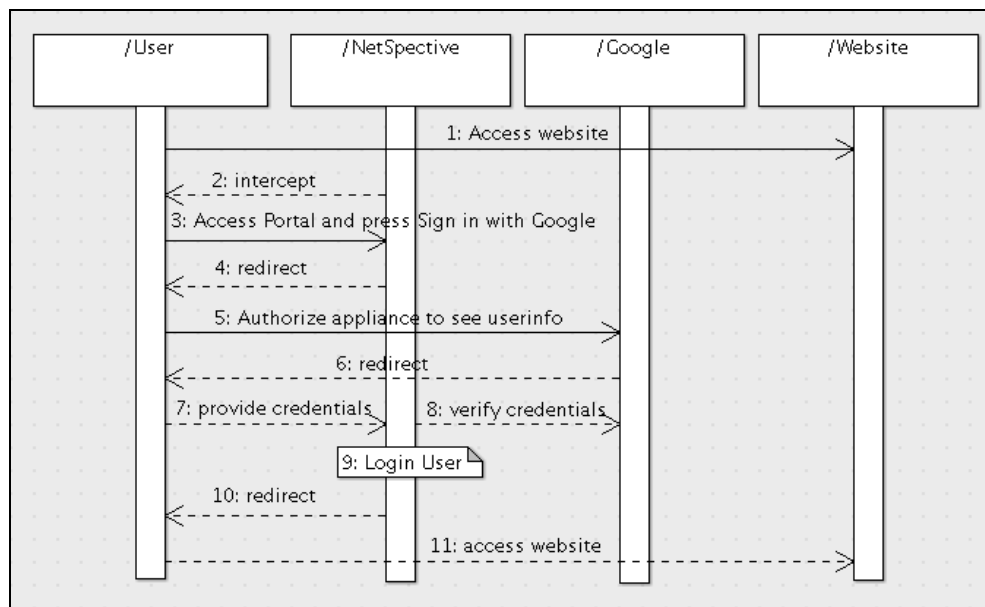
9. Paste the service account client ID obtained in step 5 into the Client ID field.
10. Cut and Paste the following URL list as one entry separated by commas into the OAuth scopes field:


```
https://www.googleapis.com/auth/admin.directory.group.readonly,  
https://www.googleapis.com/auth/admin.directory.orgunit.readonly,  
https://www.googleapis.com/auth/admin.directory.user.readonly
```
11. Press the Authorize button.
12. Log into NetSpective, access Authentication —> Directory Sources page, press Add to create a new Directory source.
13. Provide a name for the new directory source.
14. Select Source Type to Google Directory. The webpage will change to reveal the Google Apps fields.
15. Enter your Google Apps domain name.
16. Enter your Google Apps administrator’s email address.
17. Press select and then choose the service_account.json file obtained in step 4.

18. Press the Save icon to finish the operation.
19. NetSpective will automatically pull the latest directory from Google. Wait a few moments for the operation to complete. Refresh the Directory Sources page to verify the status of all the directory sources are OK.
20. In NetSpective's Management ▢ Group Settings, associate a NetSpective group with Google Apps group or organizational unit.

Sign-In with Google Authentication Sequence

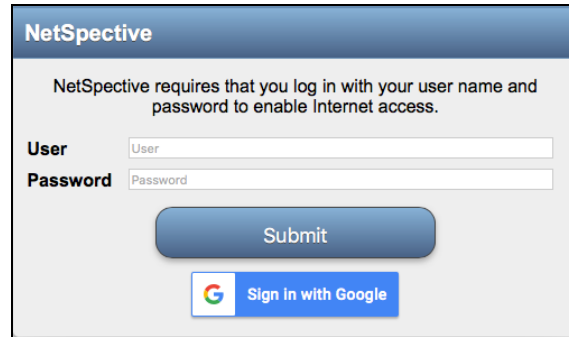
This reference section explains how NetSpective implements Sign-In with Google. It illustrates that an unauthenticated user and NetSpective requires access to Google's authentication servers.



Note: The steps illustrated with dashed lines are performed automatically.

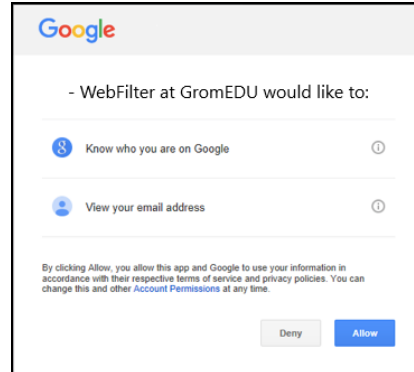
1. An unauthenticated user attempts to access an Internet website.
2. NetSpective will recognize the user is unauthenticated and redirect the user to the Authentication Portal.

3. At the Authentication Portal, the user is prompted to type in their credentials or Sign-In with Google.



The image shows a web form titled "NetSpective". Below the title, a message states: "NetSpective requires that you log in with your user name and password to enable Internet access." There are two input fields: "User" and "Password". Below these fields is a blue "Submit" button. At the bottom of the form is a "Sign In with Google" button, which includes the Google logo.

4. If the user presses the Sign-In with Google button, they will be redirected to Google for authentication credentials.
5. If the user is not logged into Google, they will be prompted to log into Google. If the user has not authorized the appliance to see their Google identity, they will be prompted to authorize.



The image shows a Google authorization screen. At the top is the Google logo. Below it, the text reads: "- WebFilter at GromEDU would like to:". There are two permission items listed: "Know who you are on Google" and "View your email address", each with a blue icon and an information icon. At the bottom, there is a paragraph of text: "By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time." Below this text are two buttons: "Deny" and "Allow".

6. If the user is logged into Google and the NetSpective was authorized, they automatically receive credentials via single sign on.
7. Google will redirect the user's web browser to the appliance with credentials.
8. The user's web browser will submit credentials to NetSpective.
9. NetSpective will validate the user's credentials. If the credentials are valid, NetSpective will fetch the user's Google Apps email address.
10. Authenticate the user in NetSpective.

11. After authentication, the user will be redirected to the destination website.
12. The user's browser will visit the destination website.