NetSpective Authentication Portal

Sign-In with Google and

Google Apps Directory Synchronization

TeleMate.Net®
SOFTWARE

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

TeleMate.Net Software
5555 Triangle Parkway, Suite 150
Norcross, Georgia 30092
http://www.telemate.net

Table of Contents

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. The 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 Developers Console at https://console.developers.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.

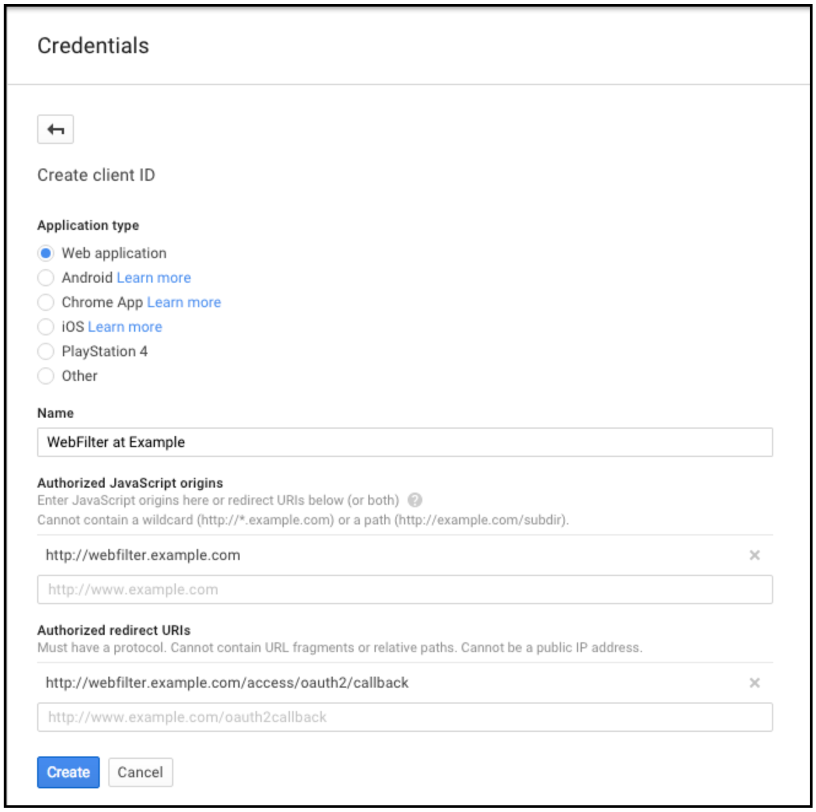
Note: Google changes the Developers Console frequently; these steps may vary.

1. Using the Google Chrome web browser, log into the Google Developers console at https://console.developers.google.com.

2. Create project associated with NetSpective. Click Select a project —> Create a Project… and provide a name.

3. Once in the project, select API Manger —> Credentials —> Add Credentials —> OAuth 2.0 client ID. If this is a new project, press the Configure consent screen button. Set the product 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.

4. You will be presented with a web form.



Credentials

Create client ID

Application type

● Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ PlayStation 4
○ Other

Name

WebFilter at Example

Authorized JavaScript origins

Enter JavaScript origins here or redirect URIs below (or both)

Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).

http://webfilter.example.com ×

http://www.example.com

Authorized redirect URIs

Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://webfilter.example.com/access/oauth2/callback ×

http://www.example.com/oauth2callback

   a. Select Web application radio button.
   b. Provide a name e.g. WebFilter at Example.
   c. Authorized JavaScript origins should be the hostname you gave the appliance in Prerequisites section e.g. http://webfilter.example.com/.
   d. Authorized redirect URIs should the hostname followed by /access/oauth2/callback e.g. http://webfilter.example.com/access/oauth2/callback.
   e. Press the Create button.

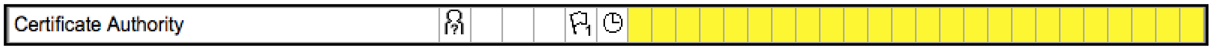
5. Locate the newly created OAuth 2.0 client ID, and then press the download icon to save the client_secrets.json file.

6. 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.

   You may want 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.

7. 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.

8. 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 the Certificate Authority category. **NetSpective's Public Group Policy should permit unauthenticated access to the Certificate Authority category without SSL interception.**



Certificate Authority

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

9. 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

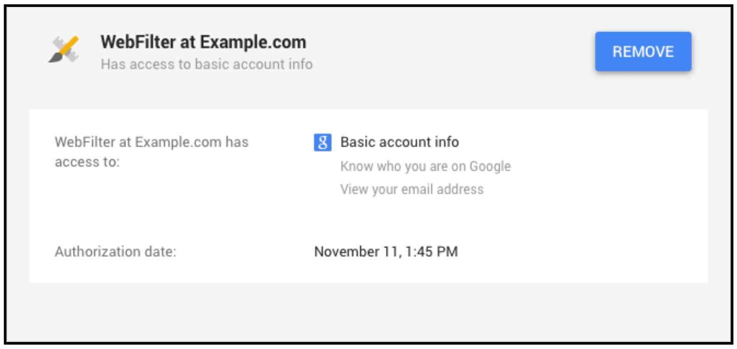
When a user authorizes NetSpective to see their identity, it updates their Google account so any device (including phones, tablets, Chromebooks, and laptops) logged into Google will also *Sign-In with Google* at NetSpective. **Users should use Sign-In with Google from the devices they own; however, this 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. http://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. http://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 oath2 logout page e.g. http://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. http://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.



WebFilter at Example.com
Has access to basic account info

WebFilter at Example.com has access to: Basic account info
Know who you are on Google
View your email address

Authorization date: November 11, 1:45 PM

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.

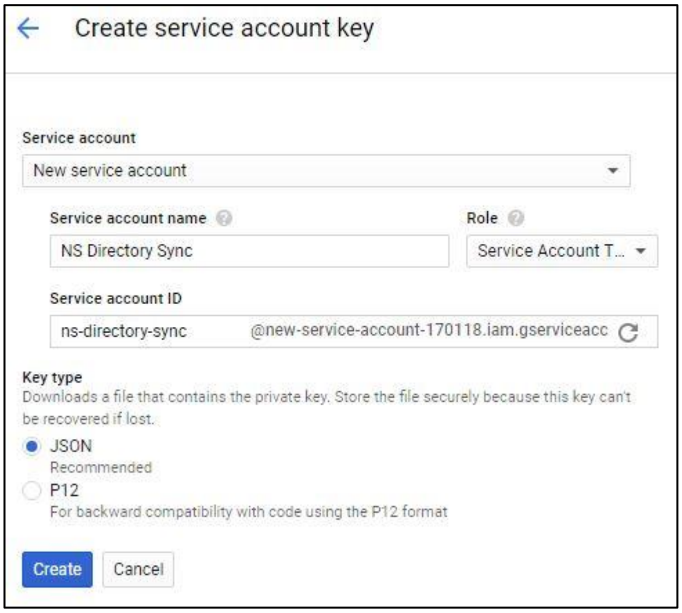
1. Using the Google Chrome web browser, log into Google Developers console at https://console.developers.google.com.

2. Select a project associated with NetSpective.

3. At the Project Dashboard, click Enable APIs, and then search for Admin SDK. Once found, click Admin SDK. In the following screen, press the Enable API button.

   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.

4. Select Credentials from the left sidebar, press the Create Credentials button and then select Service Account Key.



← Create service account key

Service account: New service account

Service account name: NS Directory Sync

Role: Service Account T...

Service account ID: ns-directory-sync @new-service-account-170118.iam.gserviceacc

Key type

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

● JSON
Recommended

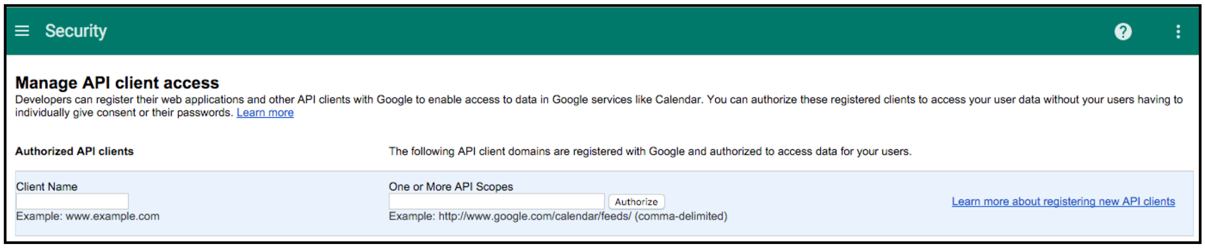
○ P12
For backward compatibility with code using the P12 format

You will be presented with a web form. Select New Service Account and then provide a name for the service account. For the Role field, select Service Account Token Creator. 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.

5. From the Credentials section, click the link to Manage service accounts. At the end of the row with the new service account key, click the menu icon, and then choose Edit. Click to Enable G Suite Apps Domain-wide Delegation, name it, and then press Save. Click View Client ID and then copy and paste the new Client ID to a text file. This Client ID will be used to set permissions on the account.

6. Using the Google Chrome web browser, log into Google Apps Admin console at http://admin.google.com/. Click the Security icon. Click the API reference section and then check the option to Enable API access.

7. Click the Show more section to reveal the Advanced Settings menu option. Click the Advanced Settings option and then Manage API client access. In Manage API client access, authorize the service account to have read only access to your Google Apps directory.



Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

Authorized API clients — The following API client domains are registered with Google and authorized to access data for your users.

Client Name
Example: www.example.com

One or More API Scopes
Example: http://www.google.com/calendar/feeds/ (comma-delimited)

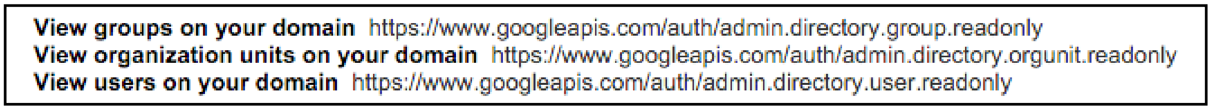
   a. Paste the service account client ID obtained in step 5 into the Client Name field.

   b. Cut and Paste the following URL list as one entry separated by commas into the API 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

   c. Press the Authorize button.

8. To verify that authorization was successful, you will see a message stating that your service account



View groups on your domain https://www.googleapis.com/auth/admin.directory.group.readonly
View organization units on your domain https://www.googleapis.com/auth/admin.directory.orgunit.readonly
View users on your domain https://www.googleapis.com/auth/admin.directory.user.readonly

has permissions to access to view users, groups, and organizational units on domain.

9. Log into NetSpective, access Authentication —> Directory Sources page, press Add to create a new Directory source.

   a. Provide a name for the new directory source.

b. Select Source Type to Google Directory. The webpage will should change to reveal the Google Apps fields.

c. Enter your Google Apps domain name.

d. Enter your Google Apps administrator's email address.

e. Press select and then choose the service_account.json file obtained in step 4.

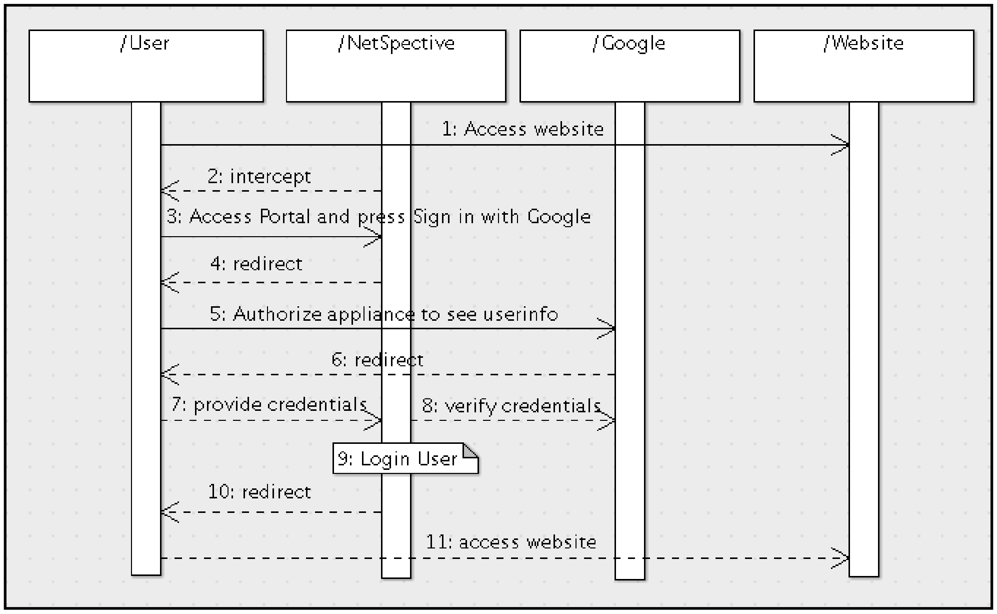
f. Press the Save icon to finish the operation.

g. 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 the all directory sources are OK.

10. 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.

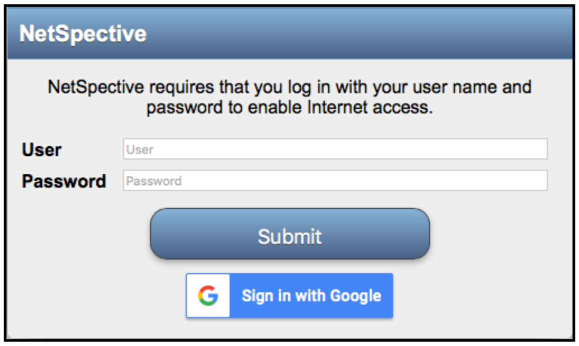


1. An unauthenticated user attempts to access an Internet website.

2. NetSpective will recognize the user is unauthenticated and redirect the user to the Authentication Portal.

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

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



NetSpective

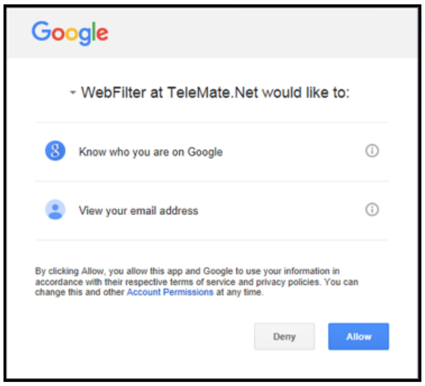
NetSpective requires that you log in with your user name and password to enable Internet access.

User User

Password Password

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.



Google

WebFilter at TeleMate.Net would like to:

Know who you are on Google

View your email address

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.

If the user is logged into Google and appliance was authorized, they automatically receive credentials via single sign on.

6. Google will redirect the user's web browser to the appliance with credentials.

7. The user's web browser will submit credentials to NetSpective.

8. NetSpective will validate the user's credentials. If the credentials are valid, NetSpective will fetch the user's Google Apps email address.

9. Authenticate the user in NetSpective.

10. After authentication, the user will be redirected to the destination website.

11. The user's browser will visit the destination website.