PingFederate®

Google Cloud Identity Connector

Version 1.1

User Guide

PingFederate Google Cloud Identity Connector *User Guide*
Version 1.1
April, 2016

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909
Web Site: www.pingidentity.com

Trademarks

Disclaimer

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **April 6, 2016**

Contents

Introduction

The PingFederate Google Cloud Identity Connector (Google CIC) allows a Service Provider (SP) to leverage Google as an Identity Provider (IdP) for access to Internet applications in the SP domain. The Google CIC uses the Google+ API, which leverages the OpenID Connect standard to authenticate users and optionally return information about that user to the SP. The Google CIC can also optionally be configured to provide the SP with information about the user using the Google Directory API.

Using the Google CIC, a Software-as-a-service (SaaS) provider, for example, can provide customers direct SSO access to its applications. In addition, an SP may leverage Google credentials for secure standards-based SSO to services in other local domains or at partner sites by using the Adapter in an SP partner connection. (For more information about identity-federation standards and partner connections, see Key Concepts in the PingFederate *Administrator's Manual*.)

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of IT infrastructure. Knowledge of networking and user-management configuration is assumed. Some exposure to the PingFederate administrative console may be helpful.

> **Note:** If you encounter any difficulties with configuration or use of the Google CIC, please try reaching the Ping Identity Support Center (`ping.force.com/Support`).

ZIP Manifest

The distribution ZIP file for the Google CIC contains the following:

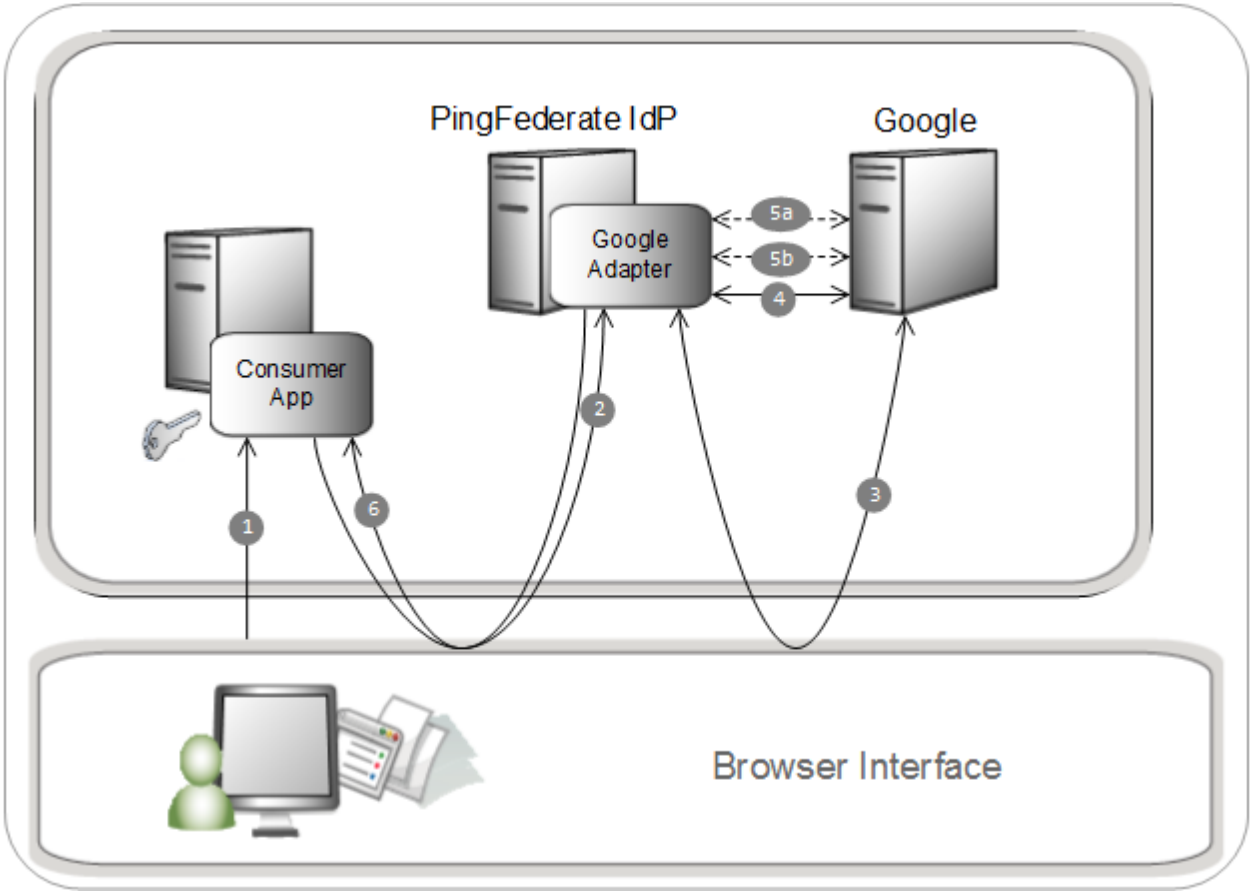
- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains the legal information:
  - `Legal.pdf` – copyright and license information
- `/dist` – contains libraries needed to run the Google CIC:
  - `pf-google-adapter-1.1.jar` – Google CIC adapter
  - `pf-google-cic-oauth-helper.war` – The OAuth Helper Web-app

System Requirements

The Google CIC requires installation of PingFederate 7.0.1 or higher.

Processing Overview

The following figure illustrates an example SSO process flow using the Google CIC:



Processing Steps

1. User navigates to a Web application and chooses to log on using Google.
2. The browser is redirected to the Google CIC.
3. The PingFederate server redirects the user to Google for authentication. A list of requested permissions is provided in this call.

   If the user is not already logged on, Google challenges the user to authenticate. Google authenticates the user and provides a consent page for the user to authorize the sharing of information from their Google profile. Once the user authorizes, Google redirects the browser to the `/ext/google-authn` endpoint with an authorization code.

   If the user does not authenticate, an error is returned rather than an authorization code.
4. The Google CIC makes an HTTP request to Google to obtain an OAuth 2.0 access token, sending the Client ID, Client Secret and authorization code as parameters. Google validates these components and returns an access token and an ID token (which contains the user's email).
5. (a) When the Google CIC is configured to retrieve Basic Profile attributes, the adapter uses the Google+ API to retrieve the user's profile in OpenID Connect format using the access token granted in step 4.

   (b) When the Google CIC is configured to retrieve Extended Profile attributes, the adapter uses the refresh token that was configured when creating the Adapter to retrieve a new access token. This access token is used to retrieve the user's profile from Google's Admin SDK Directory API.

6. The Google CIC redirects the user back to the Web application with the user attributes.

   For the list of attributes that are returned, see the Exposed User Attributes section of this User Guide.

Note: There are two ways for a PingFederate administrator to set up this process, depending on whether the service is part of the enterprise domain or outside that domain.

For information on ways to complete the configuration for services inside or outside of your domain, see the Complete the Configuration section of this User Guide.

Installation and Configuration

The following section describes how to install and configure the Google CIC with your application.

Install the Google Cloud Identity Connector

To Install the Google Cloud Identity Connector:

1. Stop the PingFederate server if it is running.
2. Remove any existing Google CIC files from the directory:

   `<PF_install>\pingfederate\server\default\deploy`

3. Unzip the distribution file and copy the contents of the `/dist` directory to the PingFederate directory:

   `<PF_install>\pingfederate\server\default\deploy`

4. Start or restart the PingFederate server.

Configure the Google Cloud Identity Connector Adapter

To configure the Google Cloud Identity Connector in PingFederate, follow the instructions in each of the following sections in order.

To configure the IdP Adapter:

1. If you have not already done so, ensure that you have your Google Application's Client ID and Client Secret available to complete the Adapter configuration.

   For information on obtaining your Client ID and Secret, see the Obtaining Client ID and Secret section of this User Guide.

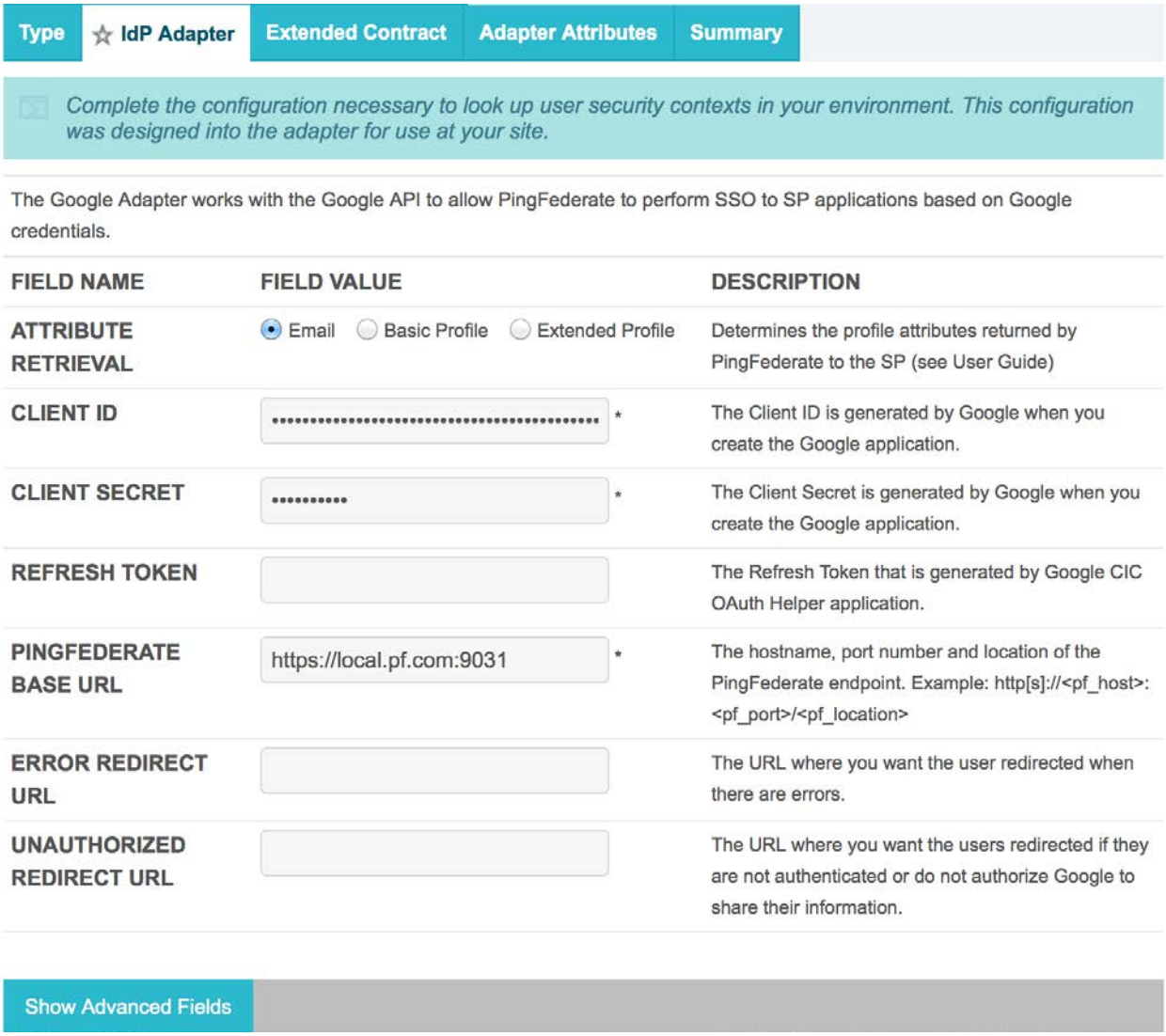
2. If you plan to set **Extended Profile** as your Attribute Retrieval selection, and have not already done so, ensure that you have an authorized OAuth 2.0 refresh token available to complete the Adapter configuration.

   For information on obtaining an authorized OAuth 2.0 refresh token, see the Generate Authorized OAuth 2.0 Token section of this User Guide.

3. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.

4. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
5. On the **Type** screen, enter an Instance Name and Instance ID.

   The Name is any you choose for identifying the Adapter Instance. The ID is used internally and may not contain spaces or non-alpha-numeric characters.
6. Select Google CIC Adapter 1.1 from the Type list and click **Next**.



7. On the IdP Adapter screen, provide entries for each of the fields shown, as indicated in the table below:

Field	Description

Field	Description
Attribute Retrieval	Determines the profile attributes returned by PingFederate to the SP once a user authenticates using the Google CIC. Email – Returns the user's email and identifier (default). Basic Profile – Returns the user's full profile using Google's people.getOpenIdConnect endpoint. Extended Profile – Returns the user's full profile using Google's Admin SDK – Directory API. **Note:** Extended Profile can only be used for user's authenticating from the same Google Apps domain that the Refresh Token was authorized for. For the list of attributes that are returned for each of these settings, see the Exposed User Attributes section of this User Guide.
Client ID	The Client ID is generated by a Google admin in the Google Developer Console. For more information on Client ID, see the Obtaining Client ID and Secret section of this User Guide.
Client Secret	The Client Secret is generated by a Google admin in the Google Developer Console. For more information on Client Secret, see the Obtaining Client ID and Secret section of this User Guide.
Refresh Token	This is required when Attribute Retrieval is configured for Extended Profile. For more information on obtaining the refresh token, see the Generate Authorized OAuth 2.0 Token section of this User Guide.
PingFederate Base URL	The fully qualified hostname, port and path for the PingFederate endpoint. Example: `http[s]:<pf_host>:<pf_port>`
Error Redirect URL	If specified, the user will be redirected to this URL if errors occur. If left blank, users will be redirected to Google's default error URL instead.
Unauthorized Redirect URL	If specified, the user will be redirected to this URL if errors occur. If left blank, users will be redirected to Google's default error URL instead.

8. (Optional) Click **Show Advanced Fields** to view additional configuration settings.

The default values for these fields may be modified if necessary:

Field	Description
Authentication URL	The endpoint Google has designated for user authentication. If Google has altered this endpoint, modify it accordingly. Default value: `https://accounts.google.com/o/oauth2/auth`
Access Token URL	The endpoint Google has designated for retrieving an OAuth Access Token. If Google has altered this endpoint, modify it accordingly. Default value: `https://accounts.google.com/o/oauth2/token`

Field	Description
Logout URL	The URL used by Google to log users out. Default value: `https://accounts.google.com/Logout?hl=en`
Basic Profile Data URL	The OpenID Connect endpoint for retrieving user data when Basic Profile attributes is selected. Default value: `https://www.googleapis.com/plus/v1/people/me/openIdConnect`
Extended Profile Data URL	The Google Directory API endpoint for retrieving user data when Extended Profile is selected. Default value: `https://www.googleapis.com/admin/directory/v1/users`
Certificate URL	The URL used to retrieve Google's current certificate, which is used by Google to sign the Id Token. Default value: `https://www.googleapis.com/oauth2/v3/certs`
Require Form Adapter Cancellation	This feature is for customers who've modified the HTML Form Adapter to provide a custom adapter flow.

9. Click **Next**.
10. (Optional) On the Extended Contract screen, extend the contract as necessary for your implementation.

    Important: By default, the Adapter's Core Contract returns the user's email. To return additional user attributes, you must extend the Adapter's Contract.

    For the full list of available user attributes, see the Exposed User Attributes section of this User Guide.

    For information on using the Extended Contract screen, see Extending an Adapter Contract in the PingFederate *Administrator's Manual*, or click **Help** on the screen.
11. Click **Next**.
12. On the Adapter Attributes screen, select a Pseudonym.

    Tip: Pseudonyms are opaque subject identifiers used for SAML account linking and are not generally applicable in the context of cloud-identity deployments. To ensure correct PingFederate performance under all circumstances however, a selection is required.

    For information on account linking, see Account Linking in the PingFederate *Administrator's Manual*, or click **Help** on the screen.
13. Click **Next**.
14. On the Summary screen, verify that the information is correct and click **Done**.
15. On the Manage IdP Adapter Instances screen, click **Save**.

Complete the Configuration

To complete the SSO setup in PingFederate:

- For SSO to an application at your site in the domain covered by PingFederate, a standard SAML connection is not necessary; instead you can use direct IdP-to-SP adapter mapping.

  For instructions on configuring an IdP-to-SP adapter mapping, see the Configure SSO to an Enterprise Service Application section of this User Guide.

- For SSO to an external SP partner (or any service outside the domain covered by PingFederate), configure an SP connection.

  For instructions on configuring an SP connection, see the Configure SSO to an SP Partner section of this User Guide.

Configure SSO to an Enterprise Service Application

1. On the Main Menu, click **Server Settings**.
2. On the Roles and Protocols screen in the Server Settings configuration, ensure that both the IdP and SP roles are enabled.

   Note: The choice of protocol is not relevant for either role to implement the Google Cloud Identity Connector for in-domain SSO, but a selection is required to enable a role.

3. Click **Save**.
4. Configure an SP Adapter Instance, if one is not already configured or you want to use a new one:
   a. Click **Adapters** under SP Configuration on the Main Menu.
   b. Configure a new Adapter; using any adapter type, such as the OpenToken Adapter (bundled with PingFederate).

   For a list of other available Ping Identity integration kits and product documentation on how to use them, see the Ping Identity Web site (`www.pingidentity.com/support-and-downloads`).
5. On the Main Manu, click **System Settings**.
6. On the **IdP-to-SP Adapter Mapping** screen in the Server Settings configuration, follow the screen flow to complete the IdP-to-SP adapter mapping:
   a. Select the Google Cloud Identity Connector that you configured earlier as the Source instance and any SP Adapter Instance as the Target

      For information on adapter-to-adapter mapping, see IdP-to-SP Adapter Mapping in the PingFederate *Administrator's Manual*, or click **Help** on the screen.

Configure SSO to an SP Partner

Use the Google Cloud Identity Connector IdP Adapter Instance you configured earlier in an SP Connection.

Tip: You select the Adapter Instance for the IdP Adapter Mapping setup under Assertion Creation.

For information on managing SP connections, see Managing SP Connections in the PingFederate *Administrator's Manual*, or click **Help** on any IdP Adapter Mapping screens for context-sensitive help.

Application Integration

For users to authenticate via the Google Cloud Identity Connector, administrators must provide a specific PingFederate URL:

For IdP-to-SP Adapter Mapping Configurations:

Use the following URL in a hyperlink on your web-application logon page to start SSO:

```
https://<pf_host>:<pf_port>/pf/adapter2adapter.ping?IdpAdapterId=<adapterId
>
```

where:

- `<pf_host>` is the host name or IP address where PingFederate is running.
- `<pf_port>` is the port number for PingFederate.
- `<adapterId>` is the Instance ID defined in the Google CIC IdP Adapter you configured earlier.

For SP Connection Configurations:

Use the following URL in your web-application for SSO to the target application:

```
https://<pf_host>:<pf_port>/idp/ startSSO.ping?PartnerSpId=<connectionId>&
IdpAdapterId=<IdPAdapterId>
```

Where:

- `<pf_host>` is the host name or IP address where PingFederate is running.
- `<pf_port>` is the port number for PingFederate.
- `<connectionId>` is the SP-connection identifier for the SP connection you configured earlier using the Google CIC Adapter instance.
- `<IdPAdapterId>` is the applicable Instance ID for the Google CIC Adapter used in the SP connection.

Exposed User Attributes

When a user is redirected to the Web application after authenticating with the Google CIC, the following user attributes are returned with them based on the Adapter's Extended Contract:

> **Note:** The Adapter's Extended Contract must be configured using the desired user attribute names exactly as they appear in the tables below.

Regardless of the Attribute Retrieval's selection, the email attribute is always available:

Attribute Name	Description
`email`	The email address of the authenticated user. This value is retrieved from the ID token.

When Attribute Retrieval is set to Email the account identifier is also available:

Attribute Name	Description
sub	The ID of the authenticated user.

When Attribute Retrieval is set to Basic Profile the following attributes are available:

Attribute Name	Description
kind	Identifies this resource as a person in OpenID Connect format. Value: plus#personOpenIdConnect
username	The username.
gender	The person's gender. Possible values include, but are not limited to, the following values: male, female and other
sub	The ID of the authenticated user.
name	The full name.
given_name	The first name.
family_name	The last name.
profile	The URL of the user's profile page.
email_verified	Boolean flag, which is true if the email address is verified.
hd	The hosted domain name of the user's Google Apps account. Example: domain.com
locale	The user's preferred locale.

When Attribute Retrieval is set to Extended Profile the following attributes are available:

Attribute Name	Description
kind	Identifies this resource as a person in OpenID Connect format. Value: plus#personOpenIdConnect
username	The username.
id	The unique ID.
givenName	The first name.
familyName	The last name.
fullName	The full name.
externalIds	The raw JSON string.
primaryAddressFormatted	The full primary address.
primaryAddressStreet	The street of the primary address.
primaryAddressLocality	The city of the primary address.
primaryAddressRegion	The state/province of the primary address.
primaryAddressPostalCode	The zip/postal code of the primary address.
primaryAddressCountry	The country of the primary address.
primaryAddressCountryCode	The country code. Uses the ISO 3166-1 standard.
primaryOrgName	The name of the primary organization.
primaryOrgTitle	The user's title within the primary organization.
primaryOrgDepartment	The user's department within the primary organization.

Attribute Name	Description
primaryOrgLocation	The location of the primary organization.
primaryOrgDescription	The description of the primary organization.
manager	The user's direct manager, as defined by the Relations entity.
mobilePhone	The mobile phone.
workPhone	The work phone.
orgUnitPath	The full path of the parent organization associated with the user. If the parent organization is the top-level, it is represented as a forward slash (/).
thumbnailPhotoUrl	Photo Url of the user (Read-only).

OpenID Attribute

To have the adapter expose the `openid_id` parameter, simply change the Authentication URL to:

```
https://accounts.google.com/o/oauth2/auth?openid.realm=https://<pf_host>:<pf_port>
```

The contract for the adapter and connection would have to be extended to support the `openid_id` parameter.

For information on Adapter Contracts, see Extending an Adapter Contract in the PingFederate *Administrator's Manual*, or click **Help** on the screen.

Generate Authorized OAuth 2.0 Token

The Google CIC can optionally be configured to provide the SP with Extended Profile attributes by using Google's Directory API. To use this feature, the Google CIC must be configured with an authorized OAuth 2.0 Refresh Token (RT). This token must be generated using the Client ID and Secret that the Google CIC is configured with.

> For more information on obtaining a Client ID and Secret, see the Obtaining Client ID and Secret section of this User Guide.

The Google CIC comes pre-packaged with a web-app to assist admins in obtaining an authorized OAuth 2.0 token. The use of this web-app to generate the OAuth 2.0 token is optional, and the steps to do so are outlined below.

> **Note:** The following steps assume you completed the optional steps for setting the Authorized Javascript Origins and Authorized Redirect URI in the Obtaining Client ID and Secret section of this User Guide.

To generate an Authorized OAuth 2.0 Token:

1. Install the Google CIC if it's not already installed.

   For information on installing the Google CIC, see the Install the Google Cloud Identity Connector section of this User Guide.

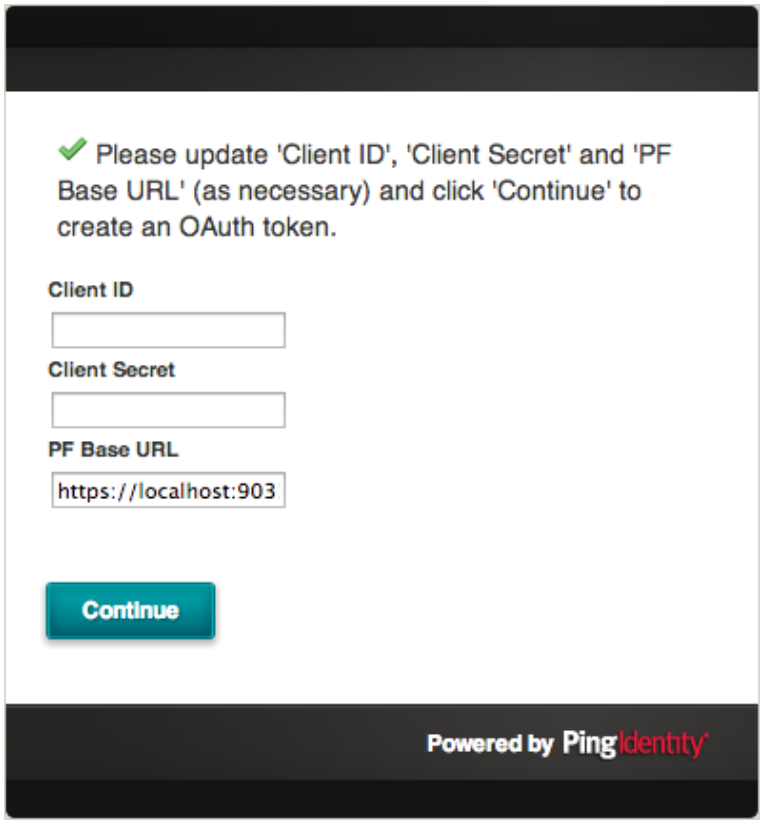
2. Start PingFederate if it's not already running.

3. Access the OAuth Helper Web-app:

   http[s]://<pf_host>:<pf_port>/pf-google-cic-oauth-helper

Note: The URL to access the OAuth Helper Web-app should match the value you used when setting the Authorized Redirect URI in the Obtaining Client ID and Secret section of this User Guide.

4. Enter the Client ID and Client Secret that you generated in the Obtaining Client ID and Secret section of this User Guide.



   Enter the PF Base URL:
   For example: `http[s]:<pf_host>:<pf_port>`

6. Click **Continue** to proceed. This generates an OAuth 2.0 authorization token and redirects you to Google for authorization.

7. Log on to Google with an administrative account.

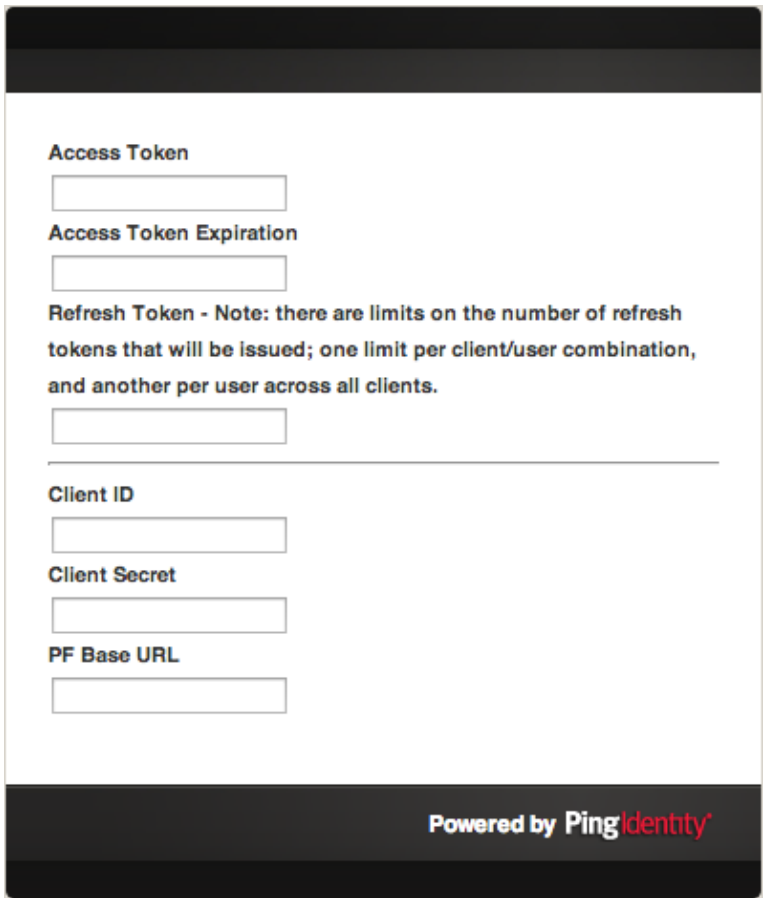
Note: If you already have an existing session with Google, this step is skipped.

8. On successful login, you are redirected to Google's OAuth authorization screen, where you'll be asked to grant access to the scopes that the Google CIC uses to make requests to the Google Directory API.

9. Once you grant acess on the OAuth authorization screen, you will be redirected to the OAuth Helper Web-app, and presented with an authorized Refresh Token to use when configuring the Google CIC.

Warning: Only one Refresh Token will be generated per Client ID; so it is important to make note of the Refresh Token presented by the OAuth Helper Web-app in the final step.

If another Refresh Token is required, you will need to obtain a new Client ID and Secret and to use with the OAuth Helper Web-app again.



Obtaining Client ID and Secret

The Google CIC makes use of the Google+ API to authenticate users and optionally, return Google profile information about the authenticating user to the SP using the OpenID Connect protocol. Alternatively, the Google CIC can be configured to retrieve the user's Google profile information using Google's Directory API, which requires the Google CIC to be configured with an OAuth 2.0 Refresh Token, authorized by an administrator of the user's Google domain.

Important: The Google CIC uses APIs provided by Google, which are subject to Google's Terms of Service described in their online documentation for the:

Google+ API here (`https://developers.google.com/+/terms`), which is only required when exposing Basic Profile attributes.

Admin SDK here (`https://developers.google.com/admin-sdk/terms`), which is only required when exposing Extended Profile attributes.

To obtain a Client ID and Secret:

Note: API Access will need to be enabled on the Google domain in order to use the Google CIC. For information on how to enable API Access for a Google domain, see Google's online documentation here (`https://support.google.com/a/answer/60757`).

1. Access the Google Developers Console (`https://console.developers.google.com`) as an adminstrative user.

   For information on the Google Developers Console, see Google's online documentation here (`https://developers.google.com/console/help/new/`).

   Note: To use the Developers Console, the Google App Engine Admin Console service will need to be enabled on your Google domain.

   For more information on enabling services for a Google domain, see Google's online documentation here (`https://support.google.com/a/answer/182442`).

2. (Optional) Create a new project.

   For information on creating projects in the Google Developers Console, see Google's online documentation here (`https://developers.google.com/console/help/new/#creatingdeletingprojects`).

3. Set the APIs for your project:

   Ensure the Google+ API is turned **ON** for your project if you wish to set the Attribute Retrieval option to Basic Profile.

   Ensure the Admin SDK is turned **ON** for your project if you wish to set the Attribute Retrieval option to Extended Profile.

   For information on activating APIs in the Google Developers Console, see Google's online documentation here (`https://developers.google.com/console/help/new/#activatingapis`).

4. (Optional) Configure the Concent Screen for your project.

   Tip: The Concent Screen is the screen users will see when authorizing the Google CIC to access their Google profile information. It is recommended that you set the Product Name and any other fields as required by your organization.

5. Generate Credentials for your project by doing the following:

   a. Create a new OAuth 2.0 Client ID for a Web Application type application.

   b. Set the Authorized Javascript Origins field to:

   `http[s]://<pf_host>:<pf_port>`

   c. Set the Authorized Redirect URI to:

   `http[s]://<pf_host>:<pf_port>/ext/google-authn`

   d. (Optional) Set a second URL in the Authorized Redirect URI field to where the OAuth Helper App can be accessed:

   `http[s]://<pf_host>:<pf_port>/pf-google-cic-oauth-helper`

Note: The above optional Authorized Redirect URI is only required when Configuring the Google CIC to expose the Extended Profile.

Note: The example urls above assume your PingFederate instance is publicly accessible.

Extended Development

Note: The Google Adapter provides no check to determine whether a requested field is available for the User API call. It is up to the SP to make this determination.

Note: Even though additional fields can be specified in the Google IdP configuration, there is no guarantee that Google will return those fields back to the Google adapter. Furthermore, when using Extended Profile (Google's Directory API) the externalIds attribute is returned as structured JSON attributes rather than single values. The returned JSON string attribute value will have to be parsed.

Upgrading from 1.0 to 1.1

Follow these steps to upgrade your existing Google CIC adapter from 1.0 to 1.1:

1. Stop PingFederate if it is running, remove the file pf-google-adapter-1.0.jar from <PF Install>/pingfederate/server/default/deploy and replace it with pf-google-adapter-1.1.jar.
2. Optionally, remove the following files, as long as they are not needed by any other installed adapters:
   a. httpcore-4.3.2.jar
   b. httpclient-4.3.x.jar
   c. json-simple-1.1.jar
3. Restart PingFederate.
4. In the PingFederate administration application, under IdP Configuration select Adapters.
5. Select the Google CIC instance name.
6. Select the IdP Adapter tab.
7. Click Advanced Settings.
8. Insert the following URL into the Certificate URL field:
   `https://www.googleapis.com/oauth2/v3/certs`
9. Click Done then Save to update the configuration.