Pulse Secure

Cloud Secure – Google

Configuration Guide

Document Revisions 3.0
Published Date December 2018

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

https://www.pulsesecure.net

Cloud Secure – Google Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.pulsesecure.net**.** By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Introduction

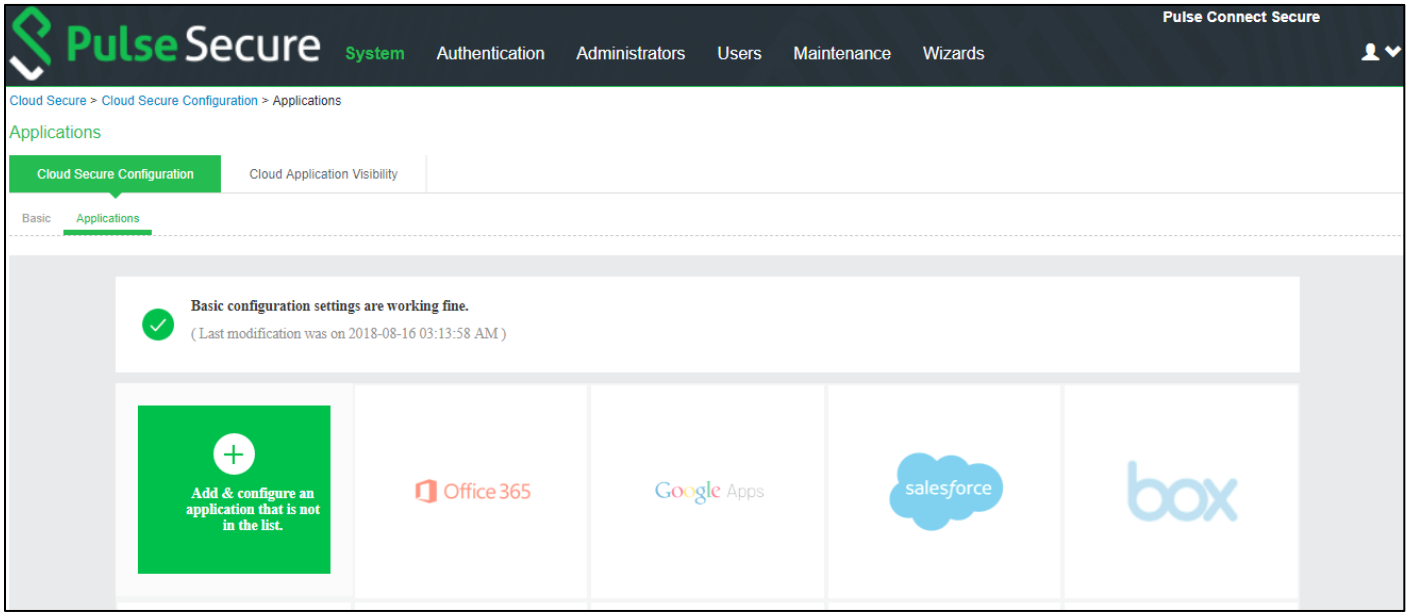
This document describes the configuration required on Google cloud service and configuration of Google Service Provider on Pulse Connect Secure to provide Secure Single Sign-On access to the users accessing various Google applications. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace (PWS) Server which are required to be enabled before configuring Service Provider specific configurations outlined in this document.

Pulse Connect Secure Configuration

For basic configurations details, refer to the following sections:

- **Configuring Pulse Connect Secure - Basic Configurations (Mandatory)**
- **Configuring Pulse Workspace**

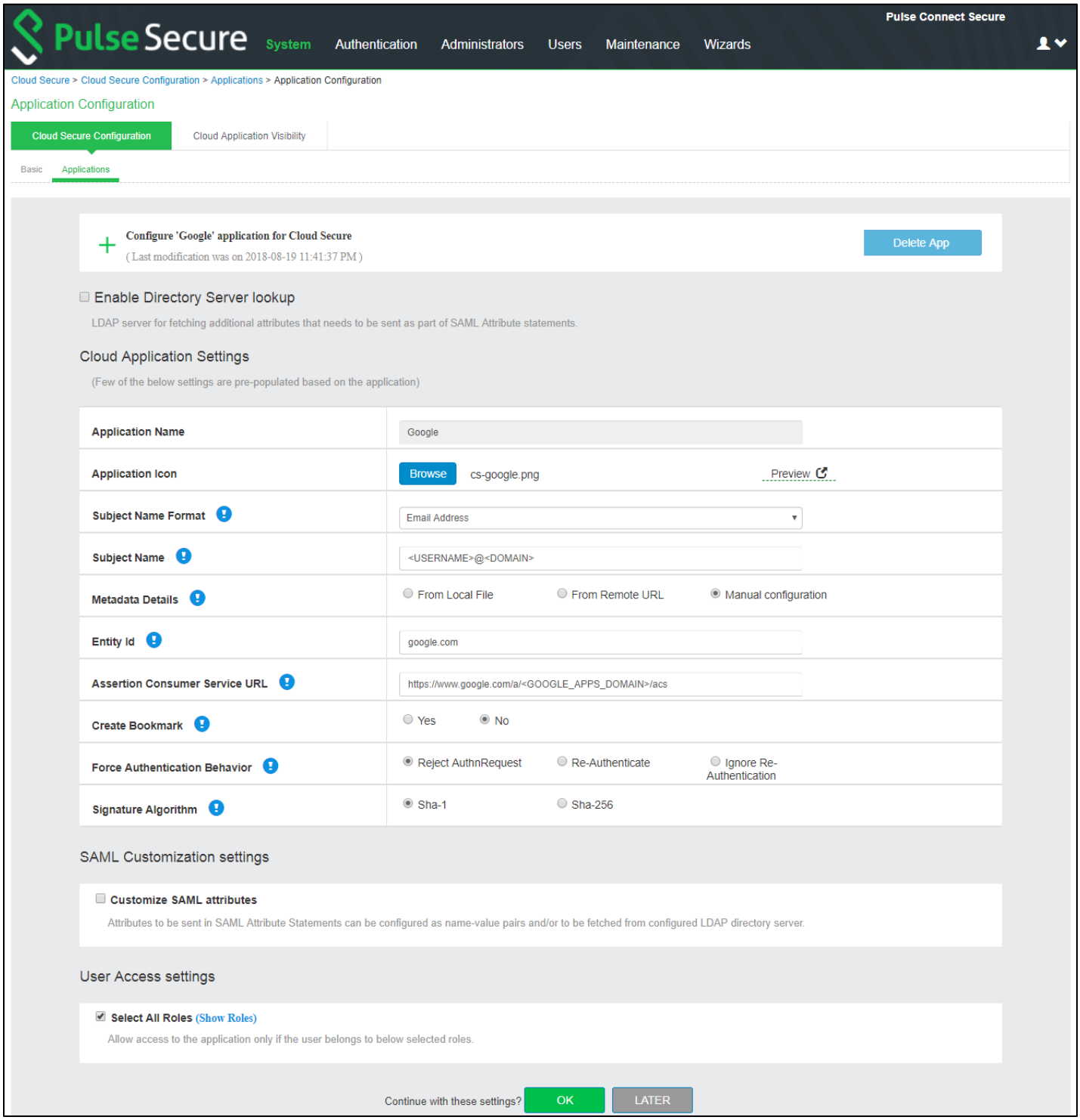
The Admin can configure the Google Cloud Applications as Peer SP once the basic configurations are completed. The Google application is available with some pre-populated application settings for ease of configuration.



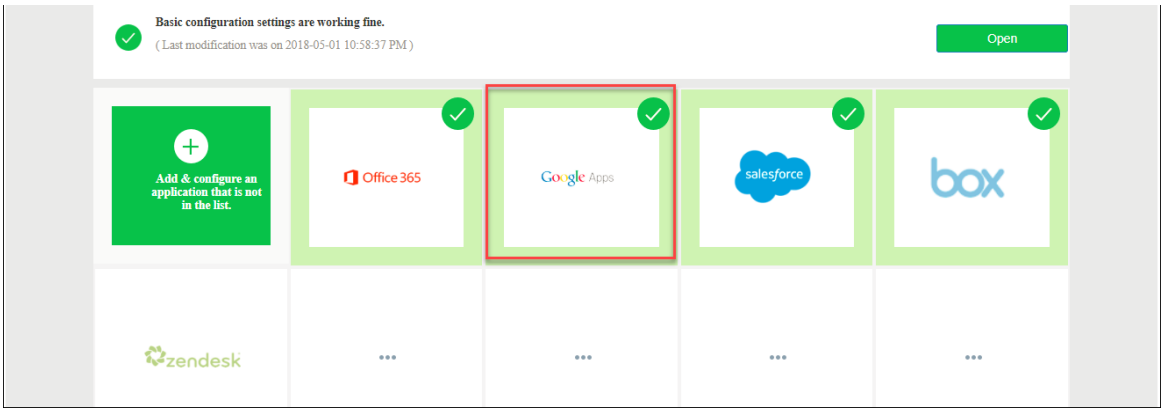
To configure Google application:

1. Click the Google Apps icon to configure the application.
2. Under Cloud Application Settings:
   a. Enter the application name.
   b. Click Browse and select the application icon.
   c. Select the Subject Name Format = Email Address.
   d. Enter the Subject Name.
   e. Under Metadata details, upload the metadata file through manual configuration by entering the Entity ID and Assertion Consumer Service URL.
      i. Entity ID = google.com
      ii. Assertion Consumer Service URL = https://www.google.com/a/<Google Domain>/acs
   f. (Optional) Set Create Bookmark to Yes to support IdP initiated SSO.
   g. Set the Force Authentication Behaviour to Ignore Re-Authentication.
   h. Set Signature Algorithm to Sha-1 or Sha-256.
3. Under User Access settings, assign the application to applicable roles.
4. Click OK.

Figure 1 Google Application



The following screen with a green tick mark on the Google Apps is displayed after a successful configuration.



Google Configuration

Google should be enabled as SAML Service Provider for supporting Single Sign-On. For Cloud Secure Solution:

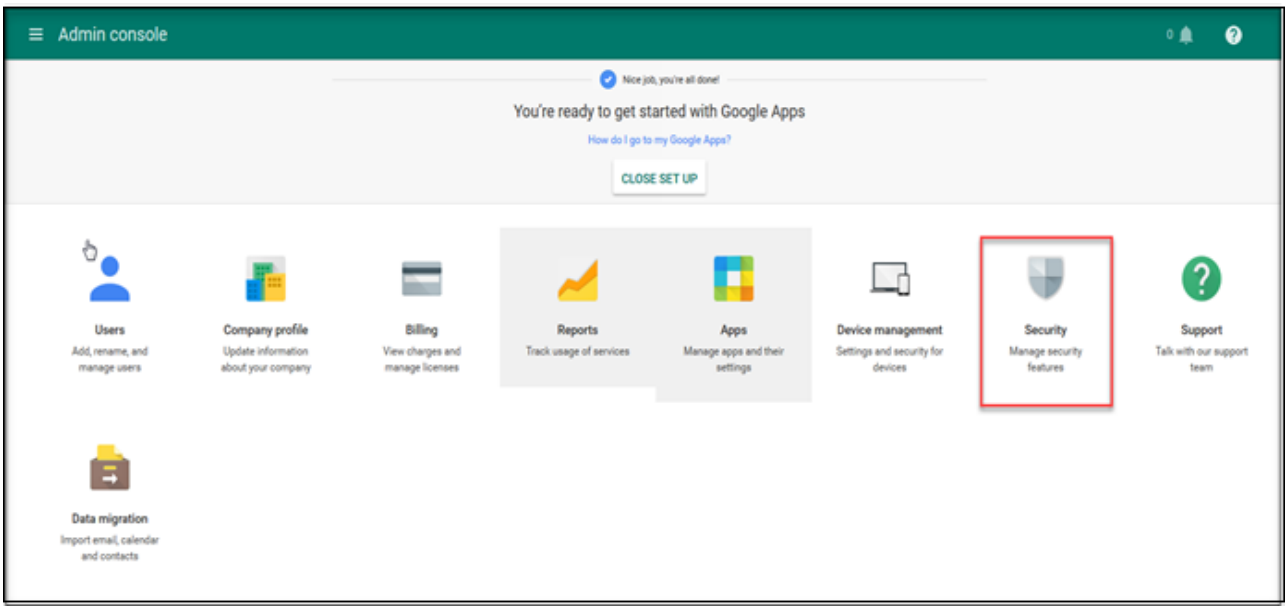
- Sign up for Google Android for Work Account
- Buy a Google Domain
- Setup SAML Single Sign-On
- Create users with different email address in the Google domain

Steps to Configure

Follow the below steps to configure Google as Service Provider:

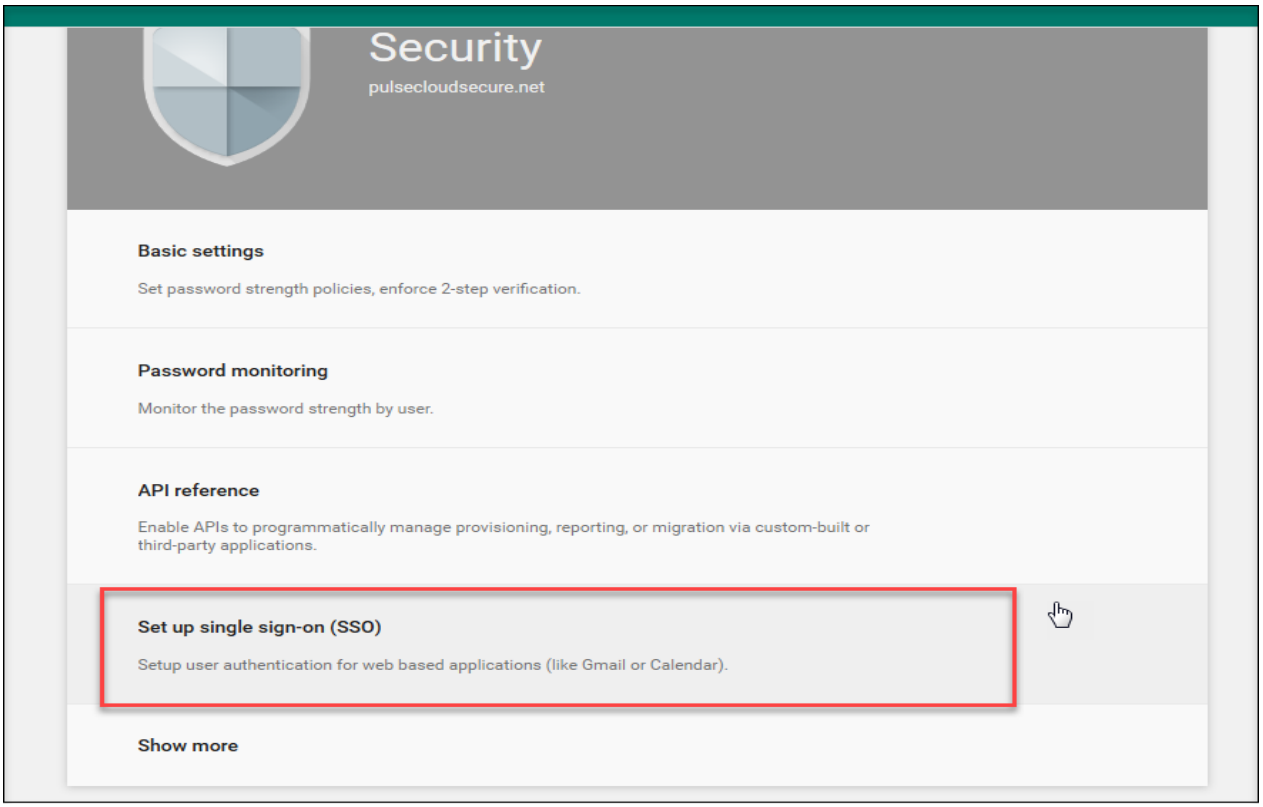
1. Sign up for Google Android for Work Account at https://www.google.com/work/apps/business/. Buy a new Google domain.
2. Log in to admin console at https://admin.google.com/ with the new domain admin credentials.
3. Click **Security**.

Figure 2 Security Settings



4. Click **Setup Single Sign-on (SSO)**.

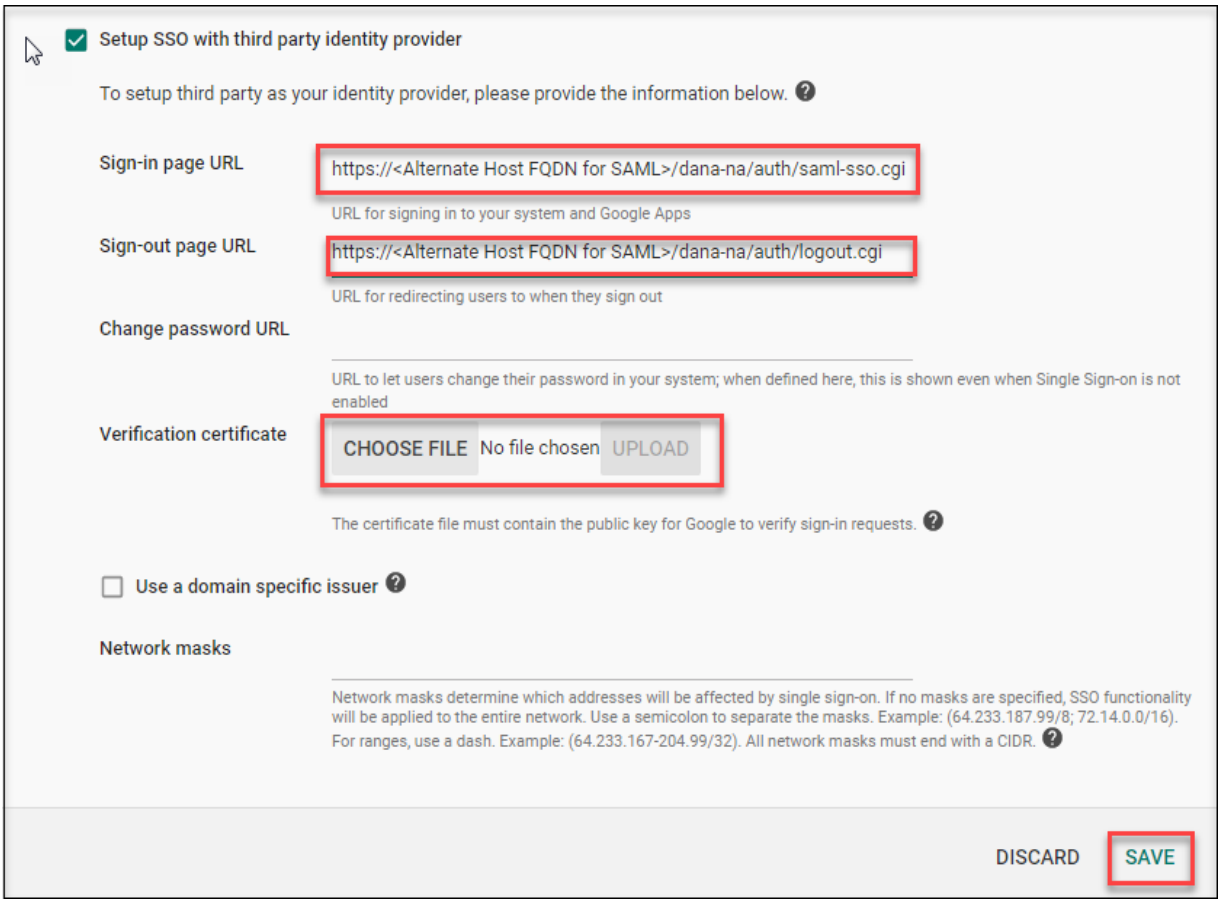
Figure 3 Setup Single Sign-On



5. Select **Setup SSO with third party identity provider** and provide the below values:
   a. Sign-in page URL = https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi
   b. Sign-out page URL = https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi
   c. Verification Certificate:
   - Download PCS Metadata file from Authentication > Signing-in > Sign-in SAML > Metadata Provider. Copy Certificate content out of PCS Metadata to a file, save it, generate X509 Certificate out of it and upload it here (or)
   - Choose the IdP Signing Certificate configured under Authentication > Signing-in > Sign-in SAML > Identity Provider page of PCS and upload it here.

   d. Click **SAVE**.

Figure 4 Configure SAML



6. Select **Users** from the menu on top left corner, click on '+' at the bottom right corner of the page to add new users. Provide user details and click **Create** to create new domain users.

Note: Super Admin user will not be able to do Single Sign-On.

End-User Flow on Mobile Devices

Once the administrator completes the Google configurations and creates a new user if not present in Pulse Workspace, user has to follow the below steps to register the mobile device with Pulse Workspace and get seamless secure Single Sign-On access to Google Applications.

1. User receives Welcome Mail with registration details.
2. Follow the instructions in the mail and register the user device.
3. Once registration of mobile device with Pulse Workspace is successful, configured profile will get installed on the device along with VPN certificate.
4. Install Google managed applications (Gmail, Google Docs, Google Sheets, Google Drive etc) when prompted.
5. Install Pulse Client on the mobile device. VPN profile will get configured automatically on Pulse Client.
6. On Android devices, open Pulse Client and establish VPN connection manually. VPN tunnel will automatically get established on iOS devices when managed application configured with Per App VPN is accessed.
7. Access Google application and provide email address.
8. Single Sign-On will happen and user will get access to the Google application.
9. Access any other Google application. It will re-use the existing account and provide access to this application as well without the need to provide any details.

End-User Flow on Desktops

Once the administrator completes the Google configurations, user can access Google domain through browser or thick application from Windows/MAC OS X Desktops. Follow the below steps to enable Secure Single Sign-On browser-based/thick app based access to Google Cloud Service.

1. Launch Pulse Client and establish a VPN session with PCS
2. Open any web browser on the desktop, access Gmail or other Google service and provide Google email address (or) access Google thick application and provide email address.
   - If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in, PCS will send SAML response to Google SP and user will be granted access to Google Cloud Service.
   - If user did not establish Pulse VPN session as mentioned in Step 1, user will be redirected to Pulse Connect Secure user login page or user will be prompted to select user certificate for authentication depending on the PCS configuration. Once authenticated, PCS will send SAML response to Google SP and user will be granted access to Google Cloud Service.

Troubleshooting

Single Sign-On for a Google user can fail due to configuration issues on Pulse Connect Secure, Google Service Provider, Pulse Mobile Client or Pulse Workspace. To troubleshoot issues with Single Sign-On:

- On PCS, under Maintenance > Troubleshooting, enable the event codes – "saml, auth" at level "50" and collect debug logs. Enable Policy Tracing and capture the Policy traces for the specific user.
- Check System > Log/Monitoring > User Access > Log for SAML AuthNRequest and Response for the specific user. Verify if 'Subject Name' is proper in the SAML Response.
- On mobile device, open Pulse Client and Send Logs to your administrator.