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

http://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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 http://www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
Table of Contents

Introduction ............................................................................................................................................. 5
  About this guide .................................................................................................................................... 5
Pulse Connect Secure Configuration ........................................................................................................ 6
Google Configuration ............................................................................................................................... 8
End-User flow on Mobile Devices........................................................................................................... 11
End-User flow on Desktops ..................................................................................................................... 12
Troubleshooting ..................................................................................................................................... 13
List Of Figures

Figure 1 Add Service Provider ......................................................................................................................... 7
Figure 2 Security Settings ................................................................................................................................. 8
Figure 3 Setup single sign-on ............................................................................................................................ 9
Figure 4 Configure SAML .................................................................................................................................. 10
Introduction

About this guide

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. Basic configurations of PCS and PWS are covered as part of Common Components Configuration Guide.
Pulse Connect Secure Configuration

Pulse Connect Secure (PCS) should be enabled as SAML Identity Provider for supporting Single Sign-On. For Cloud Secure solution PCS should be configured with:

- Network Settings
- Certificates
- Registration with Pulse One
- Pulse Workspace MDM Authentication Server configured as device attribute server
- SAML configurations
- Role and Realm configurations

For details on above configurations of Pulse Connect Secure, refer to Common Components Configuration Guide.

In addition to above configurations, Google should be configured as Service Provider on Pulse Connect Secure.

Follow below steps to configure Google SP on PCS:

1. Login to Pulse Connect Secure admin console

2. Navigate to Authentication->Signing In->Sign-in SAML->Identity Provider. Click on ‘Add SP’ on the configuration page:
   a. Select Configuration mode as Manual
   b. Entity ID = google.com
   c. Assertion Consumer Service URL = https://www.google.com/a/<Google Domain>/acs
   d. Select ‘Post’ binding
   e. Select Override Default Configuration (Optional). This configuration is required only if you wish to make SP specific changes (say, override Subject Name specified in Basic Identity Provider configuration at Authentication->Signing In->Sign-in SAML->Identity Provider)
   f. Assign required roles
   g. Click Save Changes
Figure 1 Add Service Provider
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 below steps to configure Google as Service Provider:

2. Login to admin console at [https://admin.google.com/](https://admin.google.com/) with the new domain admin credentials
3. Click on ‘Security’

*Figure 2 Security Settings*
4. Click on ‘Setup single sign-on (SSO)’

Figure 3 Setup single sign-on

5. Check ‘Setup SSO with third party identity provider’ and provide below values:
   b. Sign-out page URL = https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi
   c. Verification Certificate:
      o 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)
      o 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’
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 administrator does the above configurations and creates a new user if not present in Pulse Workspace, user has to follow 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 administrator does the above configurations, user can access Google domain via browser or thick application from Windows/MAC OS X Desktops. Follow 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
   a. 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
   b. 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.