Cloud Secure – PingOne Integration

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

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 – PingOne Integration 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

List of Figures

Introduction

About This guide

Cloud Secure Solution provides Secure Single Sign-On for Cloud services using PingOne as Identity Management Provider. In this federated solution, PingOne acts as both Identity Provider (for Cloud services) and Service Provider (for Pulse Connect Secure). PingOne allows Pulse Connect Secure to be configured as Third Party SAML Identity Provider to enable Secure Single Sign-On to Cloud applications.

This document provides configuration of PingOne SP on Pulse Connect Secure, configuration of Zendesk Service Provider and PingOne. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace Mobile Device Management (PWS) Server which are required to be enabled before configuring PingOne and cloud service specific configurations outlined in this document. Basic configurations of PCS and PWS are covered as part of Cloud Secure Admin Guide.

MobileIron and AirWatch Third-party MDM servers can also be used in this solution to manage devices and to evaluate compliance posture of the mobile devices.

Pre-requisites

Prerequisites for this solution include:

- **Identity Provider**: Pulse Connect Secure with minimum version of 8.2R3
- **MDM Server**: Pulse Workspace Server/ MobileIron/ AirWatch
- **Identity Management Provider**: PingOne
- **Clients**: iOS Device/ Android Device/ Windows/ MAC OS X Desktops

Figure 1 Architecture Diagram
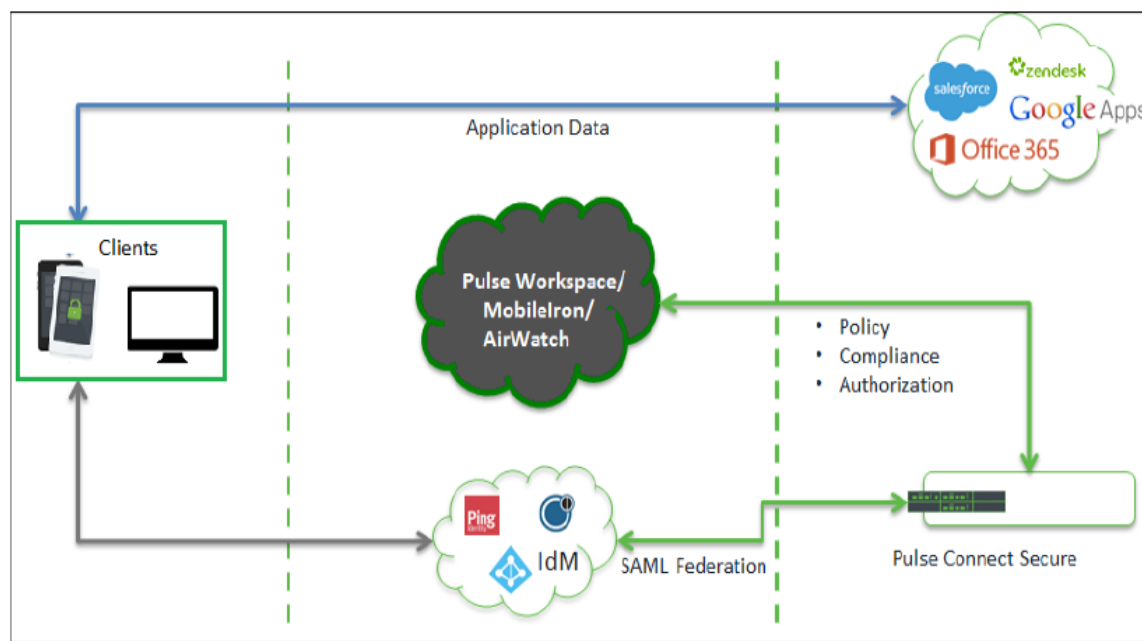
Pulse Connect Secure Configuration

Cloud Secure can be configured with the new UX, which allows you to quickly and easily configure the Cloud Secure functionality without navigating into multiple pages. The new UX enhances the administrator experience through pre-populating some of the relevant settings and reusing the existing configurations.

For basic configurations details, refer to the following sections:

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

- **Configuring Pulse Workspace**

Follow the below steps to configure PingOne as third-party IDP on PCS:

1. **Navigate to System > Cloud Secure > Cloud Secure Configuration**.

   If you have completed the basic configurations and activated Cloud Secure. Click **Open** to go back to the Basic Configuration page.

2. Click **Third-party IdP Settings**:

   a. Click **Add New** and select the **Third-party IdP** as PingOne.

   b. Select the Subject Name Format = Email Address.

   c. Enter the Subject Name.

   d. Click **Browse** and upload the metadata file (Step 7 of PingOne Configuration).

   e. Set the signature algorithm to **Sha-1** or **Sha-256**.

   f. Select the desired roles.

   g. Click **OK**.

Figure 2 New Metadata Provider

Note:
- Click Show IdP to view the details of the configured Third-Party IdP servers.

PingOne Configuration

In this solution, PingOne serves as Identity Management Provider. PingOne acts as Identity Provider for Cloud services and as Service Provider for Pulse Connect Secure. For Cloud Secure solution, PingOne has to be configured with:

- PingOne Account
- Add PCS as SAML IdP
- Configure Cloud Applications

Steps to Configure

Follow the below steps to configure PingOne::

1. Sign up for PingOne admin account at https://admin.pingone.com/web-portal/login and create your domain.
2. Log in to PingOne domain account as admin at https://desktop.pingone.com/<Domain>.
3. Navigate to **Setup > Identity Repository**. Click **Change Identity Repository**.

Figure 3 Setup Identity Repository
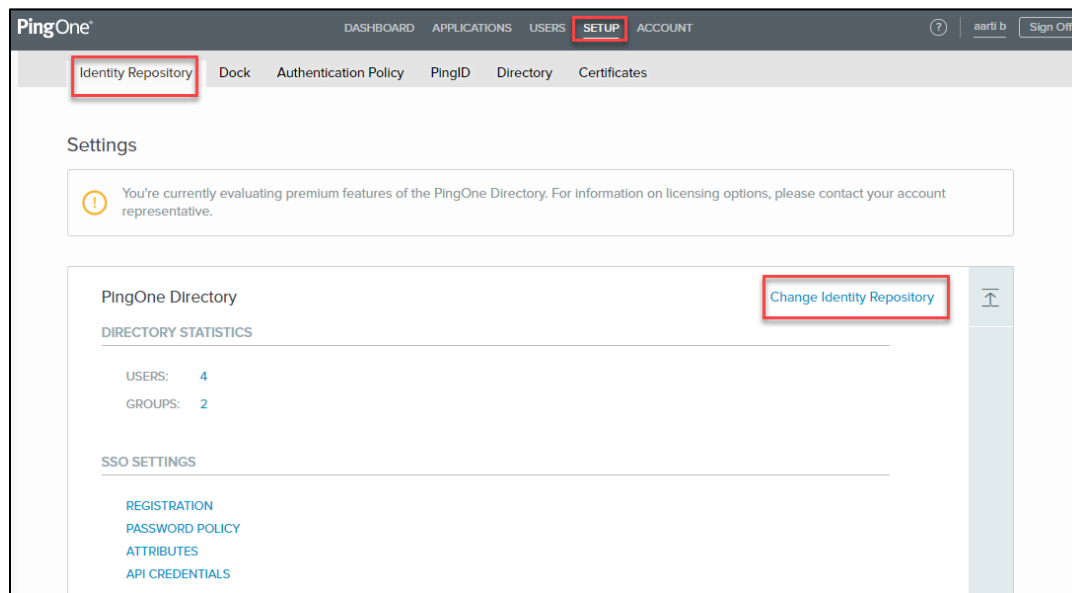
4. Select **3rd Party SAML** as Identity Repository. Click **Next**.

Figure 4 Select Identity Repository

5. Select **Enable Account Specific Entity ID**. Click **Next**.

Figure 5 Configure IDP Connection

6. Under the **Configure your PingOne Connection** section, select **Import your IDP Connection Metadata**, select **PCS SAML Metadata file** and click **Save** (To download PCS Metadata file, navigate to Authentication >Signing-in >Sign-in SAML >Metadata Provider and click on 'Download Metadata' on PCS admin console).

Figure 6 Import IDP Metadata

7. Once the settings are saved, verify that all the PingOne Settings and SAML Settings are updated. Click on the edit icon and download **PingOne SAML Metadata**.

Figure 7 Import IDP Metadata

8. To add Zendesk application in PingOne for SSO, follow below steps:
   a. Navigate to **Applications > My Applications**.
   b. Click on **Add Application** and select **Search Application Catalog**.

Figure 8 Add Application

c. Type **Zendesk** in search list. Click on Zendesk application in the results.

Figure 9 Search Application Catalog

d. Click **Setup**.

Figure 10 Setup Zendesk

e. Leave values to default and click **Continue to Next Step**.

Figure 11 SSO Instructions

f. Under 'Configure your connection' section, provide **Zendesk ACS URL** (replace ${accountname} with your Zendesk Domain). Similarly, provide **Zendesk Entity ID** (replace ${accountname} with your Zendesk Domain and prepend https://. For example, https://cloudsecure.zendesk.com). Click **Continue to Next Step**.

Figure 12 Configure SSO

g. Under **Attribute Mapping** section, leave default values and click **Continue to Next Step**.

Figure 13 Attribute Mapping

h. Click **Save and Publish** in the next page.

Figure 14 Customize PingOne App

i. Review **Setup** and click **Finish**.

Figure 15 Review Setup

9. Navigate to **Applications > My Applications** and verify that Zendesk application got configured and is **Active**. Click on the Application. All the configuration details will be displayed. Download **Signing Certificate** and make a note of the **idpid** value from **Initiate Single Sign-On SSO URL**. These will be used to configure the Service Provider.

Figure 16 Download Signing Certificate

Zendesk Configuration

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

- Register with Zendesk and create new Domain
- Configure SAML

Steps to Configure

Follow the below steps to configure Zendesk as Service Provider:

1. Register with Zendesk at https://www.zendesk.com/register#getstarted and create a new domain.
2. Log in to Zendesk domain as admin at https://<Zendesk Domain>/access/normal.
3. Navigate to **Admin (Settings gear at the bottom left corner) > Security > Admin & Agents**. Enable **Single sign-on (SSO)**, and enable **SAML**. Configure following values:
   a. SAML SSO URL = https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid> (Get idpid value from Step 9 of PingOne Configuration above)
   b. Certificate fingerprint = <Certificate Thumbprint of PingOne Certificate> (Open PingOne Signing Certificate downloaded in Step 9 of PingOne Configuration above. Go to Details tab, scroll to the end. Copy and Paste the value of Certificate Thumbprint here)
   c. Optionally configure **Remote logout URL**.
   d. Click **Save**.

Figure 17 Enable SSO for Admin
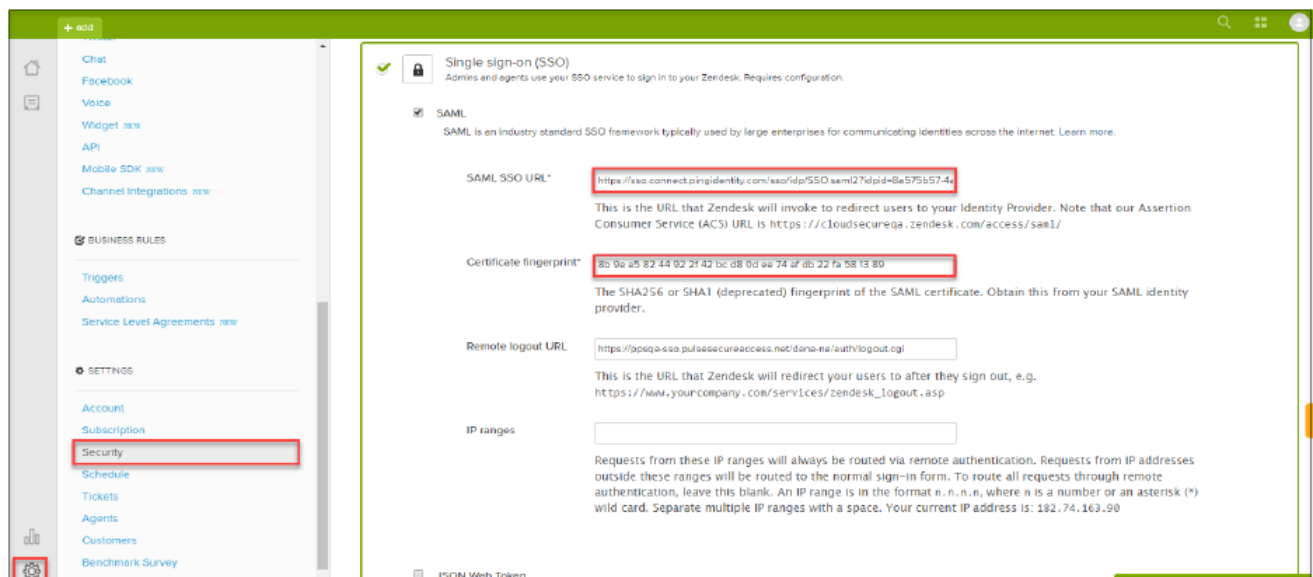
4. Navigate to **Admin (Settings gear at the bottom left corner) -> Security-> End-users**. Enable **Single sign-on (SSO)**. All the configurations made in Admin & Agents tab will get populated automatically.

Figure 18 Enable SSO for End-users
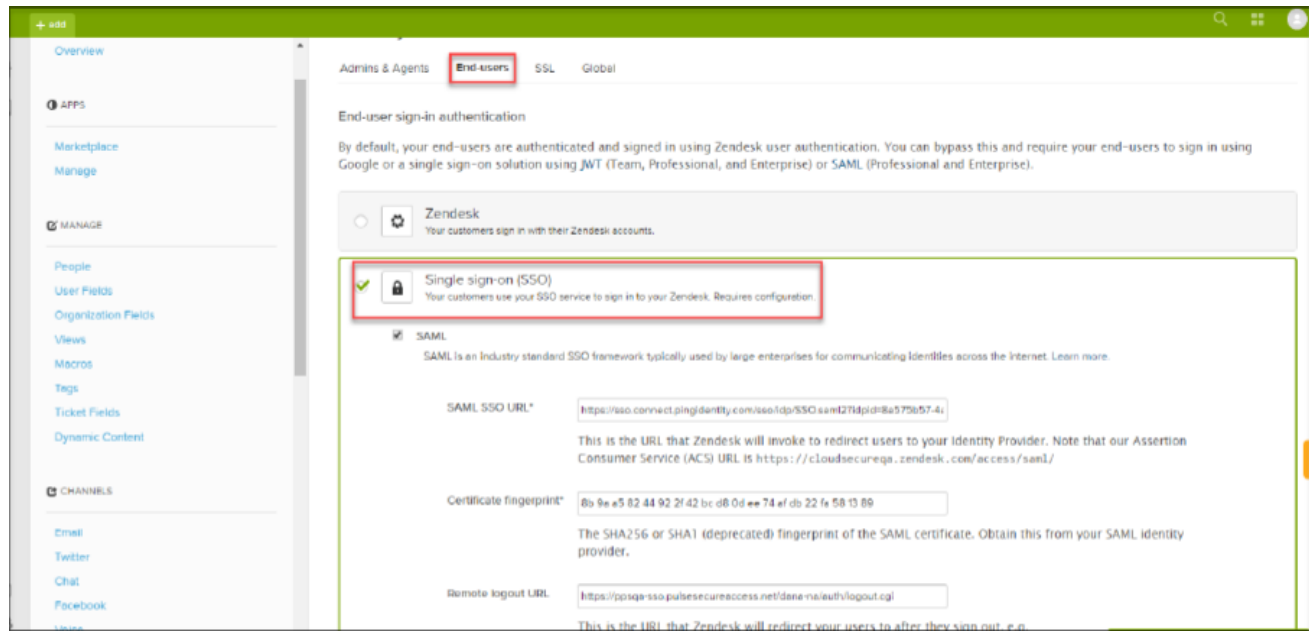
End-User Flow on Mobile Devices

Once the administrator completes the above configurations and creates a new user 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 Zendesk Application.

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 Zendesk managed application when prompted.
5. Install Pulse Client on the mobile device. VPN profile will get configured automatically on Pulse Client.
6. Access Zendesk Application and provide the domain details.
7. VPN tunnel will automatically get established.
8. Single Sign-On will happen and user will get access to the Zendesk domain.

End-User Flow on Desktops

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

1. Launch Pulse Client and establish a VPN session with PCS.
2. Open any web browser on the desktop.
3. Access SSO enabled Zendesk domain.
   - If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in, PCS will send SAML response to PingOne.
   - If user did not establish Pulse VPN session as mentioned in Step 1, user will be redirected to PingOne which in turn redirects the request 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 PingOne.
4. PingOne forwards the SAML response to Zendesk and user will be granted access to Zendesk Cloud Service.

Troubleshooting

Single Sign-On for a Zendesk user can fail due to configuration issues on Pulse Connect Secure, PingOne,, Zendesk 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.

- Log in to PingOne Domain as admin. Navigate to Dashboard-> Reports. Check the notifications to debug the failures.

- On mobile device, open Pulse Client and Send Logs to your administrator.