



Cloud Secure – PingOne Integration

Configuration Guide

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

INTRODUCTION5

 ABOUT THIS GUIDE5

 PRE-REQUISITES5

PULSE CONNECT SECURE CONFIGURATION.....6

PINGONE CONFIGURATION.....7

 STEPS TO CONFIGURE7

ZENDESK CONFIGURATION17

 STEPS TO CONFIGURE17

END-USER FLOW ON MOBILE DEVICES19

END-USER FLOW ON DESKTOPS.....20

TROUBLESHOOTING21

List of Figures

FIGURE 1 ARCHITECTURE DIAGRAM.....	5
FIGURE 2 NEW METADATA PROVIDER	6
FIGURE 4 SETUP IDENTITY REPOSITORY	7
FIGURE 5 SELECT IDENTITY REPOSITORY.....	8
FIGURE 6 CONFIGURE IDP CONNECTION.....	8
FIGURE 7 IMPORT IDP METADATA.....	9
FIGURE 8 IMPORT IDP METADATA.....	9
FIGURE 9 ADD APPLICATION.....	10
FIGURE 10 SEARCH APPLICATION CATALOG.....	11
FIGURE 11 SETUP ZENDESK.....	11
FIGURE 12 SSO INSTRUCTIONS.....	12
FIGURE 13 CONFIGURE SSO.....	13
FIGURE 14 ATTRIBUTE MAPPING.....	14
FIGURE 15 CUSTOMIZE PINGONE APP.....	14
FIGURE 16 REVIEW SETUP.....	15
FIGURE 17 DOWNLOAD SIGNING CERTIFICATE.....	16
FIGURE 18 ENABLE SSO FOR ADMIN	17
FIGURE 19 ENABLE SSO FOR END-USERS.....	18

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.

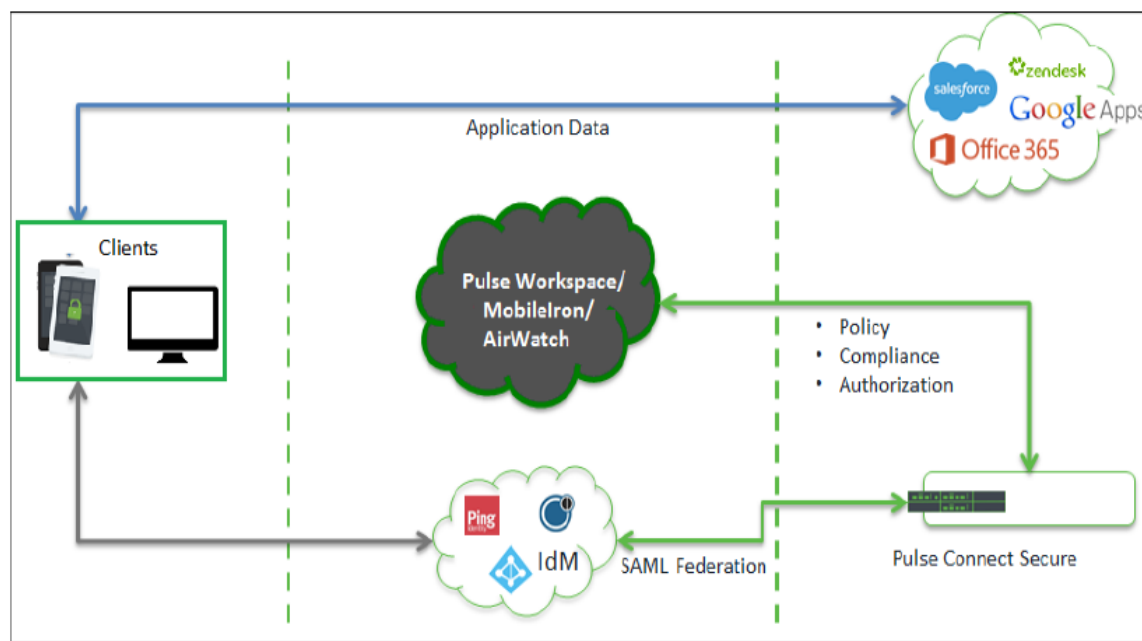
MobileIron and AirWatch Third-party MDM servers can also be used in this solution to manage devices and to evaluate compliance posture of the mobile devices.

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

Pingone Settings
Configured settings for IdP

[Edit](#) | [Add New](#) | [Show IdP](#)

User Identity

Subject Name Format ⓘ	Email Address
Subject Name ⓘ	<USERNAME>@<DOMAIN>
Metadata File ⓘ	Browse Choose file
Signature Algorithm ⓘ	<input checked="" type="radio"/> Sha-1 <input type="radio"/> Sha-256

☒ **Select All Roles** ([Show Roles](#))
Allow access to the resource only if the user belongs to below selected roles.

Bookmark Settings

☐ **Create Bookmark**
Configure bookmarks for each SP configured with this 3rd party IDP. Use the below table to override Relaystate, Subject Name format and Subject Name for specific bookmarks.

[OK](#) [LATER](#)

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:

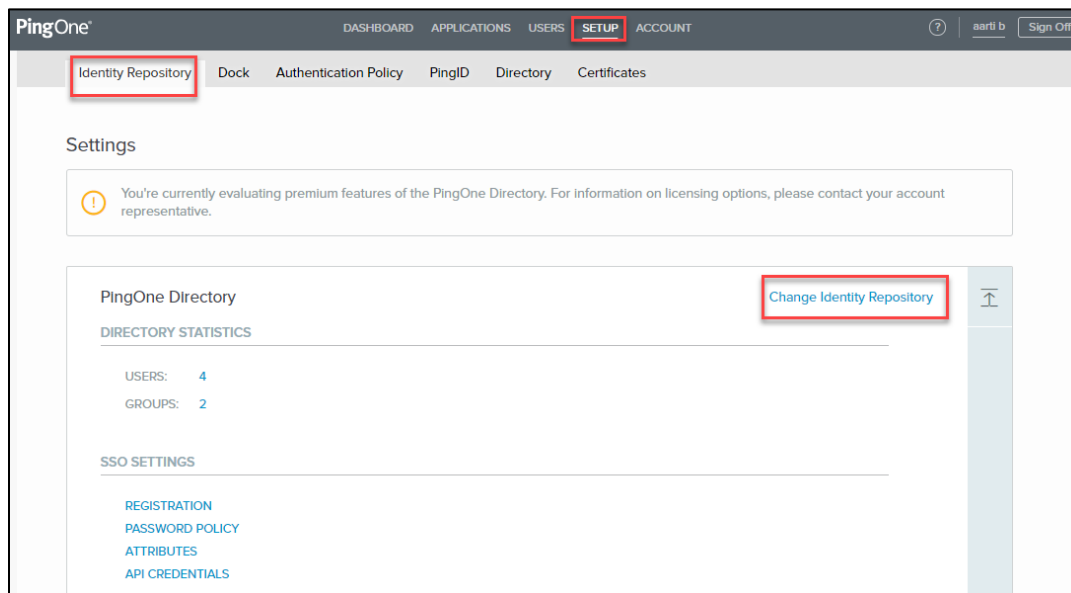
- PingOne Account
- Add PCS as SAML IdP
- Configure Cloud Applications

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

Connect to an Identity Repository

1 SELECT AN IDENTITY REPOSITORY : 3rd Party SAML

Securely connect users and groups for single sign-on through your PingOne account.

☐ AD Connect

☐ PingFederate

☐ Google

☒ 3rd Party SAML

☐ OpenID Connect

OR:

☐ Create a PingOne Directory

Next

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

Figure 5 Configure IDP Connection

Connect to an Identity Repository

2 CONFIGURE YOUR IDP CONNECTION

CHOOSE SIGNING CERTIFICATE ?

PingOne Universal Certificate Primary (Expires 20/05) v

ENABLE ACCOUNT SPECIFIC ENTITY ID ?

☒

http://pingone.com/lb35c15d-0a79-4f8d-86ca-b81i

SIGN AUTHNREQUEST FROM PINGONE

☐

SIGNING ALGORITHM ?

RSA_SHA256 v

Configure the IdP connection to PingOne at your IdP. Either upload the metadata to your IdP (recommended), or manually enter the SAML parameter values at your IdP.

☒ Download the PingOne metadata and upload it to your IdP.

Download PingOne Metadata

☐ Enter the PingOne connection information manually at your IdP. ?

Next

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

Connect to an Identity Repository

1 SELECT AN IDENTITY REPOSITORY : 3rd Party SAML [Edit](#)

2 CONFIGURE YOUR IDP CONNECTION [View](#)

3 CONFIGURE YOUR PINGONE CONNECTION

Assign IdP connection information to the PingOne SAML parameters. Either upload the metadata to your IdP (recommended), or manually enter this connection data at your IdP.

☒ Import Your IDP Connection Metadata

[Change File](#)

[saml-metadata-sa \(1\).xml](#) [Remove](#)

[USE URL](#)

☐ Manually Enter Your IDP Connection Information [?](#)

[Cancel](#) [Save](#)

- 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

PingOne

DASHBOARD APPLICATIONS USERS **SETUP** ACCOUNT

Identity Repository **Dock** Authentication Policy PingID Certificates

Settings

3rd Party SAML [Change Identity Repository](#)

PINGONE SETTINGS

ENABLE ACCOUNT SPECIFIC ENTITY ID: Yes

SIGN AUTHNREQUEST FROM PINGONE: No

PINGONE ENTITY ID: <http://pingone.com/1b35c15d-0a79-4f8d-86ca-b81a2967ba35>

ASSERTION CONSUMER SERVICE URL: <https://sso.connect.pingidentity.com/sso/sp/ACS.saml2>

RELAY STATE: [https://pingone.com/1.0\[saas_id\]](https://pingone.com/1.0[saas_id])

ACS URL PARAMETER: [?saasid=\[saas_id\]](#)

PROTOCOL: SAML 2.0

ACTIVE SIGNING CERTIFICATE: Type: PRIMARY
Expires: 2020/05/03
[Download](#)

ENCRYPTION CERTIFICATE: Expires: 2020/05/04
[Download](#)

SAML SETTINGS

ENTITY ID: <https://sso.pulsesecureaccess.net/dana-na/auth/saml-endpoint.cgi>

SSO ENDPOINT: <https://ppsqa-sso.pulsesecureaccess.net/dana-na/auth/saml-ss0.cgi>

SIGNING ALGORITHM: RSA_SHA256

PRIMARY CERTIFICATE: DN: CN=pulsesecureaccess.net, OU=Domain Control Validated
Expires: 2019/07/07

Connect to an Identity Repository

2 CONFIGURE YOUR IDP CONNECTION

CHOOSE SIGNING CERTIFICATE ⓘ

PingOne Universal Certificate Primary (Expires 20/05) ▾

ENABLE ACCOUNT SPECIFIC ENTITY ID ⓘ

☒

`http://pingone.com/1b35c15d-0a79-4f8d-86ca-b81:`

SIGN AUTHNREQUEST FROM PINGONE

☐

SIGNING ALGORITHM ⓘ

RSA_SHA256 ▾

Configure the IdP connection to PingOne at your IdP. Either upload the metadata to your IdP (recommended), or manually enter the SAML parameter values at your IdP.

☒ Download the PingOne metadata and upload it to your IdP.

Download PingOne Metadata

☐ Enter the PingOne connection information manually at your IdP. ⓘ

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

PingOne® DASHBOARD APPLICATIONS USERS SETUP ACCOUNT ⓘ aarti b Sign Out

My Applications Application Catalog PingID SDK Applications OAuth Settings






My Applications

SAML **OIDC**

Applications you've added to your account are listed here. You can search by application name, description or entityId

- Active applications are enabled for single sign-on (SSO).
- Details displays the application details.

Make sure to assign each application to the appropriate groups on the [User Groups](#) page. This enables the display of the applications in the dock and authorizes the assigned group members to use the applications.

Application Name	Type	Status	Enabled	
 Google	Web	Active	<input checked="" type="checkbox"/>	Remove ▶
 Facebook	Web	Active	<input checked="" type="checkbox"/>	Remove ▶
 Twitter	Web	Active	<input checked="" type="checkbox"/>	Remove ▶
 LinkedIn	Web	Active	<input checked="" type="checkbox"/>	Remove ▶
 Slack	Web	Active	<input checked="" type="checkbox"/>	Remove ▶

Add Application ▾

Search Application Catalog

New SAML Application

Request Ping Identity add a new application to the application catalog

Pause All SSO ⓘ

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

Figure 9 Search Application Catalog


My Applications Application Catalog

Application Catalog

Home / Applications / Application Catalog

Browse for the application you want to add or search for it by name. Don't see the application you're looking for? Fill out our [Application Request Form](#).


Zendesk Search


Application Name	Type
 Zendesk	SAML


d. Click **Setup**.


Figure 10 Setup Zendesk


Zendesk Search

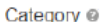
Application Name	Type
 Zendesk	SAML

Logo 

Icon 

Name  Zendesk

Description  Zendesk simplifies your support team's workflow with custom automatic actions, meaningful organization, and streamlined systems for managing support content.

Category  CRM

Setup

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

Figure 11 SSO Instructions

1. SSO Instructions

Signing Certificate

PingOne Account Origination Certificate ▼

[Download](#)

For reference, please note the following configuration parameters:

SaaS ID

e9a1bcee-4f4c-4fe2-a5b8-ec83d2a53491

Initiate Single Sign-On (SSO) URL

<https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=e9a1bcee-4f4c-4fe2-a5b8-ec83d2a53491&idpid=673b5ebc-e6ce-4326-a445-999cf3fdd8ab>

Issuer

<https://ngsaqa.pulsesecureqa.net/dana-na/auth/saml-endpoint.cgi>

Signing Algorithm

RSA_SHA256 ▼

In order to set up SSO to Zendesk, please follow the instructions below:

SETTINGS > SECURITY > Authentication

	Label	Description
1	Configure SSO parameters	Check Single Sign On
2	Configure SSO parameters	Mode: SAML
3	Configure SSO parameters	SAML SSO URL: https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={Enter your IDP ID}
4	Configure SSO parameters	https://sso.connect.pingidentity.com/sso/terminatesession?page=https://{enter a URL to redirect users to}
5	Configure SSO parameters	IP ranges (optional): Leave blank for all IPs to use SSO.
6	Configure SSO parameters	Certificate Fingerprint: Obtain the fingerprint of your PingOne signing certificate (to complete the configuration on the ZenDesk-side)

NEXT: Configure your connection

Cancel
Continue to Next Step

- 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

2. Configure your connection

Assign the attribute values for single sign-on (SSO) to the application.

Upload Metadata ⓘ Or use URL

ACS URL *

Replace the parameter(s) "\${accountname}" above with your configuration information.

Entity ID *

Replace the parameter(s) "\${accountname}" above with your configuration information.

Target Resource ⓘ

Single Logout Endpoint ⓘ

Single Logout Response Endpoint ⓘ

Primary Verification Certificate ⓘ No file chosen

Secondary Verification Certificate ⓘ No file chosen

Force Re-authentication ⓘ ☐

PingOne dock URL

Default PingOne dock URL

☐ Use Custom URL ⓘ

NEXT: Attribute Mapping

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

Figure 13 Attribute Mapping

The screenshot shows the '3. Attribute Mapping' section of the PingOne App Customization interface for Zendesk. At the top, the 'Application Name' is 'Zendesk' and the 'Type' is 'SAML'. Below the title, a instruction reads: 'Map your identity bridge attributes to the attributes required by the application.' A table lists three attributes to be mapped:

	Application Attribute	Description	Identity Bridge Attribute or Literal Value	
1	SAML_SUBJECT *	mail	SAML_SUBJECT	<input type="checkbox"/> As Literal <input type="button" value="Advanced"/>
2	displayName	The user's name to be used for display purposes.	Name or Literal	<input type="checkbox"/> As Literal <input type="button" value="Advanced"/>
3	phone	A phone number, specified as a string.	Name or Literal	<input type="checkbox"/> As Literal <input type="button" value="Advanced"/>

Below the table, a note states: '* Indicates a required attribute.' At the bottom left, it says 'NEXT: PingOne App Customization - Zendesk'. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Continue to Next Step' (which is highlighted with a red border).

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

Figure 14 Customize PingOne App

The screenshot shows the '4. PingOne App Customization - Zendesk' screen. It contains the following fields and options:

- Logo:** A green Zendesk logo with a 'Select image' button below it.
- Icon:** A green circular icon with a 'Select image' button below it.
- Name:** A text field containing 'Zendesk'.
- Description:** A text area containing 'Zendesk simplifies your support team's workflow with custom automatic actions, meaningful organization, and streamlined systems for managing support content.'
- Category:** A dropdown menu set to 'CRM'.


At the bottom left, it says 'NEXT: Review Setup'. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Save & Publish' (which is highlighted with a red border).


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

Figure 15 Review Setup

5. Review Setup

Test your connection to the application

Logo 

Icon 

Name

Description

Category

You may need to configure these connection parameters as well.

saasid

Issuer

Signing Algorithm

ACS URL

SP entityid

Initiate Single Sign-On (SSO) URL

Single Sign-On (SSO) Relay State

Single Logout Endpoint

Single Logout Response Endpoint

Force Re-authentication

Signing Certificate [Download](#)

SAML Metadata [Download](#)

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	SAML_SUBJECT *	mail	SAML_SUBJECT
2	displayName	The user's name to be used for display purposes.	
3	phone	A phone number, specified as a string.	

* Indicates a required attribute

Parameter Name	Description	Value
Administrator_Email	The account email of an admin for your Zendesk account.	
Zendesk_Api_Token	The API Token retrieved from Zendesk.	*****
Zendesk_Subdomain	The subdomain of your Zendesk account.	

[Back](#)
[Finish](#)

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

You may need to configure these connection parameters as well.

saasid	e9a1bcee-4f4c-4fe2-a5b8-ec83d2a53491
Issuer	https://ngsaqa.pulsesecureqa.net/dana-na/auth/saml-endpoint.cgi
Signing Algorithm	RSA_SHA256
ACS URL	https://cloudsecureqa.zendesk.com/access/saml
SP entityId	https://cloudsecureqa.zendesk.com
Initiate Single Sign-On (SSO) URL ⓘ	https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=e9a1bcee-4f4c-4fe2-a5b8-ec83d2a53491&idpid=673b5ebc-e6ce-4326-a445-999cf3fdd8ab
Single Sign-On (SSO) Relay State ⓘ	https://pingone.com/1.0/e9a1bcee-4f4c-4fe2-a5b8-ec83d2a53491
Single Logout Endpoint	
Single Logout Response Endpoint	
Force Re-authentication ⓘ	false
Signing Certificate	Download
SAML Metadata	Download

Zendesk Configuration

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

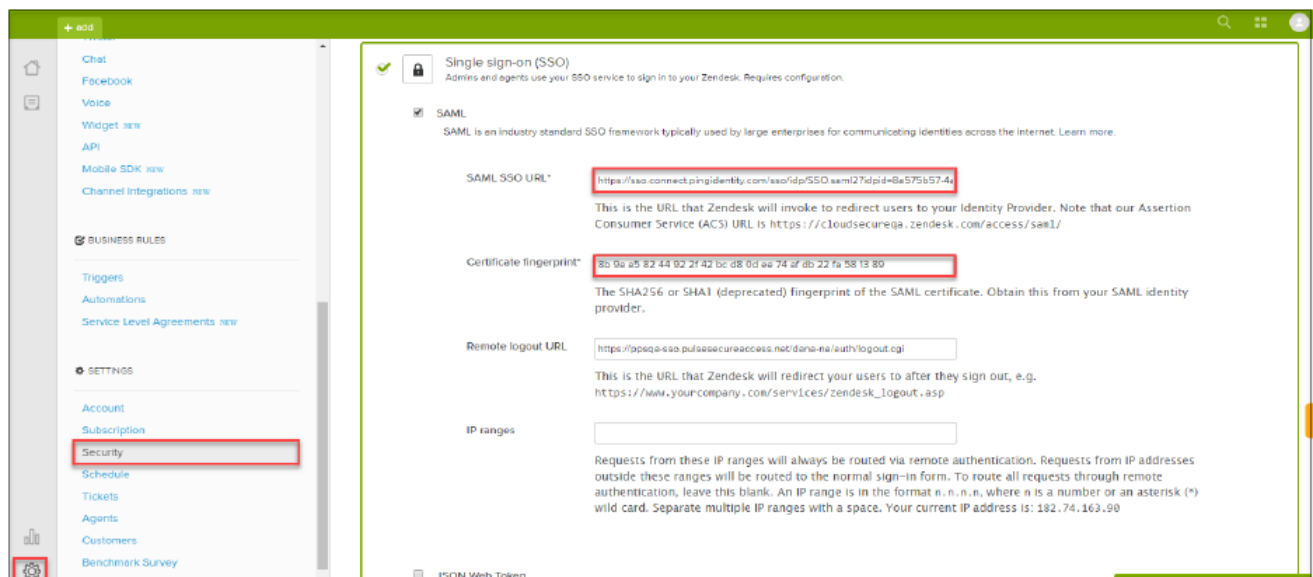
- Register with Zendesk and create new Domain
- Configure SAML

Steps to Configure

Follow the below steps to configure Zendesk as Service Provider:

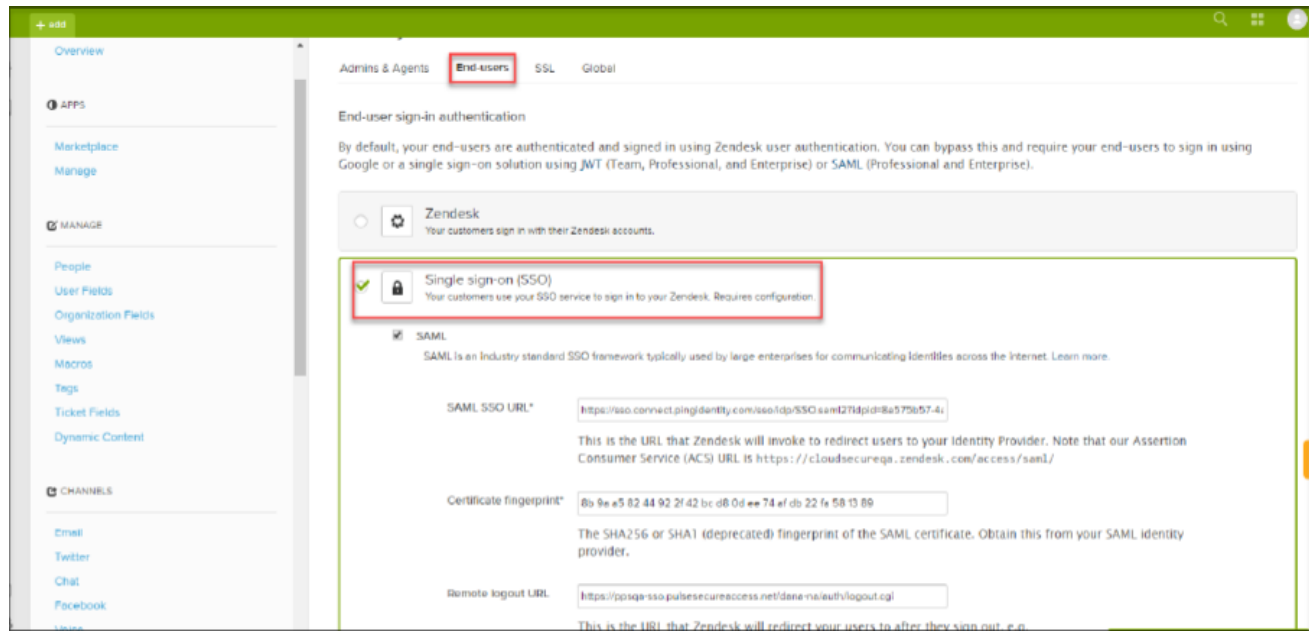
1. Register with Zendesk at <https://www.zendesk.com/register#getstarted> and create a new domain.
2. Log in to Zendesk domain as admin at <https://<Zendesk Domain>/access/normal>.
3. Navigate to **Admin (Settings gear at the bottom left corner) > Security > Admin & Agents**. Enable **Single sign-on (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.