Cloud Secure – Zendesk

Configuration Guide
Table of Contents

Introduction ...........................................................................................................................................5
  About this guide..................................................................................................................................5
Pulse Connect Secure Configuration ........................................................................................................6
Zendesk 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 Enable SSO for Admin............................................................. 9
Figure 3 Enable SSO for End-users...................................................... 10
Introduction

About this guide

This document describes the configuration required on Zendesk cloud service and configuration of Zendesk Service Provider on Pulse Connect Secure to provide Secure Single Sign-on access to Zendesk users. 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, Zendesk should be configured as Service Provider on Pulse Connect Secure.

Follow below steps to configure Zendesk 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’ in the configuration page and provide the following details:
   a. Select Configuration mode as Manual
   b. Entity ID = https://<Zendesk-domain>
   c. Assertion Consumer Service URL = https://<Zendesk-domain>/access/saml
   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

Service Provider Configuration

- **Entity ID**: https://Zendesk Domain>
- **Assertion Consumer Service URL**: https://Zendesk Domain>/access/saml
- **Default Binding**: Post
- **Signature Verification Certificate**:
  - Issued To:
  - Valid:
  - Details: Other Certificate Details
  - Upload Certificate: Browse, No file chosen, Delete
- **Encryption Certificate**:
  - Issued To:
  - Valid:
  - Details: Other Certificate Details
  - Upload Certificate: Browse, No file chosen, Delete
- **Certificate Status Checking Configuration**:
  - Enable signature verification certificate status checking
  - Enable encryption certificate status checking
- **Customize IdP Behavior**:
  - Override Default Configuration
- **Roles**:
  - Policy applies to ALL roles
  - Policy applies to SELECTED roles
  - Policy applies to all roles OTHER THAN those selected below
- **Available roles**:
  - iOS Users
  - iOS/Android Users
  - Remediation
  - SAP
  - Users

Save Changes, Cancel
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 below steps to configure Zendesk as Service Provider:

1. Register with Zendesk at [https://www.zendesk.com/register#getstarted](https://www.zendesk.com/register#getstarted) and create a new domain
2. Login to Zendesk domain as admin at [https://<Zendesk Domain>/access/normal](https://<Zendesk Domain>/access/normal)
3. Navigate to Admin (Settings gear at the bottom left corner) -> Security -> Admin & Agents. Enable ‘Single sign-on (SSO)’, enable ‘SAML’. Configure below details:
   a. SAML SSO URL = [https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi](https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi)
   b. Certificate fingerprint = Provide fingerprint of the Signing Certificate used in Identity Provider configuration on PCS. On PCS, navigate to System -> Configuration -> Certificates -> Device Certificates. Click on the desired device certificate. Expand the arrow under ‘Details’ section and copy the ‘Thumbprint’ value
   c. Remote logout URL = [https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi](https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi)
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 3 Enable SSO for End-users

By default, your end-users are authenticated and signed in using Zendesk user authentication. You can bypass this and require your end-users to sign in using Google or a single sign-on solution using SAML (Team, Professional, and Enterprise) or SAML (Professional and Enterprise).

- **Zendesk**: Your customers sign in with their Zendesk accounts.
- **Single sign-on (SSO)**: Your customers use your SSO service to sign in to your Zendesk. Requires configuration.

**SAML**

SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet. Learn more.

- **SAML SSO URL**: `https://pass-so.pulseaccess.pulsesecureaccess.net/doc/signonauth/samlssologin`
  - This is the URL that Zendesk will invoke to redirect users to your Identity Provider. Note that our Assertion Consumer Service (ACS) URL is `https://cloudsoureza.zendesk.com/access/saml/`.
- **Certificate fingerprint**: `45BD00731699DF150C34ABDEB82FOA0F36DA3F45658`
  - The SHA256 or SHA1 (deprecated) fingerprint of the SAML certificate. Obtain this from your SAML identity provider.
- **Remote logout URL**: `https://pass-so.pulseaccess.pulsesecureaccess.net/doc/signonauth/samllogout`
  - This is the URL that Zendesk will redirect your users to after they sign out, e.g.
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 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. 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 Zendesk Application and provide the URL details (Ex: pulsesecure.zendesk.com)
8. Single Sign-On will happen and user will get access to Zendesk
End-User flow on Desktops

Once administrator does the above configurations, user can access Zendesk URL via browser from Windows/MAC OS X Desktops. Follow below steps to enable Secure Single Sign-On browser-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 Zendesk URL (Ex: pulsesecure.zendesk.com)
   a. If user has an existing VPN session, ‘Re-use existing Pulse Session’ will kick in,
      PCS will send SAML response to Zendesk SP and user will be granted access to Zendesk 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 Zendesk SP 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, 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.
- On mobile device, open Pulse Client and Send Logs to your administrator.