Pulse Secure®

Cloud Secure – Zendesk

Configuration Guide

Document Revisions 4.0
Published Date April 2019

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

https://www.pulsesecure.net

Cloud Secure – Zendesk 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.

Introduction

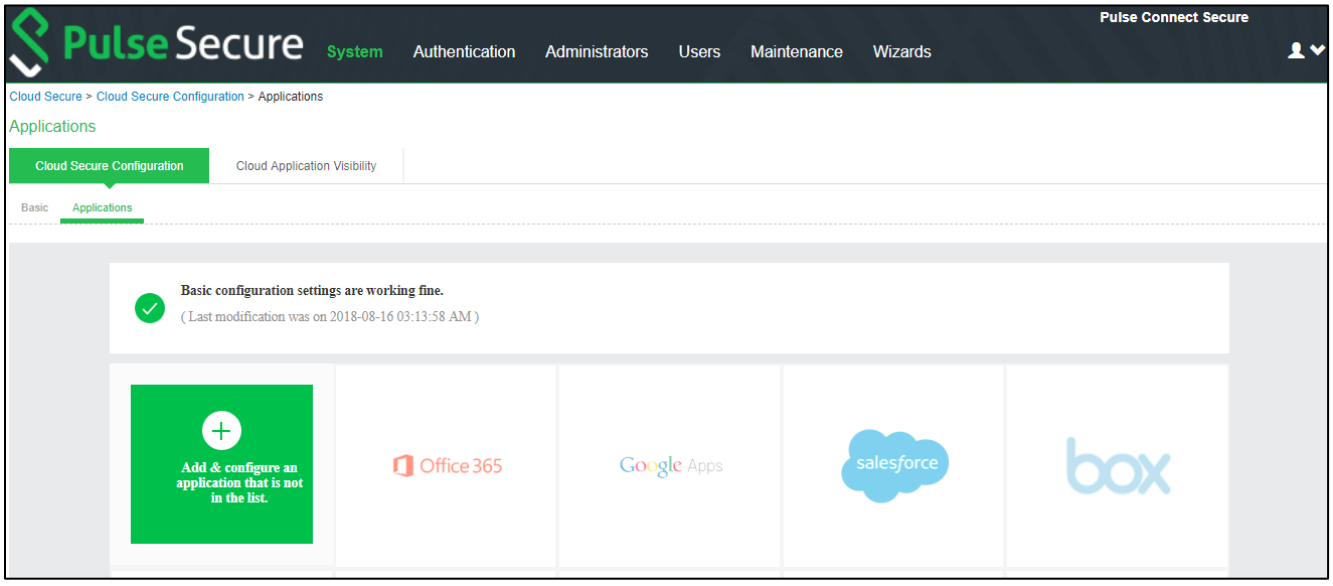
This document describes the configuration required on Zendesk cloud service and configuration of Zendesk Service Provider on Pulse Connect Secure to provide Secure Single Sign-on access to Zendesk users. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace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

Pulse Connect Secure Configuration

For basic configurations details, refer to the following sections:

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

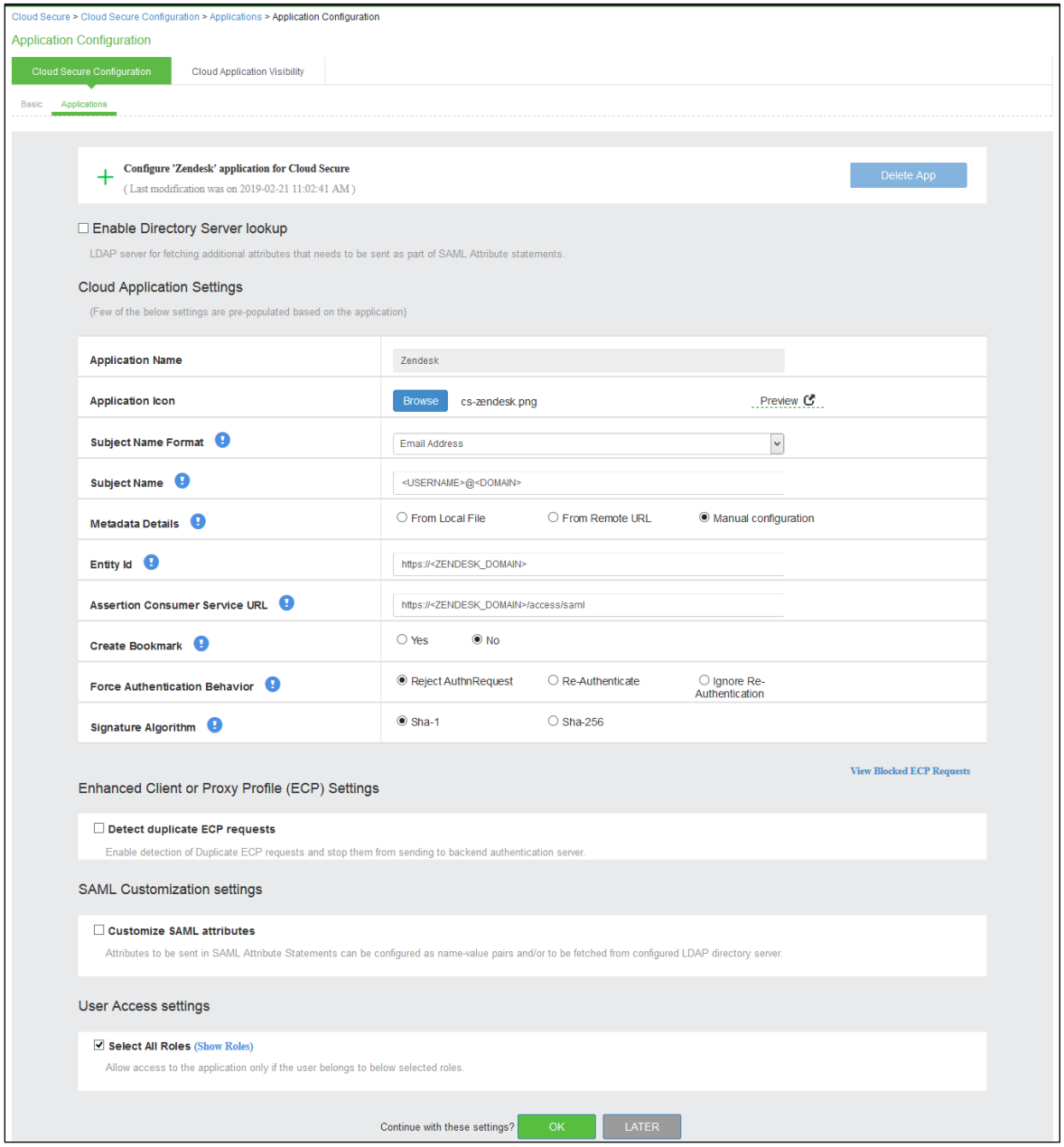
The Admin can configure the Zendesk Cloud Applications as Peer SP once the basic configurations are completed. The Zendesk application is available with some pre-populated application settings for ease of configuration.



To configure Zendesk application:

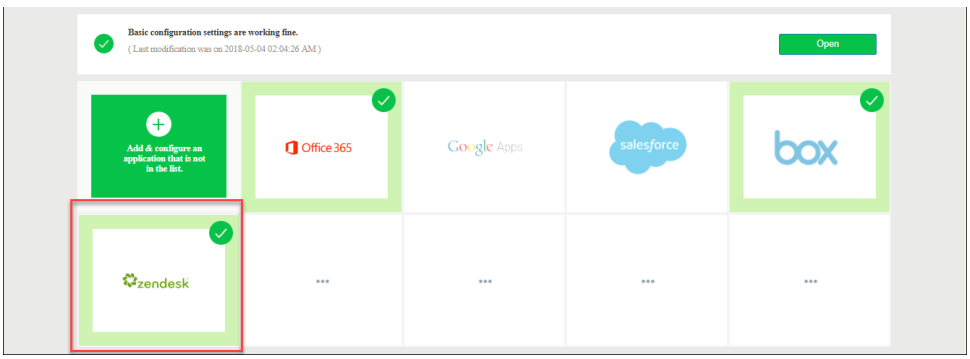
1. Click the **zendesk** icon to configure the application.
2. Under Cloud Application Settings:
   a. Enter the application name.
   b. Click Browse and select the application icon.
   c. Select the Subject Name Format =Email Address.
   d. Enter the Subject Name.
   e. Under Metadata details, select the manual configuration option for metadata details and provide the necessary details (Entity ID and ACS URL).
   f. (Optional) Set **Create Bookmark** to **Yes** to support IdP initiated SSO.
   g. Set the Force Authentication Behaviour to **Reject AuthnRequest**.
   h. Set the Signature Algorithm to Sha-1 or Sha-256.
3. Under **User Access settings**, assign the application to applicable roles.
4. Click **OK**.

Figure 1 Zendesk Application



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

Figure 2 Zendesk Configuration Completed



Zendesk Configuration

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

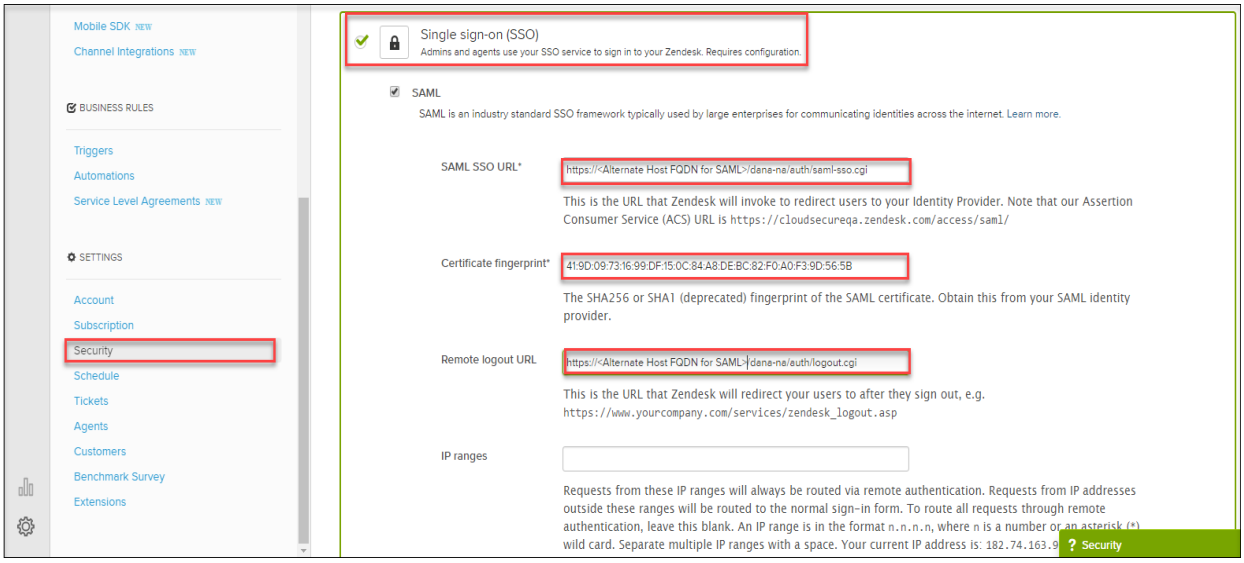
- Register with Zendesk and create a new Domain
- Configure SAML

Steps to Configure

Follow the below steps to configure Zendesk as a 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**.
4. Enable **Single sign-on (SSO)** and **SAML**.
5. Configure with the below details:
   a. SAML SSO URL = 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

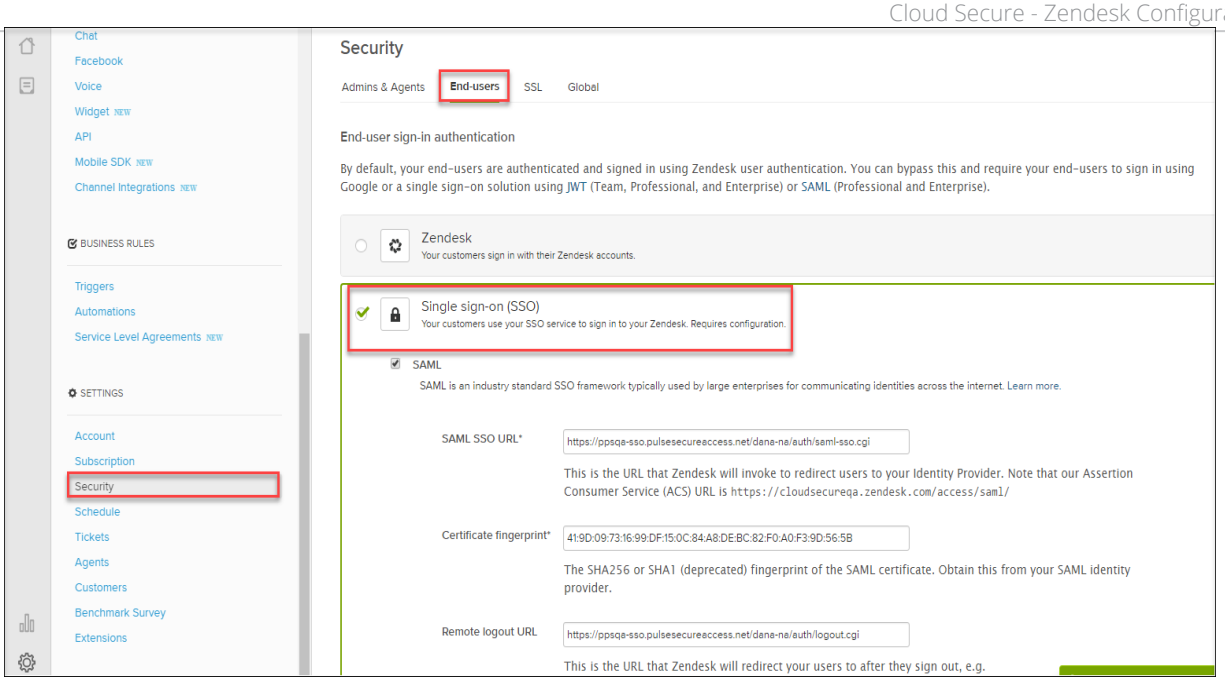
Figure 3 Enable SSO for Admin



6. Navigate to **Admin** (Settings gear at the bottom left corner) **> Security > End-users**.
7. Enable **Single sign-on (SSO).**

All the configurations made in Admin & Agents tab will get populated automatically.

Figure 4 Enable SSO for End-users



End-User Flow on Mobile Devices

Once the administrator completes the Zendesk 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 the 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 (Example: pulsesecure.zendesk.com)
8. With Single Sign-On, user will get access to Zendesk.

End-User Flow on Desktops

Once the administrator completes the Zendesk configurations, user can access Zendesk URL through browser from Windows/MAC OS X Desktops. Follow the below steps to enable Secure Single Sign-On browser-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 and access Zendesk URL.
    - 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.
    - 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.