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 – Okta 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 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
  Pre-requisites ..................................................................................................................................... 5
Pulse Connect Secure Configuration ........................................................................................................... 7
Okta Configuration .................................................................................................................................... 10
Zendesk Configuration ............................................................................................................................. 19
End-User flow on Mobile Devices ........................................................................................................... 21
End-User flow on Desktops ......................................................................................................................... 21
Troubleshooting ..................................................................................................................................... 22
List of Figures

Figure 1 Architecture Diagram ........................................................................................................ 6
Figure 2 New Metadata Provider ..................................................................................................... 8
Figure 3 Add Service Provider ........................................................................................................ 9
Figure 4 Inbound SAML .................................................................................................................. 10
Figure 5 Add Endpoint .................................................................................................................... 11
Figure 6 Download SAML Metadata .............................................................................................. 12
Figure 7 Add Application .................................................................................................................. 13
Figure 8 Add Zendesk ..................................................................................................................... 13
Figure 9 General Settings ............................................................................................................... 14
Figure 10 Enable SAML 2.0 ............................................................................................................. 15
Figure 11 Enable Provisioning Features .......................................................................................... 16
Figure 12 Assign People .................................................................................................................. 17
Figure 13 Enter user attributes ....................................................................................................... 18
Figure 14 Enable SSO for Admin .................................................................................................... 19
Figure 15 Enable SSO for End-users .............................................................................................. 20
Introduction

About this guide

Cloud Secure Solution provides Secure Single Sign-On for Cloud services using Okta as Identity Management Provider. In this federated solution, Okta acts as both Identity Provider (for Cloud services) and Service Provider (for Pulse Connect Secure). Inbound SAML capabilities of Okta allows users to authenticate to Okta using Pulse Connect Secure as external SAML Identity Provider to enable Secure Single Sign-On to Cloud applications.

This document provides configuration of Okta SP on Pulse Connect Secure, configuration of Zendesk Service Provider and Okta. 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 Okta and cloud service specific configurations outlined in this document. Basic configurations of PCS and PWS are covered as part of Common Components Configuration 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**: Okta
- **Clients**: iOS Device/ Android Device/ Windows/ MAC OS X Desktops
Figure 1 Architecture Diagram
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 Workspace
- 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, Okta should be configured as Service Provider on Pulse Connect Secure.

Follow below steps to configure Okta as Service Provider on Pulse Connect Secure:

1. Login to Pulse Connect Secure admin console.
2. Navigate to System-> Configuration-> SAML. Click on ‘New Metadata Provider’
   a. Provide Name
   b. Upload the downloaded Metadata file from Okta (Step 5 of Okta Configuration) by clicking Browse
   c. Enable Accept Unsigned Metadata
   d. Enable Service Provider under Roles
   e. Click Save Changes
3. Navigate to Authentication->Signing In->Sign-in SAML->Identity Provider. Click on ‘Add SP’ on the configuration page:

   a. Select Configuration mode as Metadata
   b. Select the Entity ID (the Entity ID will be Okta).
   c. 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)
   d. Assign required roles
   e. Click Save Changes
Figure 3 Add Service Provider
Okta Configuration

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

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

Steps to Configure

Follow below steps to configure Okta:

1. Signup for Okta developer account at https://www.okta.com/developer/signup
2. Login to Okta developer account and click ‘Admin’ on top right corner
3. Navigate to Security-> Authentication-> Inbound SAML. Click on ‘Add Endpoint’

*Figure 4 Inbound SAML*
4. Provide following details to configure Pulse Connect Secure as Identity Provider:

   a. **Alias** = <name reference to PCS>

   b. **IDP Certificate**:
      - 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)
      - Choose the IdP Signing Certificate configured under Authentication->Signing-in->Sign-in SAML->Identity Provider page of PCS and upload it here

   c. **IDP Issuer** = https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi

   d. **IDP Login URL** = https://<Alternate Host FQDN for SAML /dana-na/auth/saml-sso.cgi

   e. **IDP Binding** = HTTP-POST

   f. **Transform username** = username

   g. **Name ID Format** = Email Address

   h. **Select 'Enable SP initiated SAML'**

   i. **Click ‘Save Endpoint’**

   ![Figure 5 Add Endpoint](image)
5. After adding endpoint, Click on ‘Download SAML Metadata’ and save the xml file

Figure 6: Download SAML Metadata

6. To add Zendesk application in Okta for SSO, follow below steps:

   a. Navigate to Applications-> Applications

   b. Click on ‘Add Application’
c. Type Zendesk in search list and click on ‘Add’ on the Okta Verified Zendesk application

Figure 8 Add Zendesk
d. Provide your Zendesk domain details and Click 'Next'

*Figure 9 General Settings*
e. Select SAML 2.0 under Sign-On Options. Select ‘Email’ as Application username format under Advanced Sign-On Settings. Click on ‘View Setup Instructions’. It opens a new page with details of SAML configuration on Zendesk (To be referred to later). Click ‘Next’.

Figure 10 Enable SAML 2.0
f. Under Provisioning Settings, ‘Enable provisioning features’, provide *Zendesk admin credentials* and Click ‘Next’ at the end of the page. This is an optional configuration.

*Figure 11 Enable Provisioning Features*
g. Assign Zendesk to People. Click ‘Next’.

Figure 12 Assign People

h. Click ‘Done’ to complete the configuration
Figure 13 Enter user attributes

Note: To login to Okta developer account as admin without Single Sign-On, use https://<Okta Domain>/login/do-login
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)
   a. Configure SAML SSO URL
   b. Configure Certificate fingerprint
   c. Configure Remote logout URL

---

Figure 14 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.
End-User flow on Mobile Devices

Once administrator does the above configurations and creates a new user 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. 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 administrator does the above configurations, user can access Zendesk domain via browser from Windows/ MAC OS X Desktops. Follow 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
3. Access SSO enabled Zendesk domain
   a. If user has an existing VPN session, ‘Re-use existing Pulse Session’ will kick in and PCS will send SAML response to Okta
   b. If user did not establish Pulse VPN session as mentioned in Step 1, user will be redirected to Okta 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 Okta
4. Okta 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, Okta, 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.

- Login to Okta Domain as admin. Navigate to Dashboard-> Dashboard. Check the recent activity events to debug the failures.

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