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](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
PingOne Configuration ......................................................................................................................... 10
Zendesk Configuration ......................................................................................................................... 23
End-User flow on Mobile Devices ....................................................................................................... 25
End-User flow on Desktops ................................................................................................................... 25
Troubleshooting .................................................................................................................................... 26
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Architecture Diagram</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>New Metadata Provider</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Add Service Provider</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>Setup Identity Repository</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>Select Identity Repository</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Configure IDP Connection</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>Import IDP Metadata</td>
<td>13</td>
</tr>
<tr>
<td>8</td>
<td>Download PingOne Metadata</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>Add Application</td>
<td>15</td>
</tr>
<tr>
<td>10</td>
<td>Search Application Catalog</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>Setup Zendesk</td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td>SSO Instructions</td>
<td>17</td>
</tr>
<tr>
<td>13</td>
<td>Configure SSO</td>
<td>18</td>
</tr>
<tr>
<td>14</td>
<td>Attribute Mapping</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>Customize PingOne App</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>Review Setup</td>
<td>21</td>
</tr>
<tr>
<td>17</td>
<td>Download Signing Certificate</td>
<td>22</td>
</tr>
<tr>
<td>18</td>
<td>Enable SSO for Admin</td>
<td>23</td>
</tr>
<tr>
<td>19</td>
<td>Enable SSO for End-users</td>
<td>24</td>
</tr>
</tbody>
</table>
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 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**: PingOne
- **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, PingOne should be configured as Service Provider on Pulse Connect Secure.

Follow below steps to configure PingOne 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 PingOne (Step 7 of PingOne 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 PingOne).
   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
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 below steps to configure PingOne:

1. Signup for PingOne admin account at [https://admin.pingone.com/web-portal/login](https://admin.pingone.com/web-portal/login) and create your domain
2. Login to PingOne domain account as admin at [https://desktop.pingone.com/<Domain>](https://desktop.pingone.com/<Domain>)
3. Navigate to Setup-> Identity Repository. Click ‘Change Identity Repository’
4. Select ‘3rd Party SAML’ as Identity Repository. Click Next

Figure 5 Select Identity Repository

5. Select ‘Enable Account Specific Entity ID’. Click Next
6. Under ‘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)
7. Once the settings are saved, verify that all the PingOne Settings and SAML Settings are updated. Download PingOne SAML Metadata and save the file.
To add Zendesk application in PingOne for SSO, follow below steps:

a. Navigate to Applications-> My Applications

b. Click on ‘Add Application’, select ‘Search Application Catalog’
c. Type **Zendesk** in search list. Click on Zendesk application in the results.
d. Click **Setup**

Figure 11 Setup Zendesk

![Setup Zendesk]

```
Zendesk
```

e. Leave values to default and click ‘**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’
g. Under ‘Attribute Mapping’ section, leave default values and click ‘Continue to Next Step’
### Figure 14: Attribute Mapping

#### Application Name
- **Type**: SAML

<table>
<thead>
<tr>
<th>Application Attribute</th>
<th>Description</th>
<th>Identity Bridge Attribute or Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML_SUBJECT</td>
<td>mail</td>
<td>SAML_SUBJECT</td>
</tr>
<tr>
<td>displayName</td>
<td>The user's name to be used for display purposes.</td>
<td>Name or Literal</td>
</tr>
<tr>
<td>phone</td>
<td>A phone number, specified as a string.</td>
<td>Name or Literal</td>
</tr>
</tbody>
</table>

* Indicates a required attribute.

NEXT: PingOne App Customization - Zendesk

---

h. Click ‘Save and Publish’ in the next page
i. Review Setup and Click **Finish**
6. Review Setup

Test your connection to the application

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

You may need to configure these connection parameters as well.

saasid e9a1bcee-4f4c-4fe2-a5b8-e83d2a53491

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://ssao.connect.pingidentity.com/sso/sp/initso?saasid=e9a1bcee-4f4c-4fe2-a5b8-e83d2a53491&idpid=673b5ebc-e6ce-4326-a445-999c3f3dd8ab

Single Sign-On (SSO) Relay State https://pingone.com/1.0/e9a1bcee-4f4c-4fe2-a5b8-e83d2a53491

Single Logout Endpoint

Single Logout Response Endpoint

Force Re-authentication false

Signing Certificate Download

SAML Metadata Download

<table>
<thead>
<tr>
<th>Application Attribute</th>
<th>Description</th>
<th>Identity Bridge Attribute or Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SAML_SUBJECT</td>
<td>mail</td>
<td>SAML_SUBJECT</td>
</tr>
<tr>
<td>2 displayName</td>
<td>The user’s name to be used for display purposes.</td>
<td></td>
</tr>
<tr>
<td>3 phone</td>
<td>A phone number, specified as a string.</td>
<td></td>
</tr>
</tbody>
</table>

* Indicates a required attribute.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator_Email</td>
<td>The account email of an admin for your Zendesk account.</td>
<td></td>
</tr>
<tr>
<td>Zendesk_Api_Token</td>
<td>The API Token retrieved from Zendesk.</td>
<td>--------</td>
</tr>
<tr>
<td>Zendesk_Subdomain</td>
<td>The subdomain of your Zendesk account.</td>
<td></td>
</tr>
</tbody>
</table>
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 17 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 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 following values:
   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 18 Enable SSO for Admin](image-url)
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 19 Enable SSO for End-users*
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 PingOne
   b. 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.

- Login 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.