Cloud Secure – WebEx 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  
Pulse Connect Secure Configuration ........................................................................................................................................ 6  
WebEx Configuration ....................................................................................................................................................................... 9  
End-User flow on Mobile Devices ............................................................................................................................................. 12  
End-User flow on Desktops .......................................................................................................................................................... 13  
Troubleshooting ............................................................................................................................................................................ 14
List of Figures

Figure 1 New Metadata Provider .................................................................................................................. 7
Figure 2 Add Service Provider .................................................................................................................. 8
Figure 3 Import IdP Metadata .................................................................................................................. 10
Figure 4 SAML Configuration .................................................................................................................. 11
Introduction

About this guide

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

Follow below steps to configure WebEx SP on PCS:

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 WebEx (Step 3h of WebEx Configuration) by clicking Browse
   c. Enable Accept Unsigned Metadata
   d. Enable Service Provider under Roles
   e. Click Save Changes
Figure 1 New Metadata Provider

New Metadata Provider

Name: WebEx

Location: [Local] [Remote]

Upload Metadata File: Browse
WebEx_metadata.xml
Current File: None

Accept Unsigned Metadata

Signing Certificate:
Issued To:
Issued By:
Valid:
Details: [Other Certificate Details]

Upload Certificate: Browse [No file chosen] Delete

Enable Signing Certificate status checking

(Uses configuration in Trusted Client CAs. This applies to the certificate configured above as well as the one coming along with the metadata.)

Metadata Provider Filter Configuration

Roles:
[ ] Identity Provider
[ ] Service Provider
[ ] Policy Decision Point

List of entity ids to import, one per line. If left empty all entity ids in the file are imported.

Entity Ids to import:

Save Changes  Cancel
3. 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 **Metadata**
   b. Select the **Entity ID** (the Entity ID will be the WebEx domain)
   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 2 Add Service Provider*
WebEx Configuration

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

- Register with WebEx and enable SSO privileges for the WebEx domain
- Configure SAML

Steps to Configure

Follow below steps to configure WebEx as Service Provider:

1. Register with WebEx and create a new domain. Enable SSO privileges for the domain
2. Login to WebEx domain as admin at https://<WebEx Domain>/admin
3. Navigate to Configuration-> Common Site Settings-> SSO Configuration. Configure below details:
   a. Federation Protocol = SAML 2.0
   b. SSO Profile = SP Initiated
   c. Click Import SAML Metadata
   d. Choose PCS SAML Metadata file and click Import (To download PCS Metadata file, navigate to Authentication->Signing-in->Sign-in SAML->Metadata Provider and click on ‘Download Metadata’ on PCS admin console)
   e. ‘Issuer for SAML (IdP ID)’ and ‘Customer SSO Service Login URL’ will get populated automatically
f. To configure the values manually, provide following details:
   - Issuer for SAML (IdP ID) = https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi
   - Customer SSO Service Login URL = https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi

g. Configure following values in rest of the mandatory fields:
   - WebEx SAML Issuer (SP ID) = https://<WebEx Domain>
     (Ex: https://pulsesecure.webex.com)
   - NameID Format = Email address
   - AuthnContextClassRef = urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
   - Select 'Single Logout'. Configure Customer SSO Service Logout URL = https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi. This is an optional configuration
   - Click Update
h. Once the configuration is saved, click on Export to export WebEx SP Metadata file. Save the file.
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 WebEx 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 WebEx 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 WebEx Application, click on 'Sign In' and provide the email details
8. Single Sign-On will happen and user will get access to WebEx
End-User flow on Desktops

Once administrator does the above configurations, user can access WebEx URL via browser from Windows/MAC OS X Desktops. Follow below steps to enable Secure Single Sign-On browser-based access to WebEx Cloud Service:

1. Launch Pulse Client and establish a VPN session with PCS
2. Open any web browser on the desktop, access WebEx URL (Ex: https://pulsesecure.webex.com)
   a. If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in, PCS will send SAML response to WebEx SP and user will be granted access to WebEx 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 WebEx SP and user will be granted access to WebEx Cloud Service
Troubleshooting

Single Sign-On for a WebEx user can fail due to configuration issues on Pulse Connect Secure, WebEx 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.