Cloud Secure – WebEx

Configuration Guide

Document Revisions 3.0

Published Date December 2018

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

https://www.pulsesecure.net

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 – WebEx Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

Contents

Introduction

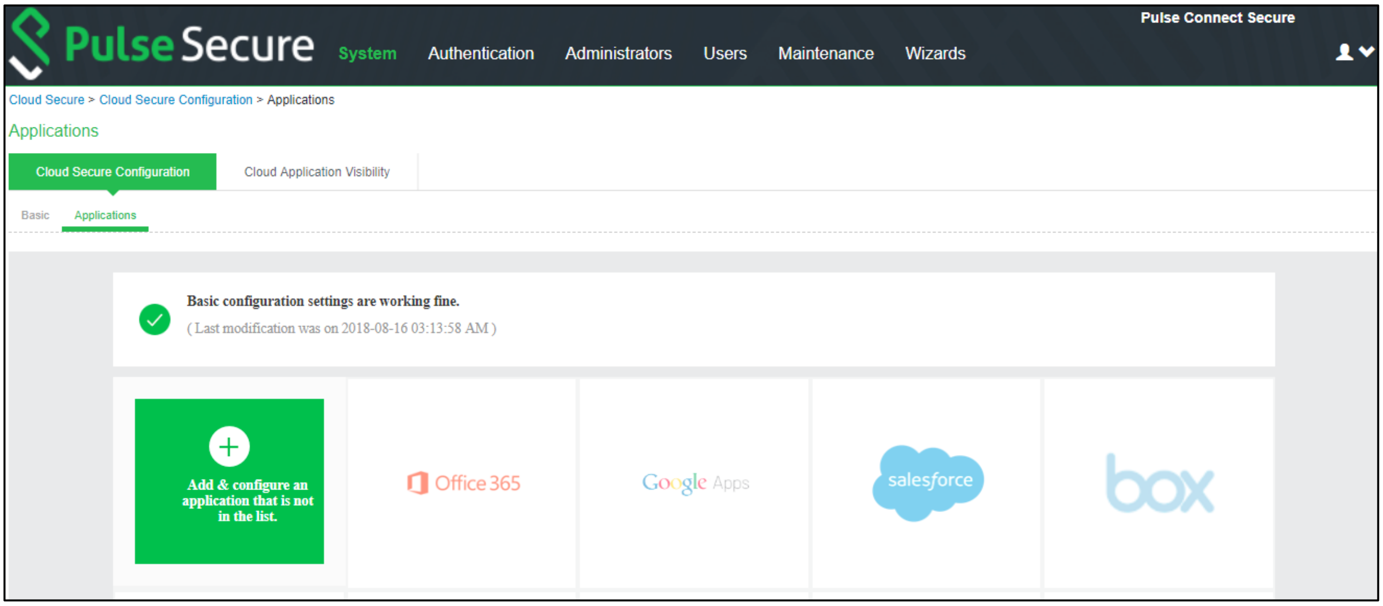
This document describes the configuration required on WebEx cloud service and configuration of WebEx Service Provider on Pulse Connect Secure to provide Secure Single Sign-on access to WebEx users. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace (PWS)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

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 Webex Cloud Applications as Peer SP once the basic configurations are completed. Click the Add & configure an application that is not in the list to configure Webex as it is not available by default.

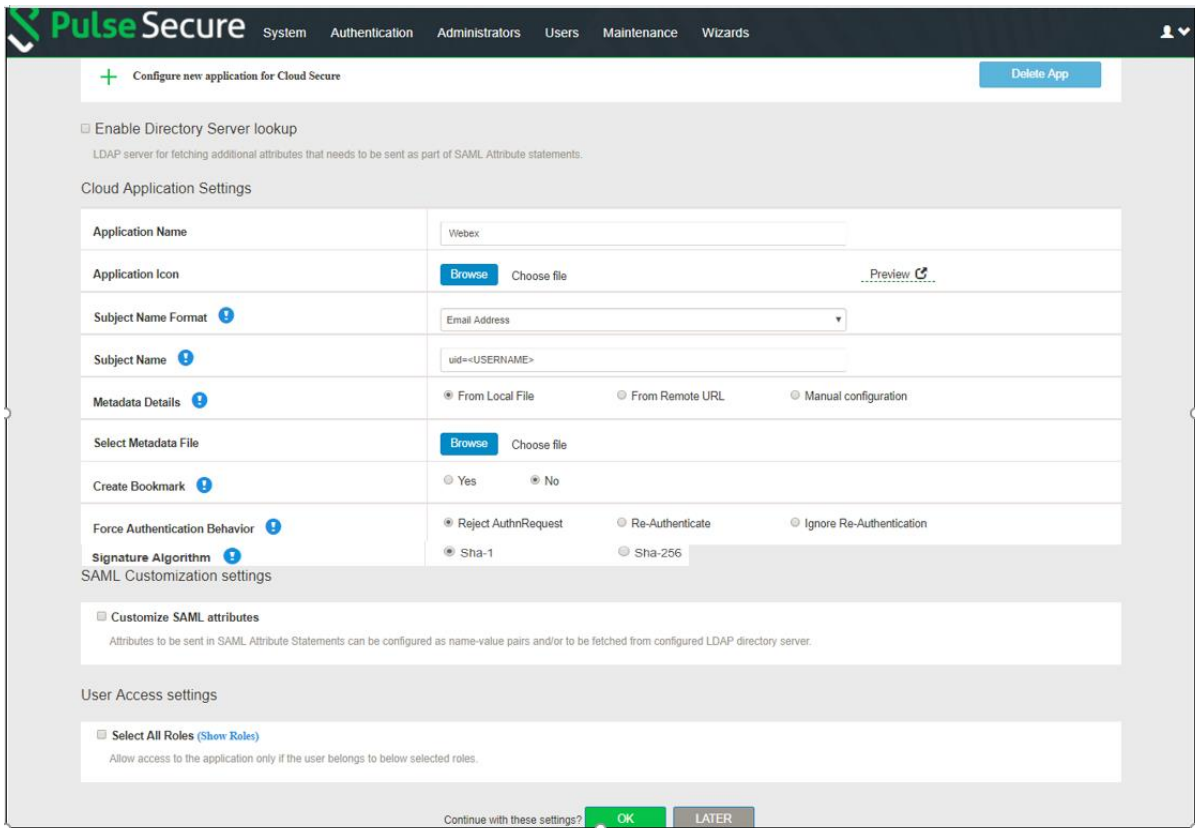

Pulse Secure
Pulse Connect Secure
System
Authentication
Administrators
Users
Maintenance
Wizards
Cloud Secure > Cloud Secure Configuration > Applications
Applications
Cloud Secure Configuration
Cloud Application Visibility
Basic
Applications
Add & configure an application that is not in the list.
Office 365
Google Apps
salesforce
box

Basic configuration settings are working fine.
(Last modification was on 2018-08-16 03:13:58 AM)

To configure Webex application:

1. Click the Add & configure an application that is not in the list 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, upload the metadata through a local file.
   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 Add Webex Application



Configure new application for Cloud Secure

□ Enable Directory Server lookup

LDAP server for fetching additional attributes that needs to be sent as part of SAML Attribute statements.

Cloud Application Settings

Application Name	Webex
Application Icon	Browse Choose file Preview
Subject Name Format	Email Address
Subject Name	uid=<USERNAME>
Metadata Details	● From Local File ○ From Remote URL ○ Manual configuration
Select Metadata File	Browse Choose file
Create Bookmark	○ Yes ● No
Force Authentication Behavior	● Reject AuthnRequest ○ Re-Authenticate ○ Ignore Re-Authentication
Signature Algorithm	● Sha-1 ○ Sha-256

SAML Customization settings

□ Customize SAML attributes

Attributes to be sent in SAML Attribute Statements can be configured as name-value pairs and/or to be fetched from configured LDAP directory server.

User Access settings

□ Select All Roles (Show Roles)

Allow access to the application only if the user belongs to below selected roles.

Continue with these settings? OK LATER

WebEx Configuration

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

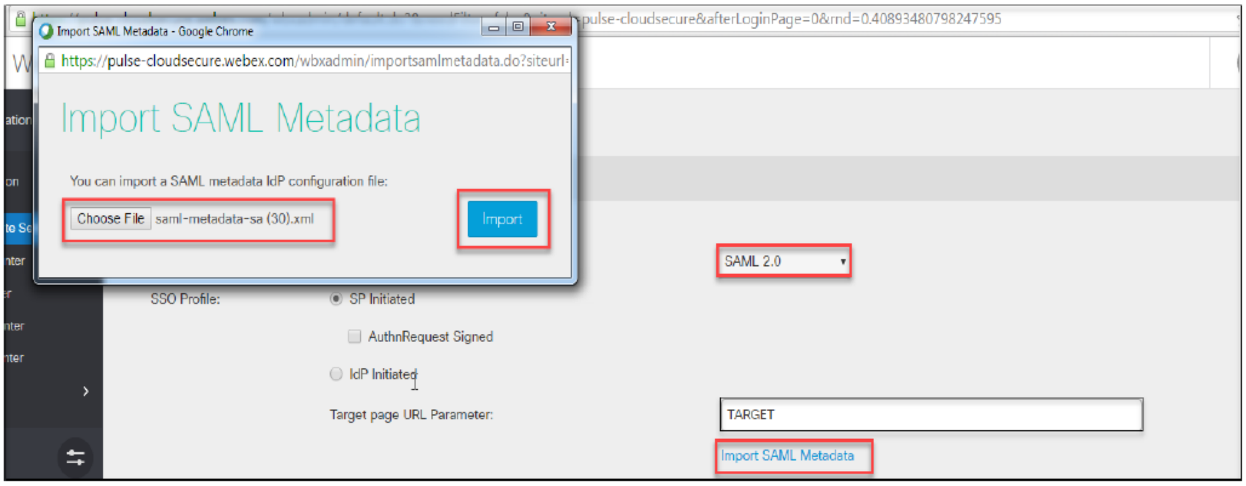
- Register with WebEx and enable SSO privileges for the WebEx domain
- Configure SAML

Steps to Configure

To configure WebEx as Service Provider, do the following:

1. Register with WebEx and create a new domain. Enable SSO privileges for the domain.
2. Log in to WebEx domain as admin at https://<WebEx Domain>/admin.
3. Navigate to **Configuration > Common Site Settings > SSO Configuration**. Configure with the 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 **Download Metadata** on PCS admin console).
   e. The **Issuer for SAML (IdP ID)** and **Customer SSO Service Login URL** will get populated automatically.

Figure 1 Import IDP Metadata



Import SAML Metadata - Google Chrome

https://pulse-cloudsecure.webex.com/wbxadmin/importsamlmetadata.do?siteurl=

Import SAML Metadata

You can import a SAML metadata IdP configuration file:

Choose File saml-metadata-sa (30).xml

SAML 2.0

SSO Profile: ● SP Initiated

□ AuthnRequest Signed

○ IdP Initiated

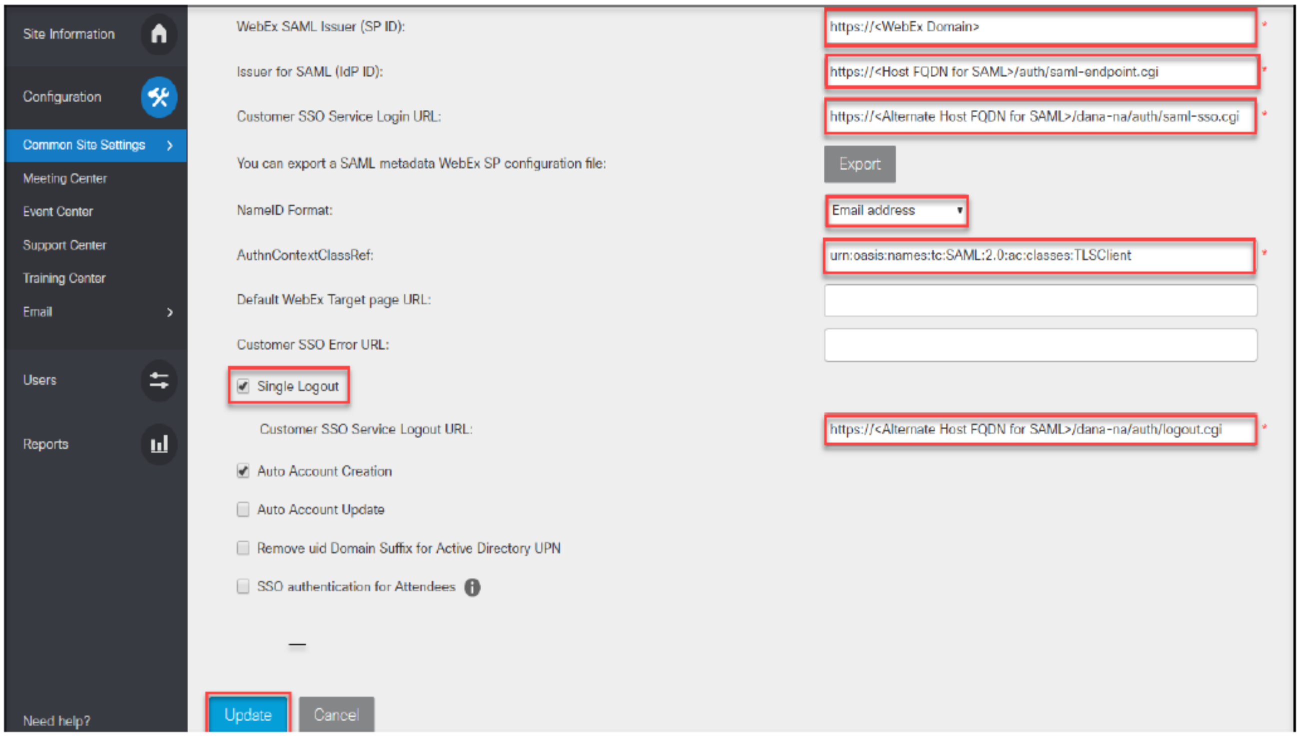
Target page URL Parameter: TARGET

   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> (Example: 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**.

Figure 2 SAML Configuration



WebEx SAML Issuer (SP ID): https://<WebEx Domain> *

Issuer for SAML (IdP ID): https://<Host FQDN for SAML>/auth/saml-endpoint.cgi *

Customer SSO Service Login URL: https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi *

You can export a SAML metadata WebEx SP configuration file:

NameID Format: Email address

AuthnContextClassRef: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient *

Default WebEx Target page URL:

Customer SSO Error URL:

☑ Single Logout

Customer SSO Service Logout URL: https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi *

☑ Auto Account Creation

☐ Auto Account Update

☐ Remove uid Domain Suffix for Active Directory UPN

☐ SSO authentication for Attendees

h. Once the configuration is saved, click **Export** to export WebEx SP Metadata file and save the file.

End-User Flow on Mobile Devices

Once the administrator completes the WebEx configurations and creates a new user if not present in Pulse Workspace, user has to follow the 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 the 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 Sign In and provide the email details.
8. Single Sign-On will happen and user will get access to the WebEx.

End-User Flow on Desktops

Once the administrator completes the WebEx configurations, user can access WebEx url through browser from Windows/MAC OS X Desktops. Follow the 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 (Example: https://pulsesecure.webex.com).
    a. If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in. The 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, then the 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.