Pulse Secure®

Cloud Secure – Box

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

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 – Box Configuration Guide

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

END USER LICENSE AGREEMENT

Introduction

About This Guide

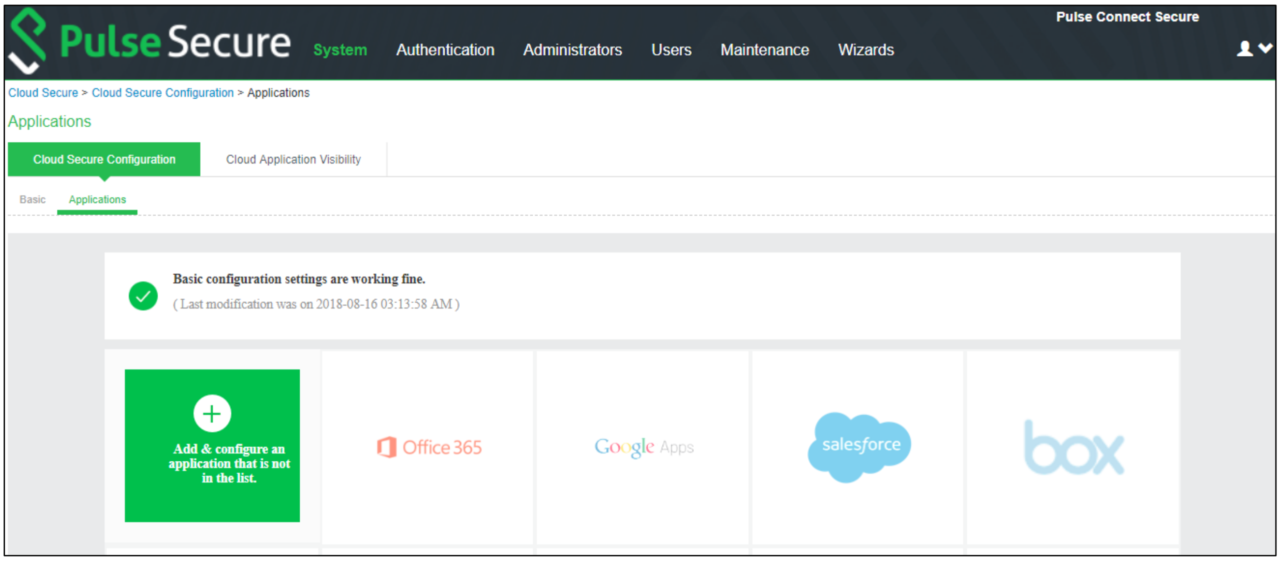
This document describes how to enable SAML configuration on Box cloud service and configuration of Box Service Provider on Pulse Connect Secure to provide Secure Single Sign-on access to Box users. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace (PWS) 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 Box Cloud Applications as Peer SP once the basic configurations are completed. The Box application is available with some pre-populated application settings for ease of configuration.

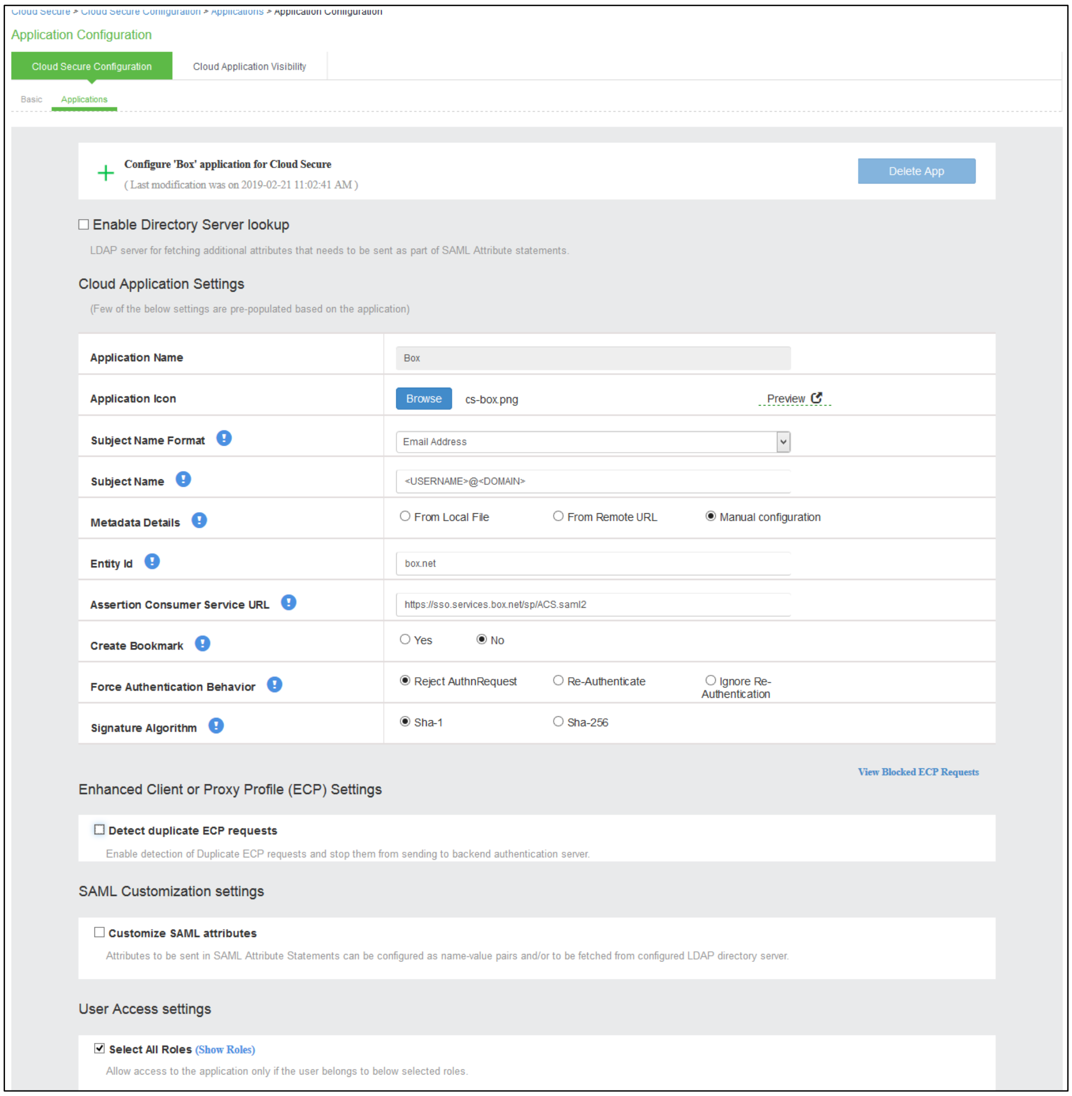

Pulse Secure
Pulse Connect Secure
System
Authentication
Administrators
Users
Maintenance
Wizards
Cloud Secure > Cloud Secure Configuration > Applications
Applications
Cloud Secure Configuration
Cloud Application Visibility
Basic
Applications
Add & configure an application that is not in the list.
Office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

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

To configure Box application:

1. Click the Box 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. Select the manual configuration 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 Signature Algorithm to Sha-1 or Sha-256.
3. Under User Access settings, assign the application to applicable roles.
4. Click OK.

Figure 1 Box Application


Cloud Secure > Cloud Secure Configuration > Applications > Application Configuration
Cloud Secure Configuration
Cloud Application Visibility
Basic
Applications
Delete App
Browse
Preview
View Blocked ECP Requests

Application Configuration

Configure 'Box' application for Cloud Secure
(Last modification was on 2019-02-21 11:02:41 AM)

□ Enable Directory Server lookup

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

Cloud Application Settings

(Few of the below settings are pre-populated based on the application)

Application Name	Box
Application Icon	cs-box.png
Subject Name Format	Email Address
Subject Name	<USERNAME>@<DOMAIN>
Metadata Details	○ From Local File ○ From Remote URL ● Manual configuration
Entity Id	box.net
Assertion Consumer Service URL	https://sso.services.box.net/sp/ACS.saml2
Create Bookmark	○ Yes ● No
Force Authentication Behavior	● Reject AuthnRequest ○ Re-Authenticate ○ Ignore Re-Authentication
Signature Algorithm	● Sha-1 ○ Sha-256

Enhanced Client or Proxy Profile (ECP) Settings

□ Detect duplicate ECP requests

Enable detection of Duplicate ECP requests and stop them from sending to backend authentication server.

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.

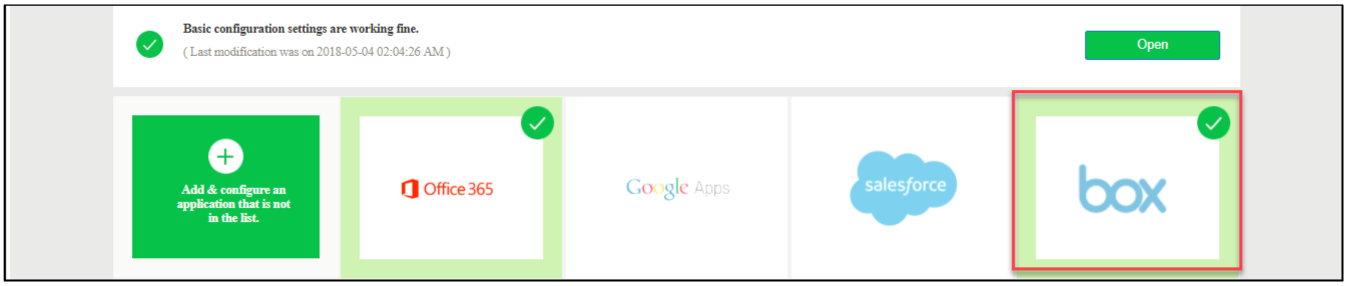
User Access settings

☑ Select All Roles (Show Roles)

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

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

Figure 2 Box Configuration Completed



Basic configuration settings are working fine.
(Last modification was on 2018-05-04 02:04:26 AM)

Box Configuration

Box should be enabled as SAML Service Provider for supporting Single Sign-On. Unlike most other cloud services, admin is not provided with the option to configure Box SP. You need to submit a case with Box for any SP side configuration once you have Box Business account. To submit SSO configuration request on Box SP, log in to your Box account and file a case with Box support at https://community.box.com/t5/custom/page/page-id/submit_sso_questionaire

Fill the form with following details:

- Leave default value in the **Subject** field.
- Select **Yes** or **No** for **Do you have a Box Consulting package?** ('No' in most cases).
- Provide Box domain in the **Company Box domain** field (Example: https://pulsesecure3.app.box.com).
- Select **Other with metadata** for **Who is your Identity Provider?**
- In the Required Information section, click **Choose File** and browse to your Pulse Connect Secure (PCS) Metadata file. To download PCS SAML Metadata:
    - Log in to PCS admin console.
    - Navigate to **Authentication** > **Signing In** > **Sign-in SAML** > **Metadata Provider**, and click **Download Metadata**.
- Provide 'emailAddress' in the **SAML Attribute: User's Email:** field.
- Submit the request.
- Mention in the request as a comment that SP should be configured to look for SAML_SUBJECT attribute in SAML Assertion as PCS sends email property in SAML_SUBJECT.

Once the request is submitted, Box support team will get back on options you would like to be enabled on your account:

- SSO Required
- SSO auto-provisioning (users who authenticate through your SSO provider, but do not have a Box account will have one automatically created for them)
- Auto roll-in (users who try to sign up for a free Box account with your company's email domain will be prompted to join your company's enterprise; only possible if SSO auto-provisioning is also enabled)

You can choose to have all the options enabled.

Note: It may take up to 3 weeks to process the request for SSO setup if you do not have an ctive consulting package.

End-User Flow on Mobile Devices

Once the administrator completes the Box configurations and creates a new user in Pulse Workspace, user has to follow below steps to register iOS/Android mobile device with Pulse Workspace and get seamless secure Single Sign-On access to Box 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 Box 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 Box Application: select Use Single Sign On (SSO) and provide Box email address.
8. With Single Sign-On, user will get access to the Box domain.

End-User Flow on Desktops

Once the administrator completes the Box configurations, user can access Box domain through browser or thick application from Windows/MAC OS X Desktops. Follow the below steps to enable Secure Single Sign-On browser-based/thick app based access to Box Cloud Service.

1. Launch Pulse Client and establish a VPN session with PCS
2. Open any web browser on the desktop, access Box domain and provide Box email address or access Box thick application and provide Box email address.
    - If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in. The PCS will send SAML response to Box SP and user will be granted access to Box Cloud Service.
    - 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 Box SP and user will be granted access to Box Cloud Service.

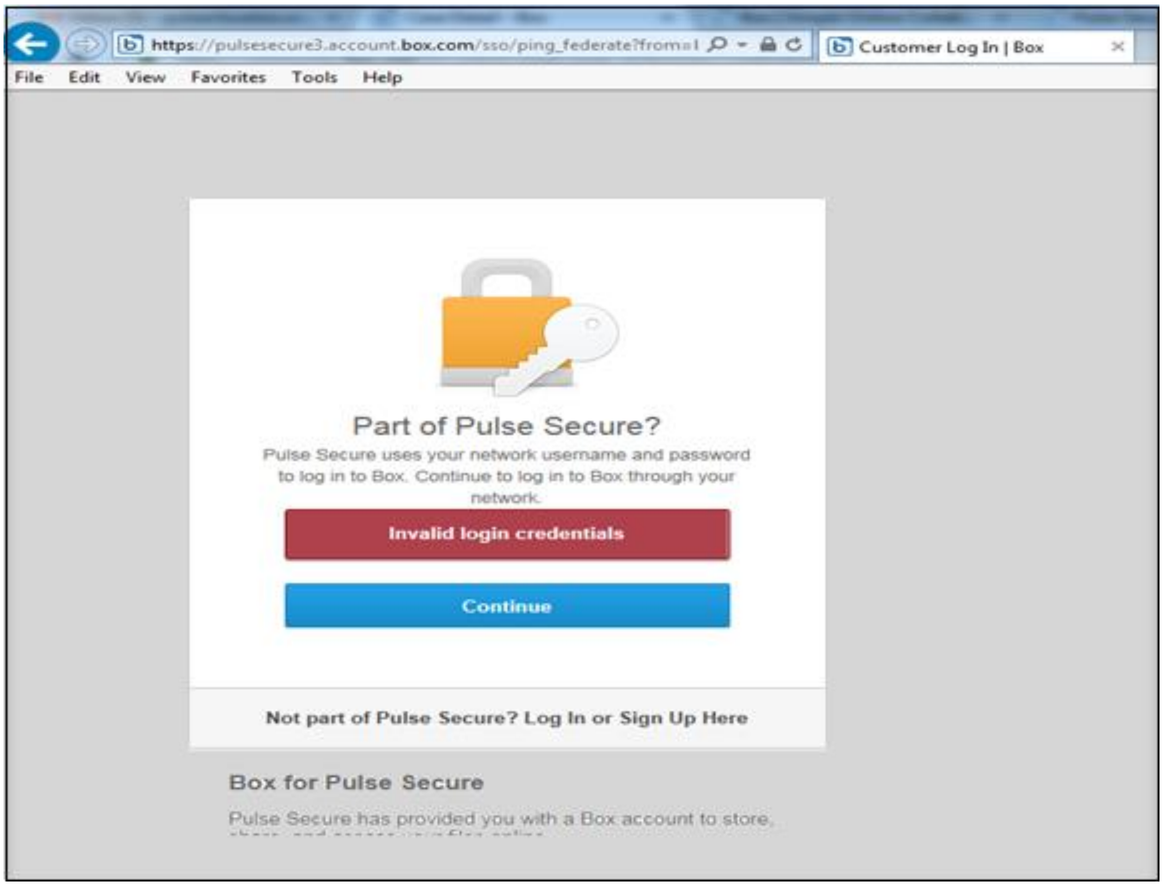
Troubleshooting

Single Sign-On for a Box user can fail due to configuration issues on Pulse Connect Secure, Box 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.
- If user receives ‘Invalid login credentials’ error while trying to do SSO with Box account even though PCS successfully sent SAML response, this could be an issue with SAML Configuration on Box SP (if Box configuration mentioned in last step of the details to be filled in the form for filing a request to set up SSO is not done). Box SP looks for the ‘emailaddress’ attribute in SAML Assertion. PCS sends email property in SAML_SUBJECT. To resolve this issue, SP should be configured to look for SAML_SUBJECT attribute in SAML Assertion. Submit a request with Box support for this configuration change.

Figure 3 Invalid Login Credentials


https://pulsesecure3.account.box.com/sso/ping_federate?from=l
Customer Log In | Box
File
Edit
View
Favorites
Tools
Help
Invalid login credentials
Continue
Not part of Pulse Secure? Log In or Sign Up Here

Part of Pulse Secure?

Pulse Secure uses your network username and password to log in to Box. Continue to log in to Box through your network.

Box for Pulse Secure

Pulse Secure has provided you with a Box account to store,