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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>About this guide</td>
<td>5</td>
</tr>
<tr>
<td>Pulse Connect Secure Configuration</td>
<td>6</td>
</tr>
<tr>
<td>Box Configuration</td>
<td>8</td>
</tr>
<tr>
<td>End-User flow on Mobile Devices</td>
<td>9</td>
</tr>
<tr>
<td>End-User flow on Desktops</td>
<td>10</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>11</td>
</tr>
</tbody>
</table>
List of Figures

Figure 1 Add Service Provider.................................................................................................................. 7
Figure 2 Invalid Login Credentials............................................................................................................ 11
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. 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, Box should be configured as Service Provider on Pulse Connect Secure.

Follow below steps to configure Box SP on PCS:

1. Login to Pulse Connect Secure admin console

2. 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 Manual
   b. Entity ID = box.net
   c. Assertion Consumer Service URL = https://sso.services.box.net/sp/ACS.saml2
   d. Select ‘Post’ binding
   e. 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)
   f. Assign required roles
   g. Click Save Changes

Note: These are standard settings for all Box accounts unlike other Service Providers which are specific to organization
Figure 1 Add Service Provider

**New Peer Service Provider**

- **Configuration Mode**: Manual
- **Entity ID**: box.net
- **Assertion Consumer Service URL**: https://sso.services.box.net/sp/ACS.saml2
- **Post**: checked
- **Certificate Status Checking Configuration**:
  - Enable signature verification certificate status checking
  - Enable encryption certificate status checking
- **Customize IdP Behavior**: Overwrite Default Configuration
- **Roles**:
  - Policy applies to ALL roles
  - Policy applies to SELECTED roles
  - Policy applies to roles OTHER THAN those selected below
  - Available roles: iOS Users, iOS/Android Users, Remediation, SAP, Users
  - Selected roles: (none)

**Save Changes**
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, login 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 ‘Subject’ field
- Select ‘Yes’ or ‘No’ for ‘Do you have a Box Consulting package?’ (‘No’ in most cases)
- Provide Box domain in ‘Company Box domain’ field (Ex: https://pulsesecure3.app.box.com)
- Select ‘Other with metadata’ for ‘Who is your Identity Provider?’
- In the ‘Required Information’ section, click on ‘Choose File’ and browse to your Pulse Connect Secure (PCS) Metadata file. To download PCS SAML Metadata:
  - Login to PCS admin console
  - Navigate to Authentication-> Signing In-> Sign-in SAML-> Metadata Provider, click ‘Download Metadata’
- Provide ‘emailAddress’ in ‘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 active consulting package
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 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 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. Single Sign-On will happen and user will get access to the Box domain
End-User flow on Desktops

Once administrator does the above configurations, user can access Box domain via browser or thick application from Windows/MAC OS X Desktops. Follow 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
   a. If user has an existing VPN session, ‘Re-use existing Pulse Session’ will kick in,
      PCS will send SAML response to Box SP and user will be granted access to Box 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 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 successful 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 setup SSO is not done). Box SP looks for attribute ‘emailaddress’ 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 2 Invalid Login Credentials*