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

http://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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 – Common Components 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
  Enable PCS as SAML IDP server ................................................................................................. 7
  Establish Connection between PCS and MDM .............................................................................. 12
  Enable secure connectivity between PCS and Pulse Client ......................................................... 15
  Configure Secure access from end user devices .......................................................................... 17
  Generating X509 Certificates ....................................................................................................... 28

**Pulse Workspace Configuration** .................................................................................................. 29
List Of Figures

Figure 1 Task Guide .............................................................................................................. 7
Figure 2 Task Guide – Step 1 .................................................................................................. 8
Figure 3 Device Certificate ................................................................................................... 9
Figure 4 SAML Settings ........................................................................................................ 10
Figure 5 Identity Provider ...................................................................................................... 11
Figure 6 Task Guide – Step 2 ................................................................................................ 12
Figure 7 Trusted Client CA ................................................................................................... 13
Figure 8 Pulse One Settings .................................................................................................. 14
Figure 9 MDM Server ........................................................................................................... 15
Figure 10 Task Guide – Step 3 ................................................................................................ 15
Figure 11 Certificate Server .................................................................................................. 16
Figure 12 Task Guide – Step 4 ................................................................................................ 17
Figure 13 Configure User Role for L4 VPN ......................................................................... 18
Figure 14 SAM Allowed Servers ......................................................................................... 19
Figure 15 Configure User Realm .......................................................................................... 20
Figure 16 Configure Role Mapping Rules .............................................................................. 21
Figure 17 SAM Resource Policy .......................................................................................... 22
Figure 18 Cloud Secure Configuration .................................................................................. 23
Figure 19 Configure User Role for L3 VPN ......................................................................... 24
Figure 20 Split Tunnel Rules ................................................................................................. 25
Figure 21 Enable Split Tunneling .......................................................................................... 26
Figure 22 Connection Profile ................................................................................................ 27
Figure 23 Add Policy ............................................................................................................. 29
Figure 24 Modify VPN Properties ......................................................................................... 30
Figure 25 Add Application ..................................................................................................... 31
Figure 26 Create New User .................................................................................................. 32
Figure 27 Register PCS ........................................................................................................ 32
Figure 28 VPN Cert ............................................................................................................... 33
Introduction

About this guide

Cloud Secure solution provides Single Sign-On for various SAML Service Provider services. For this it requires Pulse Connect Secure to be configured as SAML Identity Provider and Pulse Workspace as Mobile Device Management (MDM) Server. This document describes the basic configurations and SAML configuration required on Pulse Connect Secure to provide Secure Single Sign-On access to any cloud service. This document also specifies the detailed configuration required on Pulse Workspace for Cloud Secure solution. Beyond this basic configurations, each Service Provider specific additional configuration is covered in their respective Service Provider application configuration documents.
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

Steps to Configure

Follow below steps to configure Pulse Connect Secure (PCS) as Identity Provider:

1. Login to Pulse Connect Secure admin console
2. Navigate to System-> Network-> Internal Port| External Port-> Settings. Configure External and Internal interfaces of PCS

Note: Pulse VPN tunnel will be established with External Interface of PCS and users accessing SAML SSO enabled cloud service will be redirected to Internal Interface of PCS for authentication.

Enable PCS as SAML IDP server

In the Task Guide, click first step ‘Enable PCS as SAML IDP server’ as shown in Figure 1. List of all steps required to configure PCS as SAML IDP server will be displayed.
4. Click **System -> Configuration -> Certificate -> Device Certificate** under **Step 1 as shown in Figure 2** to import IDP device certificate. Admin will be redirected to Device Certificates page. Import wildcard or Subject Alternative Name (SAN) device certificate that will be used for signing SAML messages sent by PCS. Disassociate External Port if used by any other certificate and map External Port to the imported device certificate.
5. Click **System -> Configuration -> SAML -> Settings** under *Step 2 as shown in Figure 2* to configure SAML Settings. Admin will be redirected to SAML Settings page. Configure following details:
   a. Enter **Host FQDN for SAML** (for example: cs.pulsesecure.net)
   b. Enter **Alternate Host FQDN for SAML** (for example: cs-sso.pulsesecure.net)
   c. Click **Save Changes**
   d. Click **Update Entity Ids**

**Note:** Host FQDN for SAML is DNS Host name for External Port IP and Alternate Host FQDN for SAML is DNS Host name for Internal Port which is configured in *Step 2* above. Alternate Host FQDN for SAML is used to redirect user to IDP login URL provided in Service Provider.
6. Click **Authentication -> Signing In -> Sign-in SAML -> Identity Provider** under  [Step 3 as shown in Figure 2](#) to configure Identity Provider. Admin will be redirected to Identity Provider configuration page. Configure following details:
   a. Enable ‘Post’ Binding
   b. Select Device certificate uploaded in **Step a** above as Signing Certificate
   c. Enable ‘Reuse Existing NC(Pulse) Session’ and ‘Accept Unsigned AuthnRequest’
   d. Select SignIn Policy used to authenticate the user (Example: */)
   e. Under User Identity, select Email Address as Subject Name format and provide Subject Name as `<USERNAME>@<DOMAIN>`
      (Example: `<USERNAME>@pulsesecure.net`)
   f. Click **Save Changes**

**Note:** Subject Name is used to identify a specific user in the Service Provider. Most of the Service Providers use ‘Email Address’ as the NameIdentifier
Figure 5 Identity Provider

![Identity Provider Configuration](image)

**Basic Identity Provider (IDP) Configuration (Published in Metadata)**

- **Post**
- **Artifact**
- **Signing Certificate:** *pulsesecureqa.net*
- **Decryption Certificate:** No Encryption

**Service-Provider-related IDP Configuration**

- **Relay State:**
- **Session Lifetime:**
  - None
  - Role Based
  - Customize
- **Signin Policy:**
- **Force Authentication Behavior:**
  - Reject AuthnRequest
  - Re-Authenticate User
- **User Identity**
  - **Subject Name Format:** Email Address
  - **Subject Name:** `<USERNAME>@pulsesecure.net`

**Attribute Statement Configuration**

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

**Name-Value based configuration**, here values can be system variables available in SSO parameter fields:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Friendly Name</th>
<th>Attribute Value</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The value can contain mixed characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>.

Examples:
- `<USER>` The user's login name
- `<REALM>` The user's sign-in realm
- `<ROLE_SEP>` For a comma separated list of roles.

Mark an element as Multi-valued if it should be sent as a multi-valued attribute, in this case multiple tokens in an attribute value will be sent as individual values.

**Directory server based configuration**

<table>
<thead>
<tr>
<th>Directory Server</th>
<th>Select a directory server: Visit the Servera page to create or manage Directory server</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Establish Connection between PCS and MDM

Click ‘Return to the previous guide’ in the Task Guide. Click second Step ‘Establish Connection between PCS and MDM’ of Task Guide as shown in Figure 1. List of all steps required to establish connection between PCS and MDM Server will be displayed

Figure 6 Task Guide – Step 2

7. Click System -> Configuration > Certificates > Trusted Client CAs under Step 1 as shown in Figure 6 to import Pulse One VPN Certificate. Admin will be redirected to Trusted Client CAs page. Click ‘Import CA Certificate’; browse to the Pulse Workspace VPN Certificate downloaded in Step 2 of Pulse Workspace Configuration and click ‘Import Certificate’
8. Click **System -> Configuration > Pulse One > Settings** under Step 2 as shown in Figure 2 to register PCS with Pulse One
   
a. Provide **Registration Host** and **Registration Code** details from Step 7 of Pulse Workspace Configuration
   
b. Click **Save Changes**
   
c. Registration Status and Notification Channel Status under Status Information section should turn green after few seconds
9. Click Authentication -> Auth Servers under **Step 2 as shown in Figure 6** to create Pulse Workspace MDM Authentication Server. Select New Server of Type ‘MDM Server’. Click on New Server.
   a. Provide Name
   b. Select ‘Pulse Workspace’
   c. Click Save Changes

**Note:** MobileIron and AirWatch Third-Party MDM Servers can also be used as device attribute servers on user realm for device compliance checks
Enable secure connectivity between PCS and Pulse Client

Click ‘Return to the previous guide’ in the Task Guide. Click third Step ‘Enable secure connectivity between PCS and Pulse Client’ of Task Guide as shown in Figure 1. List of all steps required to enable secure connection between PCS and Pulse Client will be displayed.

Figure 10  Task Guide – Step 3
10. Click **Authentication** → **Auth Servers** under *Step 1 as shown in Figure 10* to configure Certificate Authentication Server. Select New Server of Type ‘Certificate Server’. Click on **New Server**.

   a. Provide **Name**
   b. Click **Save Changes**

*Figure 11 Certificate Server*
Configure Secure access from end user devices

Click 'Return to the previous guide' in the Task Guide. Click fourth Step ‘Configure Secure access from end user devices’ of Task Guide as shown in Figure 1. List of all steps required to configure Pulse Connect Secure to enable end users to make connection with PCS will be displayed.

Figure 12 Task Guide – Step 4

11. Click Users -> User Roles under Step 1 as shown in Figure 12 to configure user role. Select the desired role or create a new user role and configure following options:

   a. Select Pulse Secure Client
   b. Select Secure Application Manager and select Windows Version for L4/WSAM tunnel (Applicable to iOS/Desktops)
   c. Click Save Changes
   d. To configure WSAM Split tunneling rules, navigate to SAM tab under user role. Click on Add Server and enter the following details as shown in Figure 14
      - Enter Name to identify the server
      - Enter Allowed Server and Ports (Internal Port IP created in Step 2. For example, if Internal Port is 1.1.1.1, configure Allowed Server as 1.1.1.1/32:*).
Figure 13 Configure User Role for L4 VPN
12. Click Users -> User Realms under Step 2 as shown in Figure 12 to configure user realm. Select the desired realm or create a new user realm and configure following options:
   a. Select Certificate Server created in Step 10 for Authentication
   b. Select Pulse Workspace MDM Server created in Step 9 as Device Attribute Server
   c. Click Save Changes
   d. Navigate to Role Mapping tab of the user realm and configure role mapping rules. Create New Rule based on Device attribute for managed mobile clients. Create another role mapping rule based on other available options to be applied to Desktop clients. To create rule based on Device Attribute:
      - Select Rule based on Device attribute and Click Update
      - Provide Name
      - Select an Attribute and provide a value
      - Assign required roles
      - Click Save Changes
Figure 15 Configure User Realm
13. Click **Authentication -> Signing In -> Sign-in Policies** under **Step 4 as shown in Figure 12** to configure Sign-in policy. Assign user realm configured in above step to the desired sign-in policy or create a new sign-in policy and map the user realm

14. Click **Users -> Resource Policies > Secure Application Manager Policies** under **Step 5 as shown in Figure 12** to configure SAML Resource Access Policy. Click on ‘New Policy’ and create a new policy allowing all the resources applicable (Internal Port as configured in **Step 2**), assign require roles and Save Changes

**Note:** Compliance checks with MDM Server is applicable only for mobile devices. For desktops, classic Host Checker functionality can be used for compliance checks. Hence, Device Attribute Server configuration is not applicable for realms used for authenticating Desktop users
15. Click **Authentication -> Signing In -> Sign-in SAML -> Identity Provider** under [Step 6 as shown in Figure 12](#) to update Sign-in Policy for SAML. Select the Sign-in policy configured in [Step 6](#) above.

16. Once all the above configurations are done, navigate to **System -> Cloud Secure -> Cloud Secure Configuration** and verify if status of all the sections under Basic Settings is changed to ‘Configured’ and ‘Progress Completed’ bar is 100%.
17. To configure L3 VPN instead of L4 VPN, skip Step 11 and following below steps:

i. Navigate to Users > User Roles > <ROLE> or create a new role to configure user role with L3 VPN tunneling. Configure following options:
   a. Select Pulse Secure Client
   b. Select VPN Tunneling for L3 VPN (Applicable to iOS/Android/Desktops)
   c. Click Save Changes
Figure 19: Configure User Role for L3 VPN

**Overview**

- **Name:** Users
- **Description:** System created Users role.

**Options**

- VLAN/Source IP (Edit)
- Session Options (Edit)
- UI Options (Edit)
- **Pulse Secure client**

**Access features**

- Web
- Files, Windows
- Files, UNIX/NFS
- Telnet/SSH
- Secure Application Manager
  - Windows version
  - Java version
- Terminal Services
- Virtual Desktops
- HTML5 Access
- Meetings
- **VPN Tunneling**
- Secure Mail

Save Changes
ii. To configure L3 VPN Split tunneling rules, navigate to Users-> Resource Policies-> VPN Tunneling-> Split-tunneling Networks. Create a new policy and provide following details
   a. Provide Name
   b. Resources applicable (Internal Port as configured in Step 2)
   c. Apply the policy to required Roles
   d. Click Save Changes

*Figure 20 Split Tunnel Rules*
iii. Navigate to **VPN Tunneling** of desired user role and configure following details:
   a. **Enable** split tunneling mode
   b. **Select** Tunnel Routes
   c. **Click** Save Changes

![Figure 21 Enable Split Tunneling](image)

iv. To configure connection profile, navigate to **Users-> Resource Policies-> VPN Tunneling-> Connection Profiles**. Create a new connection profile and provide following details:
   a. Provide **Name**
   b. Select **DHCP Server** and provide DHCP Server IP Address or select **IPv4 Address Pool** and provide the IP pool
Figure 22 Connection Profile

Connection Profile

* Name: VPN Connection Profile

IPv4 address assignment

DHCP servers
Specify the name or IPv4 addresses for up to 3 DHCP servers:
10.209.112.2

DHCP options
Specify any DHCP options that should be sent to the DHCP Server. Enter the option number, option value, and option value type. Option values can be token replaced values.
Note: Please refer to Admin Guide for more details.

IPv4 address pool
Specify the assignable IPv4 address ranges for this profile, one per line.
Note: Please refer to Admin Guide for details.

IPv6 address assignment
Connection Settings
DNS Settings
Proxy Server settings
Roles

Save Changes
Save as Copy
Generating X509 Certificates

As part of Single Sign-On configuration, IDP certificate may have to be imported on Service Provider depending on the requirement of different cloud services.

To generate this X509 certificate, follow below steps:

1. Login to Pulse Connect Secure admin console
2. Navigate to Authentication-> Signing In-> Sign-in SAML-> Metadata Provider. Click on Download Metadata.
   An XML file (saml-metadata-sa.xml) will be downloaded.
3. Copy the certificate content (Content in <ds:X509Certificate> tag) from the XML file into a text file. Certificate metadata should be copied in the following format
   -----BEGIN CERTIFICATE-----
   <cert data>
   -----END CERTIFICATE-----
   Save the file in .der format to be used in Step 5 below.
4. Download OpenSSL and install on your client. An alternative to this is to use OpenSSL which is already available in Mac OS X.
5. Run the following command to generate a '.cer' extension certificate out of '.der' file:
   OpenSSL x509 -in <cert path> -outform der -out newcert.cer
6. Upload this newly generated certificate in Service Provider as IDP certificate

---

**Note:** X509 Certificate can be generated only after completion of the Pulse Connect Secure Identity Provider configuration
Pulse Workspace Configuration

Pulse Workspace acts as Mobile Device Management (MDM) Server to manage mobile devices and also to evaluate compliance posture of the devices. For Cloud Secure solution, Pulse Workspace should be configured with:

- Policy configured with VPN properties and iOS/Android applications enabled with Per app VPN
- Workspace user
- PCS appliance

Steps to Configure

Follow the below steps to configure Pulse Workspace for Cloud Secure:

1. Login to the Pulse One admin console
2. Use existing Global policy or create a new policy. To create new policy, select Policies -> Add
   a. Enter ‘Policy name’
   b. Enter ‘Has user tags’
   c. Click Save

3. Modify the VPN properties of new policy or Global policy to support Per App VPN. Navigate to ‘Properties’ tab. Scroll down to ‘VPN’ section, click the Edit icon against each field below and provide following values:
   a. Set ‘Use L3 VPN’ to true (in case of L3 VPN)
   b. VPN Host = https://<Alternate Host FQDN for SAML>
   c. VPN Safari Domains = <Alternate Host FQDN for SAML> (Required for iOS devices)
   d. Select VPN Type ‘Pulse SSL’
   e. Leave rest of the fields to defaults and Click on ‘Publish’
Note: Android devices support only L3 VPN whereas iOS devices support both L3 and L4 VPN

Figure 24 Modify VPN Properties

4. Select the ‘iOS App Rules’/‘Android App Rules’ tab under the policy created.
5. Click Add to add new application.
   a. Enter the application name in the search list (Salesforce1, Zendesk, Box etc), select the application and Click Next
   b. Select ‘Per app VPN’/‘Require VPN’ for Network Access
   c. Click Save
Figure 25 Add Application

6. Navigate to Workspaces tab. Click on Actions-> ‘Add User’ to create a new user if user does not exist. Provide following details
   a. Enter Username
   b. Enter Workspace Email. Provision Email will get populated automatically
   c. Enter Policy name created in Step 2 as Tags if required (else, Global policy will be assigned by default)
   d. Click Create
7. Select the **Appliances** tab. Click ‘**Add Appliance**’ and provide a name to register Pulse Connect Secure with Pulse One. Admin will be provided with Registration Host and Registration code details to be configured in PCS.

8. Click the **Settings** gear on the top right corner of the page.

9. Click ‘**VPN Cert**’ and then click the ‘**cert**’ link to download Pulse One VPN certificate, which needs to be uploaded in PCS as Trusted Clients CA.
Figure 28 VPN Cert