Cloud Secure

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

https://www.pulsesecure.net.

© 2016 by Pulse Secure, LLC. All rights reserved.

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 Deployment 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/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

**Table of Contents** .................................................................................................................... 3  
**List of Figures** ............................................................................................................................ 4  
**Introduction to Cloud Secure** ..................................................................................................... 5  
  - Overview ...................................................................................................................................... 5  
  - Products Briefing ........................................................................................................................... 5  
  - Salient Features of Cloud Secure .................................................................................................. 6  
  - End-User Platform Support Matrix ............................................................................................... 6  
  - Third Party Integration Support ................................................................................................... 7  
**Deployment Scenarios** .................................................................................................................. 8  
  - Deployment using Web Browser SSO Profile ................................................................................ 8  
  - Deployment using Enhanced Client or Proxy (ECP) Profile ........................................................... 9  
  - Deployment using Third Party IDP ............................................................................................. 10  
**Configurations** ............................................................................................................................ 11  
  - Configuring Pulse Connect Secure ............................................................................................. 11  
    - Steps to Configure .................................................................................................................. 11  
    - Enable PCS as SAML IDP Server ............................................................................................. 12  
    - Establish Connection between PCS and MDM ......................................................................... 16  
    - Enable Secure Connectivity between PCS and Pulse Client .................................................... 18  
    - Configure Secure Access from End User Devices ..................................................................... 19  
    - Configure Service Provider on PCS ......................................................................................... 29  
    - Configuring Compliance Failure Notification .......................................................................... 30  
    - Configuring Role Based Access Control .................................................................................. 31  
    - Configuring Pulse Connect Secure for Android/iOS Users and Desktop Users ......................... 32  
  - Configuring Pulse Workspace ..................................................................................................... 40  
    - Steps to Configure .................................................................................................................. 40  
  - Configuring Salesforce ................................................................................................................ 44  
    - Steps to Configure .................................................................................................................. 44  
  - End-User Flow on Mobile Devices .............................................................................................. 47  
  - End-User Flow on Desktops ......................................................................................................... 48  
**Dashboard** .................................................................................................................................... 49  
**Troubleshooting** .......................................................................................................................... 52  
  - Mobile Devices (iOS/Android) ..................................................................................................... 52  
  - Desktops ..................................................................................................................................... 53  
  - Pulse Connect Secure ................................................................................................................ 53  
  - Pulse Workspace ...................................................................................................................... 53  
  - Troubleshooting TIPS ................................................................................................................ 53  
  - Service Provider Specific Troubleshooting ............................................................................... 56  
    - Pulse Connect Secure ........................................................................................................... 56  
    - End User Device .................................................................................................................... 56  
**Requesting Technical Support** ..................................................................................................... 57
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Secure Sign-on to SaaS</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Secure Sign-On to Office365 using ECP</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Secure Sign-On using Third Party IDP</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Task Guide</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>Task Guide – Step 1</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>Device Certificate</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>SAML Settings</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>Identity Provider</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>Task Guide – Step 2</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>Trusted Client CA</td>
<td>16</td>
</tr>
<tr>
<td>11</td>
<td>Pulse One Settings</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>MDM Server</td>
<td>18</td>
</tr>
<tr>
<td>13</td>
<td>Task Guide – Step 3</td>
<td>18</td>
</tr>
<tr>
<td>14</td>
<td>Certificate Server</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>Task Guide – Step 4</td>
<td>19</td>
</tr>
<tr>
<td>16</td>
<td>Configure User Role for L4 VPN</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>SAM Allowed Servers</td>
<td>21</td>
</tr>
<tr>
<td>18</td>
<td>Configure User Realm</td>
<td>22</td>
</tr>
<tr>
<td>19</td>
<td>Configure Role Mapping Rules</td>
<td>22</td>
</tr>
<tr>
<td>20</td>
<td>SAM Resource Policy</td>
<td>23</td>
</tr>
<tr>
<td>21</td>
<td>Cloud Secure Configuration</td>
<td>24</td>
</tr>
<tr>
<td>22</td>
<td>Configure User Role for L3 VPN</td>
<td>25</td>
</tr>
<tr>
<td>23</td>
<td>Split Tunnel Rules</td>
<td>26</td>
</tr>
<tr>
<td>24</td>
<td>Enable Split Tunneling</td>
<td>27</td>
</tr>
<tr>
<td>25</td>
<td>Connection Profile</td>
<td>28</td>
</tr>
<tr>
<td>26</td>
<td>New Metadata Provider</td>
<td>29</td>
</tr>
<tr>
<td>27</td>
<td>Add Service Provider</td>
<td>30</td>
</tr>
<tr>
<td>28</td>
<td>Compliance Failure Notification</td>
<td>31</td>
</tr>
<tr>
<td>29</td>
<td>Role Based Access Control</td>
<td>32</td>
</tr>
<tr>
<td>30</td>
<td>Active Directory Server</td>
<td>33</td>
</tr>
<tr>
<td>31</td>
<td>Host Checker - Windows Rule</td>
<td>34</td>
</tr>
<tr>
<td>32</td>
<td>Host Checker - Mac Rule</td>
<td>34</td>
</tr>
<tr>
<td>33</td>
<td>Configure Host Checker on Role</td>
<td>35</td>
</tr>
<tr>
<td>34</td>
<td>Configure Desktop Realm</td>
<td>36</td>
</tr>
<tr>
<td>35</td>
<td>Configure HC Custom Expression</td>
<td>37</td>
</tr>
<tr>
<td>36</td>
<td>Mobile Realm Browser Restrictions</td>
<td>38</td>
</tr>
<tr>
<td>37</td>
<td>Desktop Realm Browser Restrictions</td>
<td>39</td>
</tr>
<tr>
<td>38</td>
<td>Add Policy</td>
<td>40</td>
</tr>
<tr>
<td>39</td>
<td>Modify VPN Properties</td>
<td>41</td>
</tr>
<tr>
<td>40</td>
<td>Add Application</td>
<td>42</td>
</tr>
<tr>
<td>41</td>
<td>Create New User</td>
<td>43</td>
</tr>
<tr>
<td>42</td>
<td>Register PCS</td>
<td>43</td>
</tr>
<tr>
<td>43</td>
<td>VPN Cert</td>
<td>44</td>
</tr>
<tr>
<td>44</td>
<td>Enable SAML</td>
<td>45</td>
</tr>
<tr>
<td>45</td>
<td>Configure Service Provider</td>
<td>46</td>
</tr>
<tr>
<td>46</td>
<td>Authentication Configuration</td>
<td>46</td>
</tr>
<tr>
<td>47</td>
<td>Create User</td>
<td>47</td>
</tr>
<tr>
<td>47</td>
<td>Dashboard Settings</td>
<td>49</td>
</tr>
<tr>
<td>48</td>
<td>Dashboard</td>
<td>51</td>
</tr>
</tbody>
</table>
Introduction to Cloud Secure

Overview

Emerging technologies like mobile and cloud are defining the next chapter of IT strategy, Hybrid IT, where enterprises are combining the best of the cloud with their own localized data centers.

Cloud Secure is designed to securely provide workers anytime access to Hybrid IT environments. Out of the box features, like single sign-on (SSO), eliminate workers need for multiple passwords and provide automatic access to applications and services they need. Cloud Secure solution integrates Pulse Connect Secure - VPN, Identity Provider and Pulse Workspace – with EMM Solution for user authentication and device compliance to provide secure access to data center and cloud.

In addition, Cloud Secure inter-operates with third party identity and access management (IAM) vendors for added service flexibility. Meanwhile, industry compliance is ensured by Pulse Secure's host-checking capabilities that assess the status and health of the user's devices. Pulse Workspace also ensures that mobile workers store apps and data in a secure container under enterprise control.

Cloud Secure provides secure, seamless and compliant access to SaaS and data center applications. It provides the following benefits:

- **Cloud Adoption** - Cloud Secure enables secured use of popular cloud offerings including Google Apps for Work, Office 365, Salesforce, Box and Dropbox.
- **Seamless User Experience** - Simplify user access to the data center and cloud with SSO from mobile devices and laptops.
- **Compliance and Control for Cloud Services** - Grant cloud service access based on user authentication and device security posture.
- **Simplified Administration** - Centrally manage access policies for SaaS, cloud and data center applications and services.

Products Briefing

Cloud Secure is a solution that integrates multiple Pulse Secure products for seamless secure access to hybrid IT environment.

- **Pulse Connect Secure (PCS)** - Pulse Connect Secure provides Layer 3 VPN connectivity with granular access control and wide array of authentication mechanisms. The PCS also acts as a SAML Identity Provider (IDP) and provides Single Sign-On functionality for Cloud Secure.
- **Pulse Workspace (PWS)** - Pulse Workspace acts as the MDM Server for Cloud Secure solution. Cloud secure users have to register their mobile devices with Pulse Workspace. As part of registration, the relevant Profiles and Cloud Apps get automatically provisioned to mobile device to enable Secure Single Sign On capability on that mobile device.
- **Pulse Secure VPN Client** - Pulse Secure Client provides VPN connectivity based on authentication and SSL/IPSEC encryption between the user's device and PCS. Pulse Secure Client enables secure connectivity to corporate applications and resources based on identity, realm and role. Pulse Secure VPN Client is supported on both desktop (Windows, Mac OSX) and mobile (iOS and Android) platforms. Cloud Secure delivers per application VPN connectivity for mobile devices, enabling IT teams to create more transparent and highly secure mobile app experience for their mobile users. The significant benefit of the Cloud Secure solution is that all these happen seamlessly in the background without user's VPN client initiation, which enhances the usability of the VPN access.
Salient Features of Cloud Secure

Cloud Secure harmonizes the need for Enterprises to cater to BYOD requirements with the desired levels of Enterprise Security and Mobile Device Management (MDM). Cloud Secure provides secure pathways and mechanisms to realize a highly user-centric architecture for Enterprise Customers using Cloud-based applications.

A few key features of Cloud Secure are:

- **Single Sign-on (SSO)** - Cloud Secure supports Security Assertion Markup Language (SAML) 2.0 based Single-Sign-On (SSO) that allows pre-authenticated users to access application or resources that are protected by access management system without re-entering their credentials.

- **Compliance for Cloud** - Using Pulse Secure host checking technologies, Cloud Secure verifies compliance of Windows and Mac OSX devices. Cloud Secure also integrates with Pulse Workspace and third party MDM vendors such as MobileIron and AirWatch to verify compliance of mobile devices. Compliance verification of devices ensure that only authorized users with trusted devices have secure access to Cloud resources and Data center.

- **Mobile-Ready** - Cloud Secure integrates with Pulse Workspace and leading EMM solutions for compliance enforcement and for BYOD container security.

- **Extensible Identity Management** - Pulse Connect Secure can also serve as a SAML Identity Provider (IDP) enabling easy integration with the third party identity management providers.

- **Scalable Connectivity** - Cloud Secure eliminates data center hair pinning by only sending authorization and compliance checks to Pulse Connect Secure and sending application data directly to the cloud. This avoids performance bottlenecks since user data traffic is not passing through PCS.

- **Role Based Access Control** - PCS supports Role Based Access Control through roles and resource access policies. PCS uses this framework to provide access control of resources based on the assigned roles. Cloud Secure supports Role Based Access Control feature to provide access control for cloud services based on the assigned roles. If an end user is not authorized to access the cloud service based on the assigned role, access to cloud service is denied and access denial message is sent to the end user.

- **Compliance Failure Notification** - When an end user tries to access cloud service from non-compliant device, the cloud service access is denied. This feature sends a notification message to the end user when cloud service access is denied because of compliance failure.

End-User Platform Support Matrix

Cloud Secure is supported on the following end-user platforms for seamless cloud services access:

- iOS 9.x onwards
- Android with APW support (5.1.1 onwards)
- Windows 7, Windows 8, Windows 8.1, and Windows 10
- Mac 10.11 onwards
Third Party Integration Support

Cloud Secure provides great level of flexibility with integration to various third party vendors as mentioned below:

- **MDM Vendors** – In the Cloud Secure solution, the third party MDM servers can be used for administration and compliance posture assessment of the mobile devices. Cloud Secure seamlessly integrates with third party MDM servers to provide Secure Single Sign-On for configured SaaS applications from compliant mobile devices. Cloud Secure supports integration with AirWatch and MobileIron.

- **IDP Vendors** – Cloud Secure solution provides Secure Single Sign-On for Cloud Services using third party SAML Identity Provider (IDP). In this integrated solution, third party IDPs act as both IDP (for Cloud Services) and SP (for PCS). Cloud Secure solution supports integration with IDPs such as Ping Identity and Okta.
Deployment Scenarios

For different deployment scenarios, Cloud Secure uses Security Assertion Markup Language (SAML) for exchange of authentication information between client device (Mobile, Desktops, and other devices), Service Provider (Cloud applications like Office 365, Salesforce etc.) and Identity Provider (Pulse Connect Secure) to provide SSO.

SAML Profiles - A SAML profile describes how SAML assertions, protocols, and bindings combine to support a defined use case. The most important SAML profile is the Web Browser SSO Profile.

Deployment using Web Browser SSO Profile

In SAML Web Browser SSO Profile, an endpoint web browser is used to exchange SAML messages between endpoint, SP and IDP. Here the web browser requests for a service from the service provider. As part of the authentication flow, Service Provider requests and receives an identity assertion from the Identity Provider through the browser. Before providing identity assertion to SP, the IDP requests web user for the credentials to authenticate the web user.

Figure 1 Secure Sign-on to SaaS

For web browser SSO, Pulse VPN client on mobile or desktop is used to deliver strong authentication and device compliance check. On mobile devices, cloud applications can be configured with per-app VPN client which is launched automatically when cloud application tries to access cloud service. On desktop, Pulse client may be connected manually by an end user. On mobile devices, users authenticate using certificates to eliminate the need to enter password. For mobile device compliance check, Pulse Workspace or third party MDM servers such as MobileIron or AirWatch is used. Pulse client host checker is used for desktop device’s compliance check. Once authentication and compliance check are completed successfully, application data flows directly between the endpoint and the service provider.
Deployment using Enhanced Client or Proxy (ECP) Profile

The Enhanced Client or Proxy (ECP) is similar to web browser SSO, but it is designed for applications other than browsers. Here, instead of exchanging SAML messages over user’s browser, SP and IDP communicate directly.

**Figure 2 Secure Sign-On to Office365 using ECP**

The native outlook applications on mobile devices use ECP profile (unlike web browser SSO profile) for authentication. For ECP profile, Cloud Secure solution uses the unique token generated by Pulse Workspace for authentication and to retrieve device compliance details. As part of the mobile device registration, Pulse Workspace generates and provisions unique token to mobile device. Once mobile device gets registered, the native outlook application is automatically provisioned to connect to Office 365 using the username and unique token. This generates a login request to Office 365. Upon receiving a login request, Office 365 delegates the authentication responsibility to PCS by providing user name and unique token through ECP. PCS verifies the user and checks the device compliance through PWS using this unique token. Once authentication and compliance check are successful, PCS provides an assertion to Office 365, which provides an email access to native outlook application.
Deployment using Third Party IDP

Cloud Secure also provides Secure Single Sign-On for cloud services by integrating with third party Identity Providers. Cloud Secure supports integration with Third Party IDPs such as Ping Identity and Okta. For Cloud Secure Solution, the Third Party IDPs act as IDPs for cloud services and act as SP for PCS (as IDP). Here users get authenticated by the Third Party IDPs using PCS as an external SAML IDP to provide Secure Sign-On to cloud applications.

*Figure 3 Secure Sign-On using Third Party IDP*
Configurations

This section covers the configurations required on different components involved in Cloud Secure solution. It also describes the end user flow on managed mobile devices and desktops.

For Cloud Secure solution, admin needs to configure Pulse Connect Secure as SAML Identity Provider, Cloud Service (For example, Salesforce) as SAML Service Provider and Pulse Workspace as Mobile Device Management (MDM) Server.

Configuring Pulse Connect Secure

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 using Cloud Secure Configuration Guidance pages:

1. Log in 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 on the first step ‘Enable PCS as SAML IDP server’ as shown in Figure 4. 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 5* 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 the PCS. Disassociate External Port if used by any other certificate and map it to the imported device certificate.

*Figure 6 Device Certificate*

5. Click **System > Configuration > SAML > Settings** under Step 2 as shown in *Figure 5* to configure SAML Settings. Admin will be redirected to the SAML Settings page. Configure the 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.

Figure 7 SAML Settings

6. Click Authentication > Signing In > Sign-in SAML > Identity Provider under Step 3 as shown in Figure 5 to configure Identity Provider. Admin will be redirected to Identity Provider configuration page. Configure the following details:
   a. Enable 'Post' binding.
   b. Select the 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
Figure 8 Identity Provider

[Image of PulseSecure Sign-In page]

- **Protocol** to use for SAML Response:
  - [ ] Post
  - [x] Artifact

- **Signing Certificate**: pulseeuropeqa.net
- **Encryption Certificate**: No Encryption

- **Service Provider-related IdP Configuration**
  - Relay State:
  - *Session Lifetime:
    - [ ] None
    - [ ] Role Based
    - [x] Customize

- **Sign-in Policy**: */
- **Force Authentication Behavior**:
  - [ ] Reject AuthnRequest
  - [ ] Re-Authenticate User

- **User Identity**
  - *Subject Name Format**: Email Address
  - *Subject Name*: <USERNAME>@pulseeurope.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 values can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this `<variable>`. Examples:
- `<USERNAME>`: The user's login name
- `<REALM>`: The user's realm
- `<ROLE>`: A comma separated list of roles.
- `<ROLE>`: A comma separated list of roles.

**Directory server based configuration**

- Directory Server: None

Select a directory server. Visit the `Servers` page to create or manage directory servers.
Establish Connection between PCS and MDM

To establish connection between PCS and MDM:

Click ‘Return to the previous guide’ in the Task Guide. Click Step 2 ‘Establish Connection between PCS and MDM’ of Task Guide as shown in Figure 4. List of all steps required to establish connection between PCS and MDM Server will be displayed.

7. Click System > Configuration > Certificates > Trusted Client CAs under Step 1 as shown in Figure 9 to import Pulse One VPN Certificate. Admin will be redirected to Trusted Client CAs page. Click on ‘Import CA Certificate...’ browse to the Pulse Workspace VPN Certificate downloaded in Step 9 of Pulse Workspace Configuration and click ‘Import Certificate’.
8. Click **System > Configuration > Pulse One > Settings** under Step 2 as shown in *Figure 9* to register PCS with Pulse One.
   a. Enter **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.

*Figure 11 Pulse One Settings*

9. Click **Authentication > Auth Servers** under Step 2 as shown in *Figure 9* to create Pulse Workspace MDM Authentication Server. Select New Server of Type ‘MDM Server’. Click **New Server**.
   a. Enter **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

To enable secure connectivity between PCS and Pulse Client:

Click 'Return to the previous guide' in the Task Guide. Click the third Step 'Enable secure connectivity between PCS and Pulse Client' of Task Guide as shown in Figure 4. List of all steps required to enable secure connection between PCS and Pulse Client will be displayed.

10. Click Authentication > Auth Servers under Step 1 as shown in Figure 13 to configure Certificate Authentication Server. Select New Server of Type 'Certificate Server' and click New Server:
   a. Enter Name.
   b. Click Save Changes.
Configure Secure Access from End User Devices

To configure secure access from end user devices:

Click 'Return to the previous guide' in the Task Guide. Click the fourth step 'Configure Secure access from end user devices' of Task Guide as shown in Figure 4. List of all steps required to configure Pulse Connect Secure to enable end users and to make connection with PCS will be displayed.

Figure 15 Task Guide – Step 4
11. Click **Users > User Roles** under Step 1 as shown in *Figure 15* 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 then 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 **Add Server** and enter the following details as shown in *Figure 17*

      - 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 Servers as 1.1.1.1/32:*)

*Figure 16 Configure User Role for L4 VPN*
12. Click Users > User Realms under Step 2 as shown in Figure 15 to configure user realm. Select the desired realm or create a new user realm, and configure following options:

   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.
      - Enter Name.
      - Select an Attribute and provide a value
      - Assign required roles.
      - Click Save Changes.
Figure 18 Configure User Realm

Figure 19 Configure Role Mapping Rules
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.

13. Click Authentication > Signing In > Sign-in Policies under Step 4 as shown in Figure 15 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 15 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 required roles and Save Changes.

Figure 20 SAM Resource Policy

15. Click Authentication > Signing In > Sign-in SAML > Identity Provider under Step 6 as shown in Figure 15 to update Sign-in Policy for SAML. Select the Sign-in policy configured in Step 13 as shown in Figure 15.
16. Once all the above configurations are complete, 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%.

![Figure 21 Cloud Secure Configuration](image)

17. (Optional) To configure L3 VPN instead of L4 VPN, skip Step 11 and follow the 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.
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. Enter Name.
b. Resources applicable (Internal Port as configured in Step 2).
c. Apply the policy to required Roles.
d. Click Save Changes.
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.
iv. To configure connection profile, navigate to Users-> Resource Policies-> VPN Tunneling-> Connection Profiles. Create a new connection profile and provide following details:

a. Enter Name.
b. Select DHCP Server and provide DHCP Server IP Address or select IPv4 Address Pool and provide the IP pool
c. Click Save Changes
**Figure 25 Connection Profile**

A screenshot of the Pulse Secure interface showing the configuration of a VPN connection profile. The screenshot highlights the DHCP servers and IPv4 address pool settings. The DHCP servers section is configured with a specific IPv4 address (10.200.112.2). The IPv4 address pool section allows for entering ranges of IPv4 addresses. The screenshot also includes options for IPv6 address assignment, connection settings, DNS settings, proxy server settings, and roles.
Configure Service Provider on PCS

To configure Salesforce Service Provider on PCS:

1. Navigate to System > Configuration > SAML.
2. Click ‘New Metadata Provider’, and then:
   a. Enter Name.
   b. Click Browse to upload the downloaded Metadata file from Salesforce.com (Step 10 of Salesforce Configuration).
   c. Enable Accept Unsigned Metadata.
   d. Enable Service Provider under Roles.
   e. Click Save Changes.

Figure 26 New Metadata Provider
3. Navigate to Authentication > Signing In > Sign-in SAML > Identity Provider.
4. Navigate to the bottom and Click ‘Add SP’ on the configuration page, and then:
   a. Select the Configuration mode as Metadata.
   b. Select Entity ID (the Entity ID will be the Salesforce domain).
   c. Select Override Default Configuration (Optional). This configuration is required only if you want 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 27 Add Service Provider]

Configuring Compliance Failure Notification

When an end user tries to access any cloud service from non-compliant device, cloud service access will be denied and a notification message with appropriate details will be provided to end user

To enable this configuration on PCS, follow the below steps:

1. Navigate to Users > User Roles. Create a new Remediation role and enable all the options as specified in Step 11 above.
2. Navigate to ‘UI Options’ tab of the user role. Scroll down to bottom. Enable the ‘Show Compliance Failure notification message on user's page’ check box and click Save Changes
3. Admin has the option to customize the compliance failure notification message displayed to the end user. To configure this, modify the default message in the 'Compliance Failure Notification' section and click Save Changes.

![Figure 28 Compliance Failure Notification](image)


5. Create a new role mapping rule to assign user to Remediation role created in Step 1 of this section above in case compliance check fails on user device.

**Configuring Role Based Access Control**

Cloud Secure supports Role Based Access Control feature which provides admin the option to control access for cloud services based on the roles assigned to the end user. If an end user is not authorized to access any cloud service based on the assigned role, access to cloud service is denied and access denial message with appropriate details will be displayed to the end user.

To enable this configuration on PCS,

1. Navigate to Authentication > Signing In > Sign-in SAML > Identity Provider.
2. Access the Service Provider configured, say, Salesforce, and configure the Roles section.
   a. **Policy applies to ALL roles**: This is the default option. This implies user assigned to any role will be provided access to the cloud service.
   b. **Policy applies to SELECTED roles**: Select this option and configure desired roles to restrict access to the cloud service only if any of the user roles configured are assigned.
c. **Policy applies to all roles OTHER THAN those selected below**: Select this option and configure desired roles to restrict access to the cloud service only if any of the user roles other than the ones selected are assigned.

*Figure 29 Role Based Access Control*

---

**Configuring Pulse Connect Secure for Android/iOS Users and Desktop Users**

Cloud Secure solution should work seamlessly on Android/iOS mobile devices as well as on Windows/ Mac OS X desktops. On mobile devices, certificate based authentication is used to establish secure and seamless Pulse VPN connection to PCS whereas on desktops it is suggested to use username/password based authentication. Also, compliance checks on mobile devices is achieved using MDM Server as device attribute server whereas on desktops Host checker policies solve this purpose.

To enable PCS to provide secure and seamless access to cloud services both to mobile users and desktop users, follow below steps in addition to the configurations done in ‘Configuring Pulse Connect Secure’ section above:

2. Create a new server of type ‘Active Directory / Windows NT’ and enter the following details:
   a. Name = <Reference Name>.
   b. Domain = <NetBIOS name of domain>.
   c. Kerberos realm = <DNS Name of Active Directory domain> (Example: pulsesecure.net).
   d. Username = <Active Directory admin username>.
   e. Password = <Active Directory admin password>.
   f. Leave rest of the values to default and click Save Changes. Domain Join Status should turn green after some time.
3. Navigate to **Authentication > Endpoint Security > Host Checker**.

4. Click ‘*New*’ under Policies and create a HC policy with rules for Windows and Mac OS X platforms.
   a. Enter **Policy Name** and click **Continue**.
   b. Under **Windows** tab, select any **Rule Type**, say, Custom: Process and then click **Add**.
   c. Enter **Rule Name** and **Process Name**. Select Required or Deny option and click **Save Changes**.
   d. Similarly, under **Mac** tab, select **Rule Type**, say, Custom: File and then click **Add**.
   e. Enter **Rule Name** and **File Name**. Select Required or Deny option and click **Save Changes**.
5. Navigate to Users > User Roles and create a new role for Desktop users, say, Desktop Role.

6. Configure user role as specified in Step 11.

7. To configure host checker restrictions on user role, navigate to Restrictions > Host Checker tab of Desktop role, select the ‘Allow users whose workstations meet the requirements specified by these Host Checker policies’ option and add the Host checker policy created in Step 4 of this section.

8. Click Save Changes.
9. Navigate to Users > User Realms and create a new realm for Desktop users, say, Desktop Realm.

10. Configure the following options:
   
   a. Select Active Directory Server created in Step 2 above as Authentication Server.
   
   b. Select the Role Mapping tab of user realm. Create a new role mapping rule based on custom expressions. Create a new expression based on hostcheckerPolicy from the available expressions in dictionary, hostcheckerPolicy = <HC Policy created in Step 4 of this section>.
   
   c. Insert Expression and Add Expression.
   
   d. Select this expression as rule, assign Desktop role. Select 'Stop processing rules when this rule matches' and click Save Changes.
   
   e. Create another role mapping rules based on username. If username is *, then assign to Remediation role (to assign role to non-compliant devices) and click Save Changes.
Figure 34 Configure Desktop Realm
11. Navigate to Authentication > Signing In > Sign-in Policies.


13. Map Desktop realm in addition to existing realm (used for iOS/Android users) to the sign-in policy.

14. Create browser restrictions for mobiles and desktop user realms so that Mobile users will be mapped to only mobile realm and Desktop users will be mapped to only Desktop realm.


   b. Select ‘Only allow users matching the following User-agent policy. Note that some browsers allow users to change this string, so this is not a guaranteed method of identifying the browser type,’ option and add a new User-agent string pattern.

      - *PulseAppConnect* - Allow
      - *PulseSecureiPhone* - Allow
      - *Android* - Allow

d. Select 'Only allow users matching the following User-agent policy. Note that some browsers allow users to change this string, so this is not a guaranteed method of identifying the browser type.' option and add new User-agent string patterns (rules should appear in following order once created).

- *PulseAppConnect* - Deny
- *PulseSecureiPhone* - Deny
- *Android* - Deny
- * - Allow
Note: Desktop users need to manually establish Pulse connection before accessing any cloud service to get seamless Single Sign-On access to the cloud services.

- For better user experience on Windows, Credential Provider feature can be used. To configure Credential Provider for Pulse Connection on PCS, navigate to Users > Pulse Secure Client > Connections > <Connection Set>. Access the desired Pulse L3 connection. Under ‘Connection is established’ section, select ‘Enable pre-desktop login (Credential provider)’ option and Save Changes.
- For better user experience on Mac, Location Awareness rules can be configured for Pulse Connection on PCS so that Pulse connection triggers automatically once user accesses his Mac machine. To configure Location Awareness rules on PCS, navigate to Users > Pulse Secure Client > Connections > <Connection Set>. Access the desired Pulse L3 connection. Under ‘Location Awareness rules’ section, create a new rule based on the requirements.
Configuring Pulse Workspace

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. Log in 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 as ‘Pulse SSL’.
   e. Leave rest of the fields to defaults and click ‘Publish’.
**Note:** Android devices support only L3 VPN whereas iOS devices support both L3 and L4 VPN.

---

**Figure 39 Modify VPN Properties**

4. Select the ‘iOS App Rules/Android App Rules’ tab under the policy created.

5. Click Add to add a 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.
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** (of this section) 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.

**Figure 42 Register 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.
Configuring Salesforce

For Cloud Secure solution Salesforce should be configured with:

- Admin account
- Register Domain
- SAML configurations
- Users

Steps to Configure

Follow below steps to configure Salesforce as Service Provider:

1. Sign up for a new Salesforce account. Register a new Salesforce domain.
2. Once domain is registered, log in to the domain (Ex: cloudsecure-dev-ed.my.salesforce.com). Click “Setup” on top right corner of the page.
4. Click ‘Edit’, check ‘SAML Enabled’ and then click ‘Save’.
6. Click ‘New’ under ‘SAML Single Sign-On Settings’. Enter the following details:
   a. Name: <Name>
   b. API Name: <Name>
   c. Issuer: https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi
   d. Entity ID: <Salesforce Domain>; Example: https://cloudsecure-dev-ed.my.salesforce.com
   e. Identity Certificate:
      ▪ Download PCS Metadata file from Authentication > Signing-in > Sign-in SAML > Metadata Provider. Copy Certificate content out of PCS Metadata to a file, save it, generate X509 Certificate out of it and upload it here (or)
      ▪ Choose the IdP Signing Certificate configured under Authentication > Signing-in > Sign-in SAML > Identity Provider page of PCS and upload it here
   f. Service Provider Initiated Request Binding: HTTP Redirect
   g. Identity Provider Login URL: https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi
   h. Leave rest of the fields with default values and click ‘Save’.
7. Navigate to Domain Management > My Domain on the left panel.

8. Click ‘Edit’ under ‘Authentication Configuration’ section, then check ‘<Name>’ (configured in Step 6a) and click ‘Save’.


10. Click ‘Download Metadata’ and save the metadata xml file.

11. Navigate to Administer > Manage Users > Users.

12. Click ‘New User’ to create a new Salesforce user if user does not exist. Provide following details:
   a. Enter First Name.
   b. Enter Last Name. Alias will get populated automatically.
   c. Enter Email. Username and Nickname will get populated automatically.
d. Select **Role** for the user.
e. Select **User License** as ‘**Salesforce**’.
f. Select **Profile** for the user.
g. Click **Save**.

*Figure 47 Create User*

---

**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 Salesforce 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 Salesforce 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 Salesforce application, select the ‘**Use Custom Domain**’ link in the Salesforce application and enter the Salesforce URL details (Ex: `cloudsecure-dev-ed.my.salesforce.com`).
8. Click the ‘**sso**’ link at the bottom of the application. Single Sign-On will happen and user will get access to the Salesforce.
End-User Flow on Desktops

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

1. Launch Pulse Client and establish a VPN session with PCS.
2. Open any web browser on the desktop, access Salesforce URL (Ex: cloudsecure-dev-ed.my.salesforce.com) and click ‘SSO’.
   a. If the user has an existing VPN session, ‘Re-use existing Pulse Session’ will kick in. PCS will send SAML response to Salesforce SP and the user will be granted access to Salesforce Cloud Service.
   b. If the 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 Salesforce SP and user will be granted access to Salesforce Cloud Service.
Dashboard

This section provides details about the Cloud Secure Dashboard. Dashboard captures the cloud secure applications that are getting accessed by users and the device platform from where these applications are getting accessed. This provides a consolidated view to the administrators.

1. To improve the visibility and experience, administrators are given options to configure the regex patterns for matching the applications and device details to the display strings in dashboard. These settings are accessible from System > Cloud Secure > Dashboard Settings page.
   a. Enable the Dashboard by selecting Enable Cloud Secure Dashboard under General Settings.
   b. Configure the required Timeframe for the charts and Refresh interval under General Settings.
   c. Configure the regex patterns for Device Platforms, Device Versions, Device Models and Applications under corresponding sections.
   d. Click Save Changes.

Note: By default, some of the regex patterns for Device Platforms, Device Versions, Device Models and Applications are present on PCS.

Figure 48 Dashboard Settings
2. Navigate to System > Cloud Secure > Dashboard page for accessing the Cloud Secure Dashboard page. This page contains 6 charts capturing the applications and device details.

a. **Top 5 Successful SSO Apps:** This chart is used for capturing the details about the applications that end users are able to access successfully. Top 5 such successful applications are represented in form of bar chart.

b. **Top 5 Failed SSO Apps:** This chart captures details of applications for which access is failed for the end users. This chart displays top 5 such failed applications.

c. **SSO Device Compliance Details:** This chart captures the details of compliance status of the devices from which users are accessing the applications. This chart captures the compliance status in " states and represents them in form of pie chart.

d. **SSO Device Details:** This chart captures details of the device OS version and platform from which the applications are getting accessed. These details are captured in form of Donut chart with inner circle capturing " details and corresponding outer circle capturing " details.

e. **SSO Apps Trend:** This chart contains details about applications trend. This captures trend of top 5 application in form of line chart.

f. **Top 5 SSO User Roles:** This chart captures details about the roles that are given to the end users. This captures top 5 roles in form of bar chart.

---

**Note:**

- 'Top 5 Failed Apps' chart captures details of only applications for which access failed due to Role Based Access Control restrictions or Compliance failure case on end user device.
- All the counters in above charts are incremented once per VPN session. If same application is accessed more than once during same VPN session, it is still counted as one.
- Admin can zoom into any particular chart by clicking on the chart in the dashboard.
Figure 49 Dashboard
Troubleshooting

This section provides details on commonly faced issues encountered during integration of multiple components involved in Cloud Secure Solution and probable solution to resolve them.

In most of the cases, Single Sign-On for an end user doesn’t work due to simple misconfigurations. As there are multiple devices involved, validate the configurations before doing SSO for cloud services. Below are the step by step procedures to validate all the configurations for all the components involved in the solution.

Follow the below sections to validate the configurations on the end user devices.

Mobile Devices (iOS/Android)

- Check if user device is registered successfully with MDM Server.
  - iOS devices
    - Open Settings-> General-> Device Management. Check if Workspace profile is installed.
  - Android devices
    - Access Pulse Workspace mobile application. Check if the profile got configured. You will be able to see list of all managed applications here.

- Check if VPN certificate is installed.
  - iOS devices
    - Open Settings-> General-> Device Management-> Workspace-> More Details. Check if certificates list has user VPN certificate.

- Check if desired cloud applications got installed.
  - Check if all the desired managed cloud applications got installed on the user device as part of mobile registration with MDM Server.

- Check if ActiveSync profile along with token got pushed onto user device for Native Mail Access.
  - iOS devices
    - Open Settings-> Mail, Contacts, Calendars. Check if Accounts section has ActiveSync profile pushed by Pulse Workspace. Verify the account details and check if email, server and username details are auto-populated and token is configured as password in the profile.

- Open Pulse Workspace > Policy > Configuration.
  - Check if ‘Divide’ section has registered user details.
Desктопы

- Проверьте, установлен ли Просмотритель и доступен ли требуемый VPN-соединение.

**Просмотритель Pulse Connect Secure**

Следуйте нижеприведенным шагам для подтверждения конфигурации на Просмотрителе Pulse Connect Secure.

- Проверьте, правильно ли настроены ограничения Realm/Role HC.
- Карточки с сертификатами, которые включают в себяWildcard или SAN (subject Alternative Name), должны использоваться на PCS для подписания SAML сообщений для бесшовного SSO доступа к облачным услугам.
- Сертификаты Host FQDN для SAML должны быть разрешимы, когда сервис через SSO доступен по веб-браузеру.
- Убедитесь, что настройки роли для L3 или L4 VPN туннелей настроены соответствующим образом в Pulse Workspace для мобильных клиентов. В случае использования Android мобильных устройств и Macintosh лэптопов, L3 VPN является единственной поддерживаемой туннельной технологией.
- Сертификаты промежуточных CA также должны быть загружены на Просмотритель Pulse Connect Secure, если ваше устройство сертификаты идентифицирует с помощью промежуточного CA.
- Убедитесь, что сервер LDAP доступен из Просмотрителя Pulse Connect Secure.

**Просмотритель Pulse Workspace**

Следуйте нижеприведенным шагам для подтверждения конфигурации на Просмотрителе Pulse Workspace.

- Убедитесь, что все приложения настроены с персонализированным доступом к сеансам VPN, кроме приложения Divide Productivity на устройствах Android по правилам приложений.
- Убедитесь, что все приложения установлены на устройстве пользователя. Перейдите в Workspaces->Users-><Username>-><Device>. Это показывает список установленных приложений. Если установка успешна, значок Просмотрителя изменится на зеленый для соответствующего приложения. Если установка не удалась, значок Просмотрителя остается серым.
- Убедитесь, что регистрация Appliance успешно завершена. Перейдите в Appliance tab. Pulse One Status should show as Connected for the respective Pulse Connect Secure.
- ‘VPN Certificate Auth’ should be set to true.
- ‘Use L3 VPN’ should be set to true for Android devices.

**Разрешение проблем (Типы)**

Эта часть содержит общие ошибки или проблемы, которые могут возникнуть во время интеграции решения Secure Cloud с несколькими провайдерами сервисов и предлагает вероятные решения для их разрешения.

**Сценарий**: Просмотритель Pulse Connect Secure не смог передать SAML Response к Серверу PROVIDER.

**Симптомы**:

- Просмотритель Pulse Connect Secure получил SAML AuthnRequest от Сервера PROVIDER, но не отправил SAML Response. Перейдите в User Access Logs на Просмотритель Pulse Connect Secure для проверки этих SAML сообщений.
- Пользователь要么收到了“Authorization Failed. Please contact your administrator. Details: You are not authorized to access the requested resource.”要么“Compliance Check Failed. Please contact your administrator. Details: You have limited connectivity because your device does not meet compliance”.
policies.” error message on the application and did not get access to the Cloud Service.

1. **Possible cause:** Role Based Access Control to the Service Provider failed. User is not authorized to access the cloud service due to the role assigned
   - **Possible solution:** On Pulse Connect Secure admin console, navigate to Authentication -> Signing In -> Sign-in SAML -> Identity Provider and configure specific Service Provider to allow access to the user role assigned to the end user

2. **Possible cause:** Compliance check failed for the end user. User receives compliance failure notification
   - **Possible solution:** Make the end user device compliant to get assigned to user role with full access

3. **Possible cause:** Access Control Lists are not configured to allow the accessed resource
   - **Possible solution:** Configure SAM/VPN Tunneling Access Control Lists on Pulse Connect Secure to allow access to the resource accessed

**Scenario:** Pulse Connect Secure successfully sent SAML Response to Service Provider but user did not get access to the cloud service.

**Symptoms:**
- Pulse Connect Secure received SAML AuthnRequest from Service Provider and successfully sent SAML Response. Check User Access Logs on Pulse Connect Secure to verify these SAML messages.
- User either received "Authorization Failed. Please contact your administrator. Details: You are not authorized to access the requested resource." or "Compliance Check Failed. Please contact your administrator. Details: You have limited connectivity because your device does not meet compliance policies.” error message on the application and did not get access to the Cloud Service.

1. **Possible cause:** Time on Pulse Connect Secure and Service Provider is out of sync.
   - **Possible solution:** Re-sync Pulse Connect Secure server clock by configuring reliable NTP Server.

2. **Possible cause:** Private key used by Pulse Connect Secure to sign the SAML Response does not match the public key certificate that is configured on Service Provider.
   - **Possible Solution:** On Pulse Connect Secure admin console, navigate to Authentication > Signing In > Sign-in SAML > Identity Provider and check if proper signing certificate is configured. Also check the signing certificate configured on Service Provider.

3. **Possible cause:** SAML Response sent by Pulse Connect Secure does not have a viable user identity.
   - **Possible Solution:** On Pulse Connect Secure admin console, navigate to Authentication > Signing In > Sign-in SAML > Identity Provider and check if Subject Name Format and Subject Name details configured under User Identity section are valid and should match the user configured in the Service Provider for cloud service access. If Identity Provider default configuration is overridden for the specific Service Provider, check if the details under User Identity section for that specific Service Provider are valid.
4. **Possible cause:** User created in the Service Provider do not have required privileges.
   • **Possible solution:** Make sure that the user created in the Service Provider has the Required SSO privileges. This configuration is on Service Provider and varies accordingly.

**Scenario:** Per-App VPN tunnel did not get established automatically on accessing managed cloud application.

**Symptoms:**
- When user accesses any managed cloud application, VPN symbol does not appear on the top of the mobile screen.

1. **Possible cause:** Desired application is not configured with Per-App VPN network access method on Pulse Workspace policy.
   • **Possible solution:** Edit the configured application on Pulse Workspace policy and enable it to use Per-App VPN.

2. **Possible cause:** VPN hostname is not resolvable from user device.
   • **Possible solution:** Make the VPN hostname publicly resolvable or configure host entry in internal DNS Server.

3. **Possible cause:** CA certificate that issued the PCS device certificate is not imported in all the required sections on PCS. This causes a certificate prompt when Pulse connection is being established on end device.
   • **Possible solution:**
     - Navigate to **System > Configuration > Certificates > Trusted Client CAs**. Import CA certificate that issued the device certificate imported in Step 1 of section ‘Enable PCS as SAML IDP server’.
     - Navigate to **System > Configuration > Certificates > Trusted Server CAs**. Import CA certificate that issued the device certificate imported in Step 1 of section ‘Enable PCS as SAML IDP server’.
     - In case if the CA that issued the device certificate imported in Step 1 of section ‘Enable PCS as SAML IDP server’ is an Intermediate CA, navigate to **System > Configuration > Certificates > Device Certificates**. Click the Intermediate CAs and import the Intermediate CA certificate.

4. **Possible cause:** User is not assigned to any user role.
   • **Possible solution:** Pulse Connect Secure is not successfully registered with Pulse One and unable to query and retrieve device attributes from Pulse Workspace MDM Server.
Service Provider Specific Troubleshooting

Refer to respective Cloud Service Configuration guides to get troubleshooting tips on specific Cloud Service.

If the administrator is unable to resolve any issue for any reason, submit a request with Pulse Secure support team and provide the following logs from different components:

**Pulse Connect Secure**

- Navigate to System > Log/Monitoring. Click ‘Save All Logs’ and save the logs.
- Provide server debug logs with event codes "saml,auth,soap,dsdash,cloudsecure" at level 50.
- Provide Policy tracing for the specific user session with proper realm.

**End User Device**

- Collect logs from Pulse Client mobile application/desktop application using Send Logs feature.
- Access the cloud service from Firefox browser enabled with SAML Tracer plugin on desktop and provide the SAML Tracer logs.
Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—for product warranty information, visit [https://www.pulsesecure.net](https://www.pulsesecure.net).