Pulse Secure®

Cloud Secure Administration Guide

Product Release	9.1R8
Published	July 2020
Document Version	3.0.3

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

https://www.pulsesecure.net.

Cloud Secure Administrator 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 https://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

The following table lists the changes to this document from the previous release.

Table Lists changes to this document from the previous release

Feature	Add	Drop or Move	Effective Release	Notes
Conditional Access	Updated "Conditional Access" section.		9.1R8	
Conditional Access	Updated "Conditional Access" section.		9.1R5	Added location based access.
Conditional Access	Added "Conditional Access" section.		9.1R4	
IdP Initiated Single Logout	Added "Configuring IdP Initiated Single Logout" section.		9.1R2	
URI Filtering	Added URI Filtering functionality in the section "Configuring Cloud Secure Application Policies" and modified the section "Cloud Application Visibility Dashboard".		9.1R1	
ECP Throttling	Added "ECP Throttling" section.		9.1R1	
Cloud Application Visibility	Added a new chapter for "Cloud Application Visibility".		9.0R2	
Sha-256 support	Sha-256 support is added while configuring SAML/IdP settings, Third-Party IdP settings and so on.		9.0R2	
Location Awareness for Android	The "Configuring PWS for Location Awareness" section is updated.		9.OR2	

Table of Contents

Cloud Secure Overview

Cloud Secure provides secure, seamless, and compliant access to cloud resources on a hybrid IT environment where companies are combining the best of the cloud with their own localized data centers.

Product Briefing

Cloud Secure is a solution, which integrates multiple Pulse Secure products for seamless secure access in a hybrid IT environment. The solution includes the following components:

- **Pulse Connect Secure (PCS)** – PCS provides VPN connectivity with granular access control and wide array of authentication mechanisms. 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 Mobile Device Management (MDM) Server for Cloud Secure solution. Cloud secure users must 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.
- **Pulse Policy Secure (PPS)** – PPS provides network access to On-Premise users after authentication and compliance posture assessments.
- **Licensing** - Cloud Secure is a licensed feature. For any existing deployments/users upgrading to Release 9.0R3. Admin should procure and install the Cloud Secure license to use the Cloud Secure UX and features. A warning message to procure license is displayed on the Cloud Secure dashboard page for the existing users.

For more information on how to apply and install license, see License Management Guide.

Salient Features of Cloud Secure

The key features of Cloud Secure are:

- **Single Sign-On (SSO)** - Cloud Secure supports SAML based SSO which allows pre-authenticated users to access resources without entering credentials again for applications which are accessed. It also tunnels authentication exchanges between client and PCS thus providing Secure Single Sign-On to SaaS, Cloud, and Enterprise hosted resources.
- **Single Logout (SLO)** - Single Logout allows administrator to deny user access to services and initiate Single Logout in the following scenarios when: the machine goes out of compliance during a session, the user session times out, the administrator deletes the session in PCS configured as IDP, or the user logs out from PCS (as IDP) landing page.
- **Compliance** - Cloud Secure leverages Pulse Secure's Host Checking capabilities in desktops and MDM device attributes in mobile devices to give best in class compliance posture assessment capabilities and allows for varying levels of access based on device compliance and well as user-based information.
- **Mobile-Ready** - Cloud Secure integrates with Pulse Workspace and leading EMM solutions for compliance enforcement and for BYOD container security.
- **Extensible Identity Management** - Cloud Secure integrates well with Third-Party Identity Providers (IdP) to support existing customer deployments that have already implemented these Identity management solutions.
- **Role Based Access Control** - Cloud Secure supports Role Based Access Control (RBAC) feature to provide access control for cloud services based on the roles assigned to users.
- **Compliance Failure Notification** - Cloud Secure supports notifications for compliance failure scenarios. A remediation notification helps notify end users about the reason of failure and the necessary steps to get the device into a compliant state.
- **MDM Servers** - Cloud Secure integration with MDM servers helps in better management of mobile devices by keeping the corporate data secure from personal data. In addition to this, better compliance rules and enforcement methods are possible with device attributes retrieved from MDM servers.
- **On-Premise SSO** - Cloud Secure supports SSO for On-Premise users authenticated to Pulse Policy Secure (PPS). This is done by sharing session information from PPS to PCS through IF-MAP federation and removes the need to establish a VPN tunnel directly to PCS.
- **Cloud Secure Configuration Simplification through new Admin Interface–** Cloud Secure configuration is made simpler through a simplified and intuitive admin interface. This enhances the admin experience and helps them by prepopulating the relevant settings, reuse existing configurations and guide them with insightful help sections.

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 AFW 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** – 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 Service Provider (SP for PCS). Cloud Secure solution supports integration with **Ping One**, **Okta**, and **AD FS**.

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 such as O365, salesforce and so on) and Identity Provider (PCS) to provide SSO.

Single Sign-On, using SAML is classified into IdP initiated and SP Initiated scenarios:

- **SP initiated scenario** - The user tries to access the application, the cloud service triggers SAML authentication requests and redirects them to IdP for authentication.
- **IdP initiated scenario** - The user first authenticates with Identity provider before accessing the cloud service.

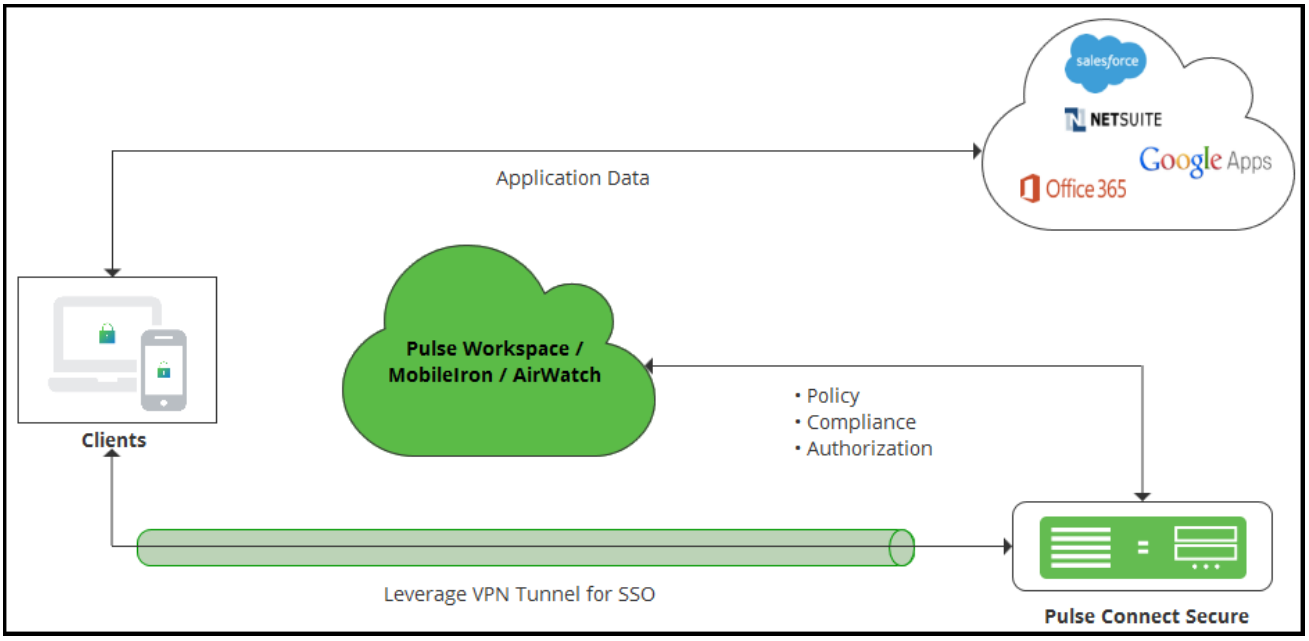
This section describes the following deployment scenarios:

- Deployment using Web Browser SSO Profile
- Deployment using Enhanced Client or Proxy (ECP) Profile
- Deployment using Third-Party IdP
- Deployment for On-Premise Users

Deployment using Web Browser SSO Profile

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

Figure: Secure Sign-on to SaaS

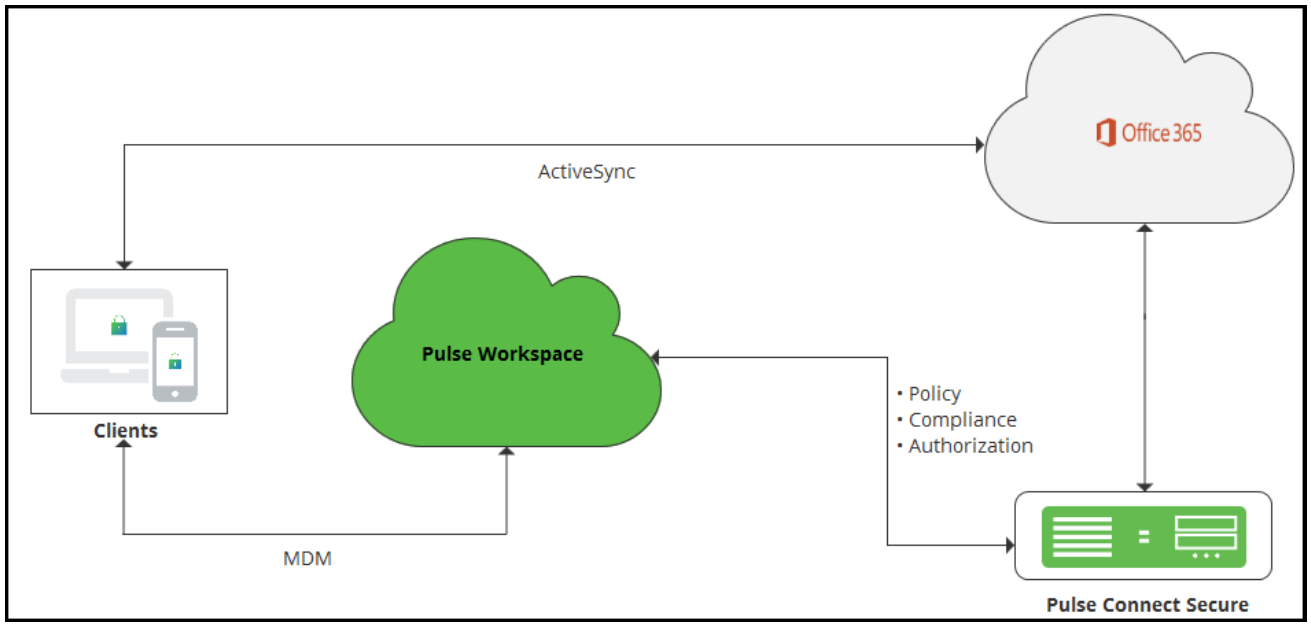


For web browser SSO, Pulse VPN client on mobile or desktop is used to deliver strong authentication and device compliance check. On mobile devices, cloud applications can be configured with per-app VPN client which is launched automatically when cloud application tries to access cloud service. On desktop, 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 web browsers. The SP and IdP communicate directly instead of exchanging SAML messages over user's web browser.

Figure: Secure Sign-On to Office365 using ECP



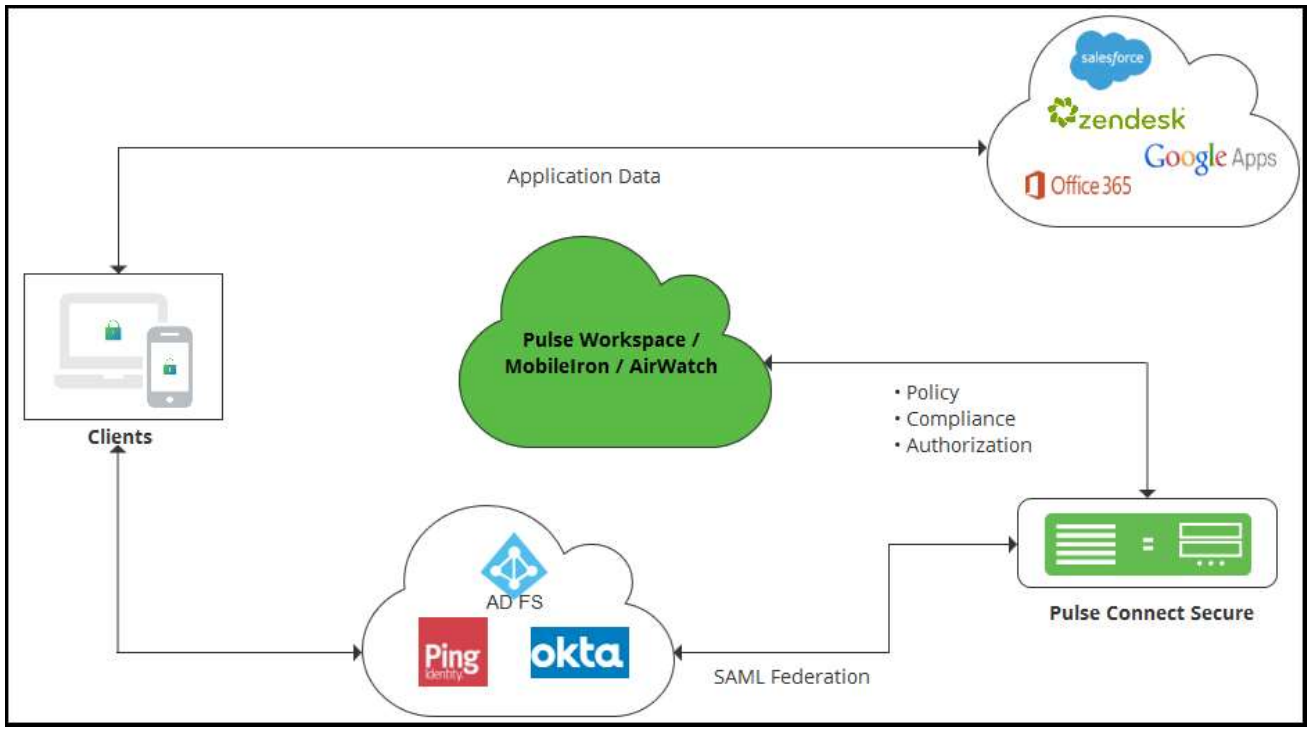
The native outlook applications on mobile devices use ECP profile (unlike web browser SSO profile) for authentication. For ECP profile, Cloud Secure solution uses the unique token generated by Pulse Workspace for authentication and to retrieve device compliance details. As part of the mobile device registration, 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 One, Okta and Microsoft AD FS.

For Cloud Secure Solution, the Third-Party IdPs act as both IdP (for cloud services) and SP (for PCS acting as IdP). Third-Party IdPs allow PCS to be configured as external SAML Identity Provider to authenticate users and enable secure Single Sign-On to cloud applications.

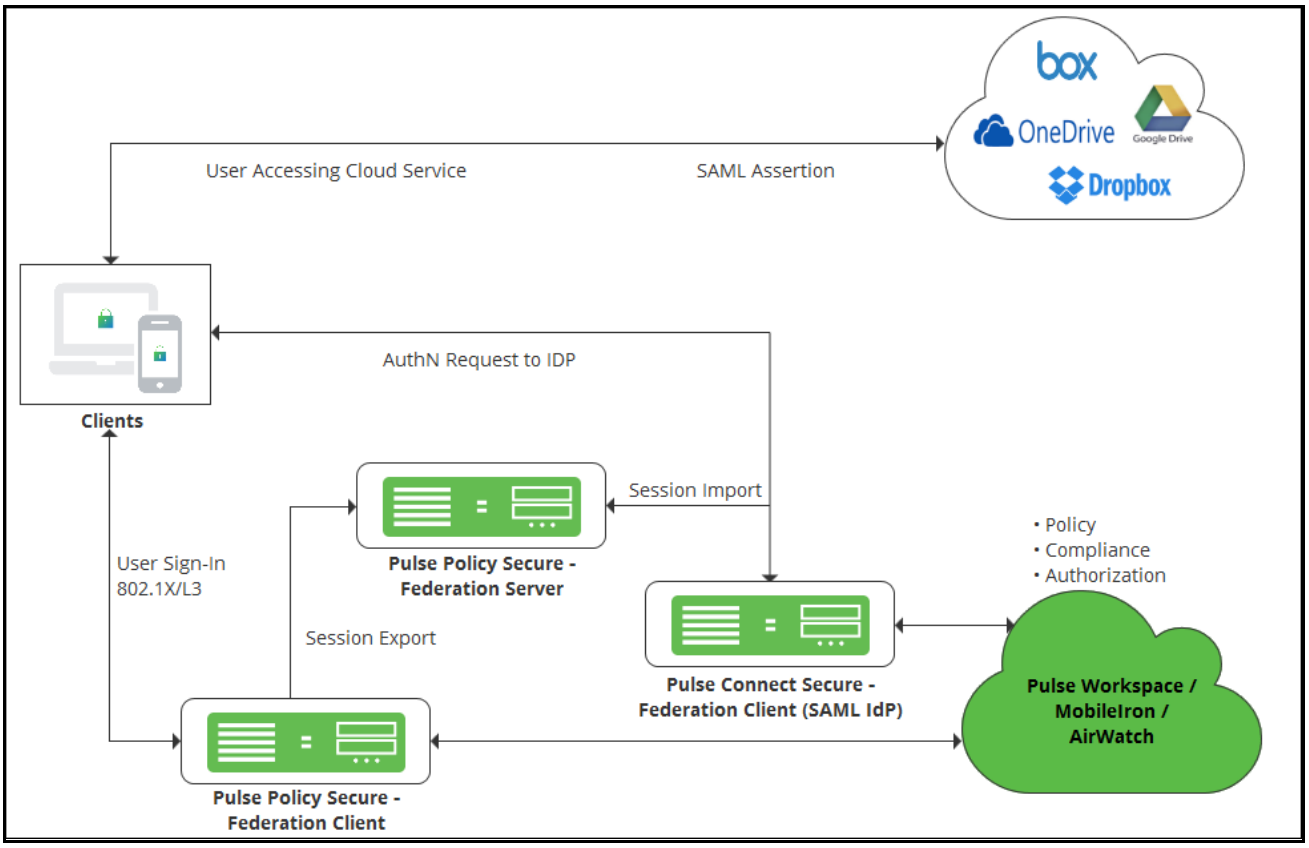
Figure: Secure Sign-On using Third-Party IdP



Deployment for On-Premise Users

Cloud Secure provides Single Sign-On access to cloud services for On-Premise users authenticated to PPS after compliance posture assessment. On premise users are authenticated by PPS when they are connected to enterprise network. PPS exports this session to Federation server through IF-MAP federation capability. PCS acts as Federation client and imports session information from Federation Server and uses this imported session information to generate SAML assertions to provide access to On-Premise users. This eliminates users providing credentials again with every application access.

Figure: Secure Sign-On for On-Premise Users



Note: IF-MAP Federation is used for session sharing between PPS and PCS.

On-Premise user SSO Flow

1. User Sign-In:
   a) On-Premise users authenticate to PPS (Federation Client) via Pulse Client or native supplicant. As part of this 802.1x authentication, compliance check will be performed before granting access to the user.
   b) In case of mobiles, user connects to SSID (SSID settings will be pushed from Pulse Workspace) and authenticates with PPS using certificate authentication. PPS uses Pulse Workspace return attributes for mobile compliance checks before granting access.
2. Session Export: Since PPS is configured as Federation Client, IF-MAP session information will be exported to Federation Server
3. Access Cloud Service: User accesses cloud service enabled with Single Sign-On
4. AuthN Request: PCS acting as SAML IdP and Federation Client will receive the SAML Authentication Request
5. Session Import: On receiving SAML AuthnRequest, since PCS is configured to use existing Pulse VPN session and existing IF-MAP imported session, it will initially check for a local Pulse VPN session. If not found, PCS will import the IF-MAP session from Federation Server
6. SAML Assertion: PCS will use this imported session information to generate SAML response/assertion and sends it to cloud service thus providing SSO access to On-Premise users

Configurations

This section covers the configurations required on different products involved in Cloud Secure solution.

To enable Cloud Secure solution, admin needs to configure PCS as a SAML Identity Provider, Cloud Service (For example, O365) as SAML Service Provider, PPS for On-Premise SSO, and Pulse Workspace as Mobile Device Management (MDM) Server.

This section lists the following configurations:

Configuring Pulse Connect Secure

The Cloud Secure simplified UX is a modern, faster and responsive user interface which allows you to quickly and easily configure the Cloud Secure functionality without navigating into multiple pages. The new UX enhances the administrator experience through pre-populating the relevant settings, reusing the existing configurations, and guides the user with help sections. It also enables simpler way of configuring the cloud applications as Service Providers.

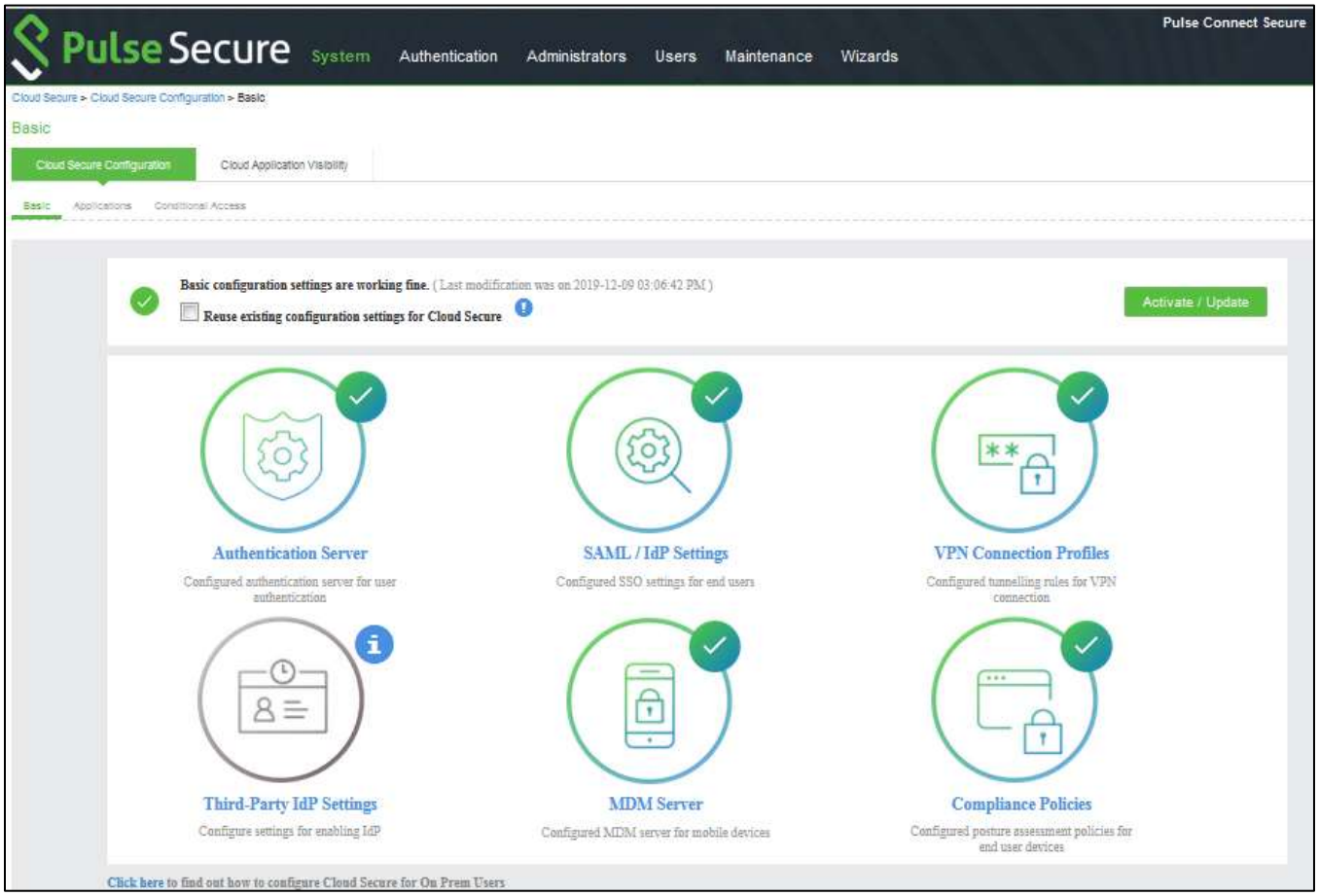
The Admin can choose to configure Cloud Secure in two ways:

- Completing all the basic configurations
- Reusing the existing PCS configurations

Basic Configurations

To launch the configuration page, select **System > Cloud Secure > Cloud Secure Configuration**.> Basic

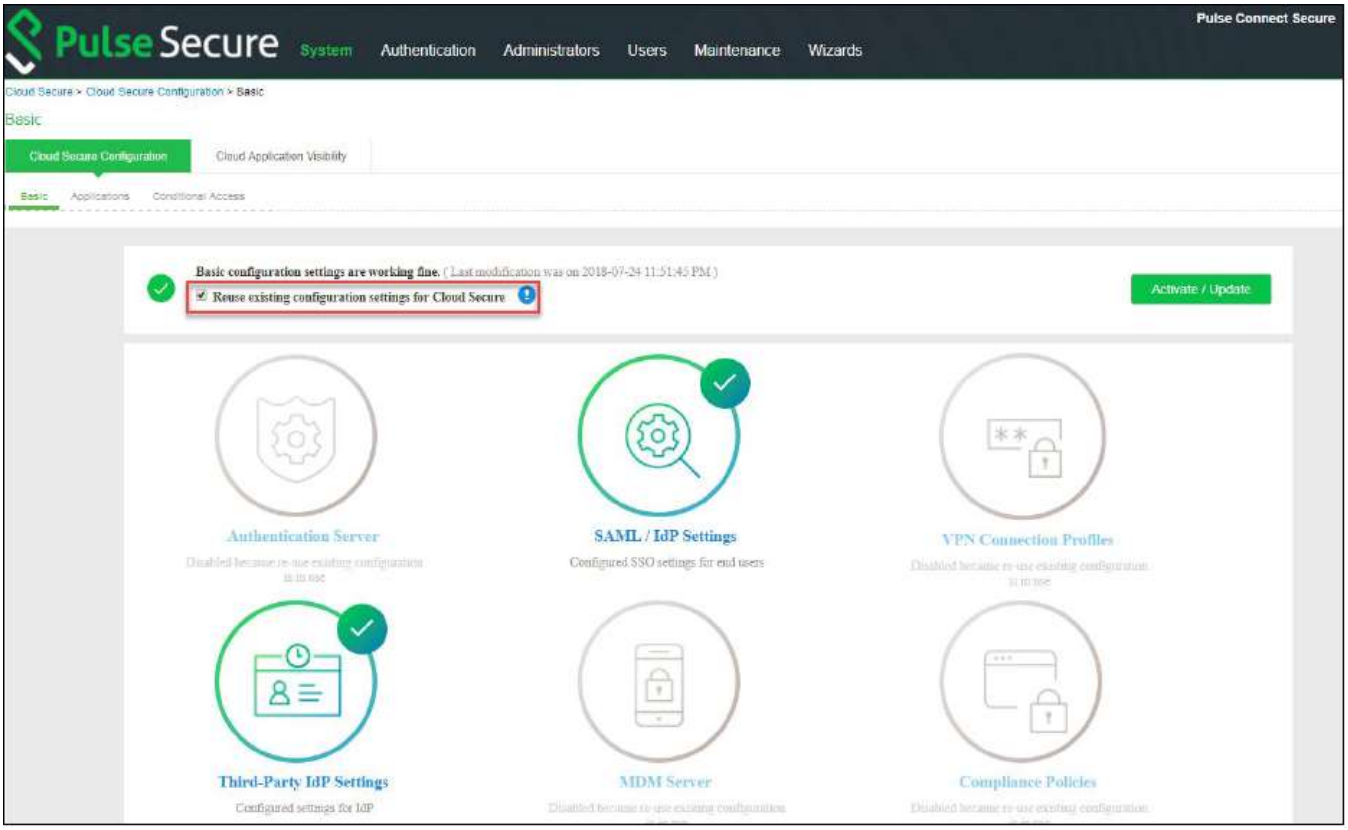
Figure: UX Home Screen



Reusing existing PCS configurations

If the user has already configured the Role, Realms, Authentication server and so on. The existing configurations can be reused for Cloud Secure by enabling the **Reuse existing configuration settings for Cloud Secure** option from the Cloud Secure UX Home Screen. It simplifies the Cloud Secure configurations for the existing users as it requires only SAML/IdP settings to be configured.

Figure: Reuse Existing Configurations



Prerequisites

The following information should be available before configuring Pulse Connect Secure:

1. Authentication server details for authenticating end users.
2. Device Certificates and Trusted Server and Client CAs for establishing connections from clients, external servers (MDM, IdP) and for signing SAML assertions.
3. **(Optional)** Metadata file of Okta/PingOne/Microsoft AD FS, in case of Deployments with Third-Party IdP servers.
4. **(Optional)** MDM server details (Pulse Workspace/Airwatch/MobileIron) including the required certificates for VPN connection establishment.

Limitations

The following configurations should be done by navigating through respective pages:

- Clustering configurations
- Advanced configurations like multiple role mapping rules. Administrator must browse to respective pages on the UI for such configurations.

Basic Configurations (Mandatory)

The following configurations are mandatory to enable Cloud Secure:

- Configuring Authentication Servers
- Configuring SAML/IdP Settings
- Configuring VPN Connection Profiles

Configuring Authentication Servers

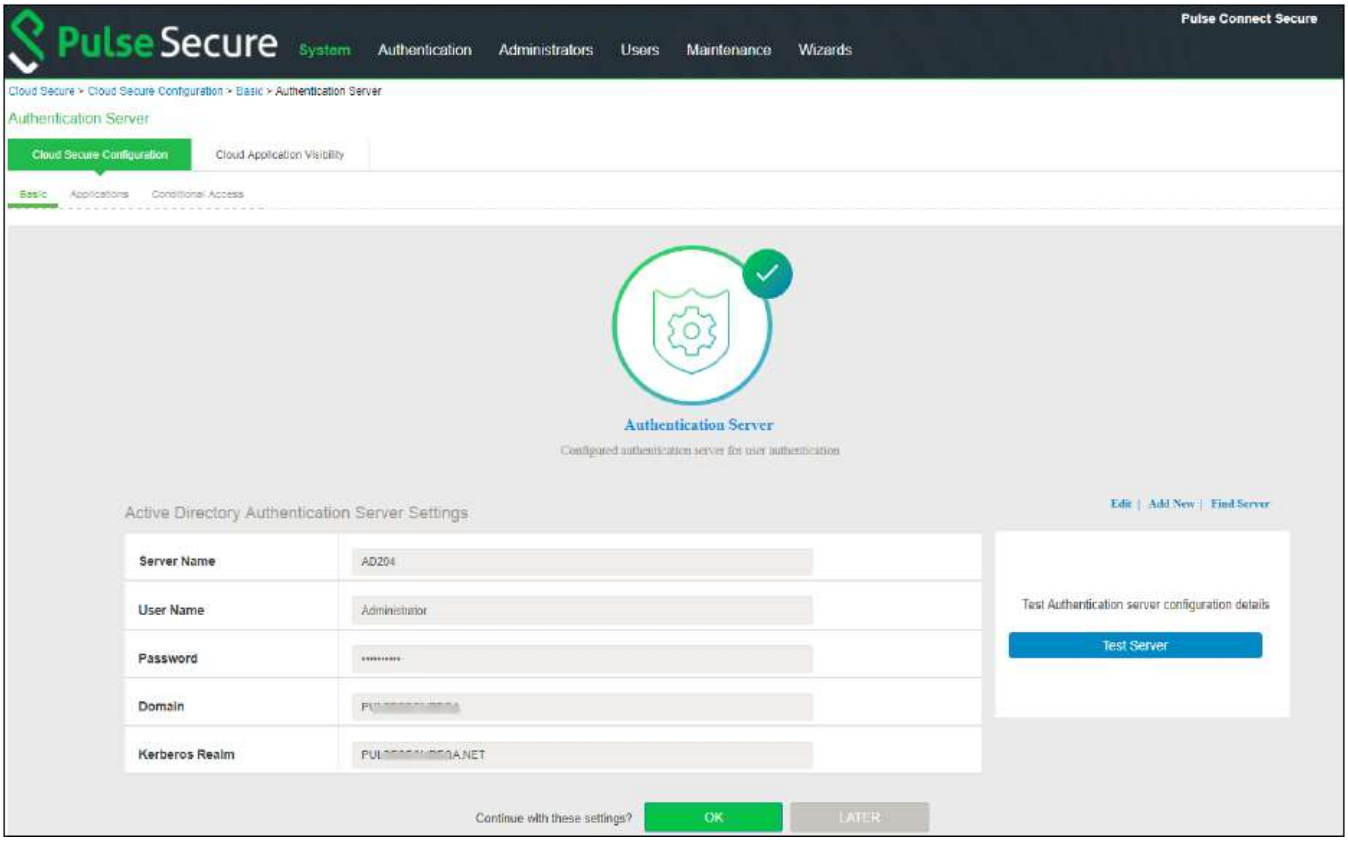
The user accesses the data and applications remotely when they are hosted in Cloud. The Administrators need to implement user access control for Cloud resources similar to the local resources that reside in the data center.

Cloud Secure supports many authentication mechanisms. It is suggested to use Certificate authentication for mobile devices, AD authentication for Desktops.

Cloud Secure UX allows configuring AD/LDAP authentication servers.

1. Select **Authentication Server**.
2. Click **Add New**.
3. Select **Server Type** as *Active Directory*.
4. Enter **Server Name**.
5. Enter the administrator **Username** and **Password** for communicating with the AD server.
6. Enter **Domain Name**.
7. Enter **Kerberos Realm**.
8. Click **OK.**

Figure: UX: Authentication Server

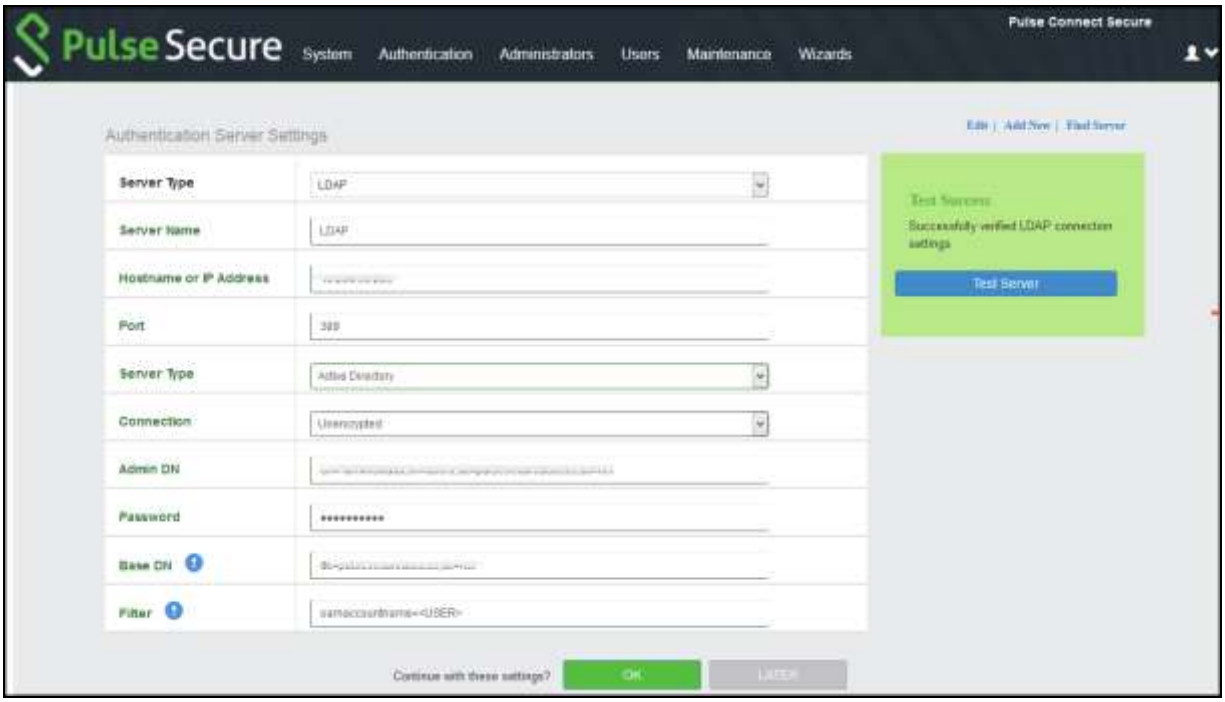


Note: Office 365 Services need LDAP server to retrieve user attributes before sending SAML assertions.

To configure/add LDAP Authentication Server.

1. Select **Authentication Server**.
2. Click **Add New**.
3. Select **Server Type** as *LDAP*.
4. Enter **Server Name**.
5. Enter server IP address in the **Host Name** field.
6. Select appropriate **Server Type** from the drop-down list.
7. Select appropriate **Connection** from the drop-down list.
8. Enter **Admin DN** details.
9. Enter **Password**.
10. Enter **Base DN**.
11. Click **OK**.

Figure: UX: Authentication Servers



Note:

- Cloud Secure UX allows reusing existing AD/LDAP server configurations by selecting the already existing server from the Find Server option.
- Cloud Secure UX allows validation of AD/LDAP server connection and configuration details. "**Test**" option Validates connectivity, Domain reachability, Login credentials and so on.
- Cloud Secure UX allows to edit the **Authentication Server** settings.

Configuring SAML/IdP Settings

Cloud Secure supports SAML based SSO which allows authenticated users to access Cloud resources without entering credentials again. Pulse Connect Secure acts as Identity Provider and responds to all SAML requests from Cloud Services.

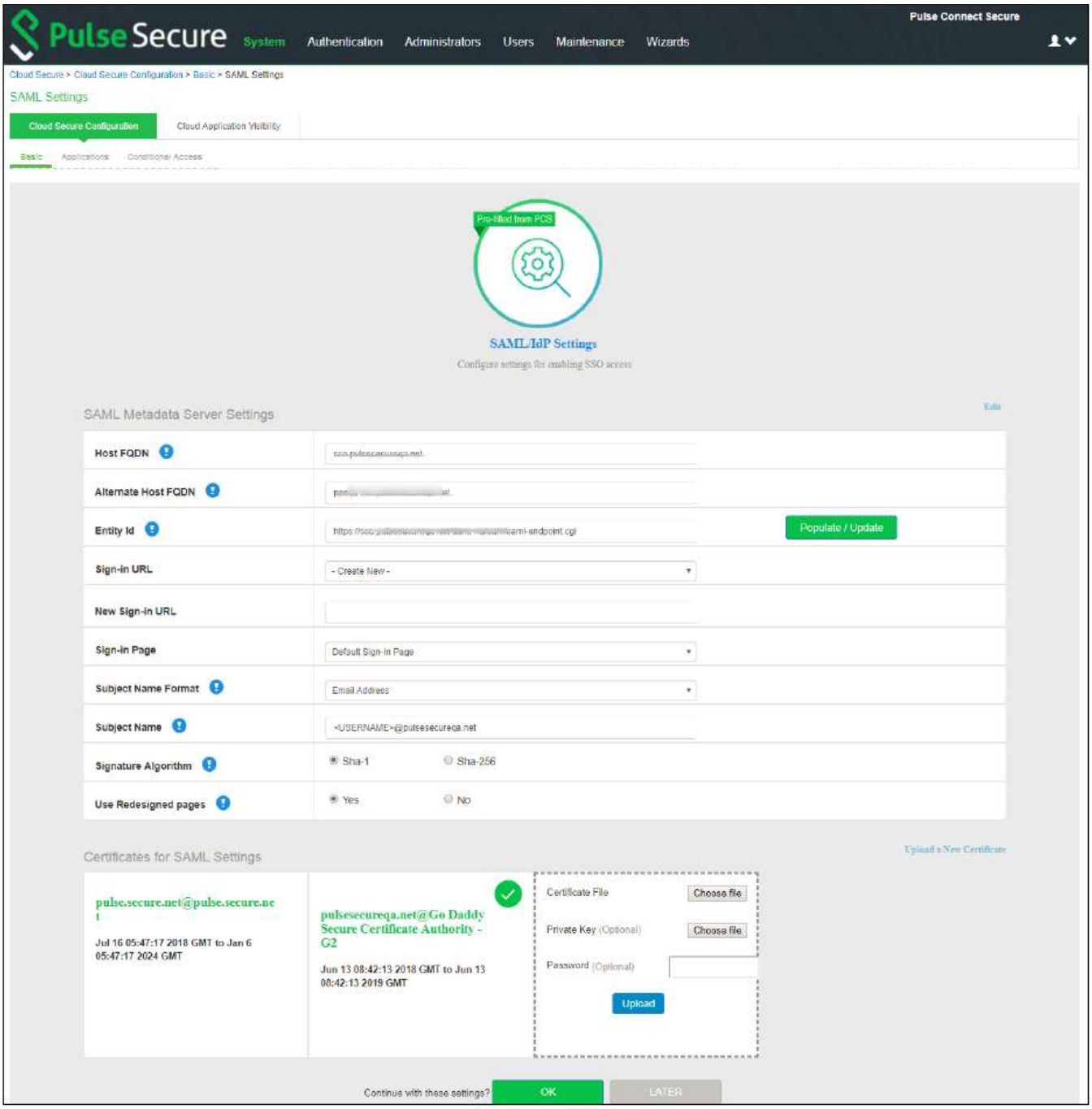
1. Select SAML Settings.
2. Enter **Host FQDN** for SAML.
3. Enter **Alternate Host FQDN** for SAML.
4. Enter the **Entity Id**, that is SAML unique identifier for PCS. The administrator can also choose to update/populate this field using the Host FQDN.
5. **Sign-in URL:** Admin can either use an existing Sign-in URL or create a new URL. To create a Sign-in URL, select **Create New** and give **New Sign in URL** Name and select **Sign-in Page**.

   Note: Create New url option appears only if the Admin unchecks the Reuse existing configuration settings for Cloud Secure option in the configuration page.
6. Select **Subject Name Format** from the drop-down list.
7. Enter **Subject Name**.
8. Set the **Signature Algorithm** to *Sha-1* or *Sha-256*.
9. Click Yes to use the new redesigned end user pages while accessing Cloud Secure. This option is enabled by default. However, if you are upgrading the Cloud Secure from a previous release to the latest release, you must enable this option manually.
10. Upload a new signing certificate or select the certificate from the existing certificates. After uploading a new signing certificate, click on the **Device Certificate** link populated for configuring the certificate on network ports.
11. Click OK.

Note:

For most of the use cases **Subject Name Format** is *Email Address* and **Subject Name** is *<USERNAME>@<DOMAIN>*.

Figure: UX: SAML/IdP Settings



Note:

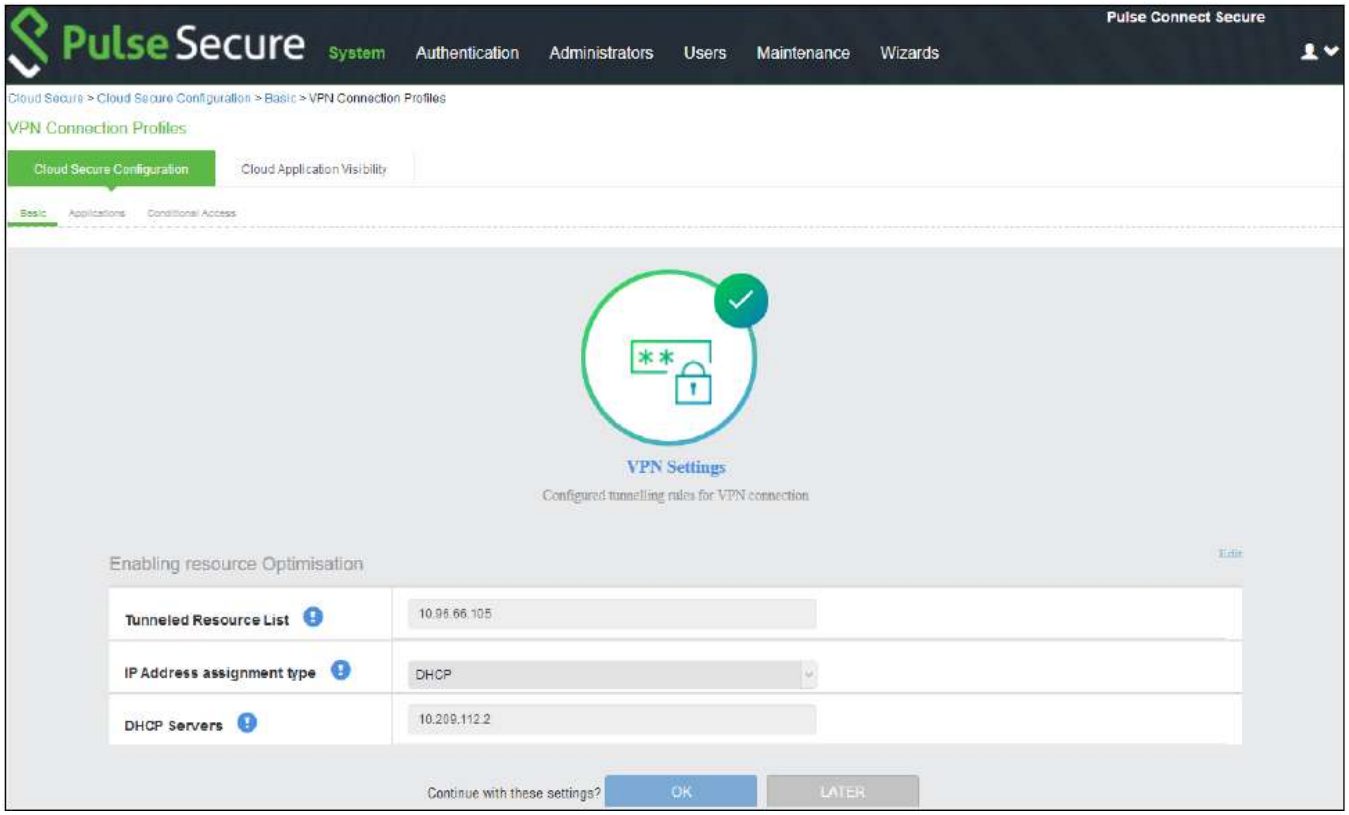
- For two arm deployments, Host FQDN for SAML is DNS Host name of External Port and Alternate Host FQDN is DNS Host name for Internal Port. Alternate Host FQDN for SAML configured on PCS is used to redirect user to IdP login URL provided in Service Provider. On public DNS servers, both Host FQDN and Alternate Host FQDN should resolve to External Port IP Address. In local DNS servers, Alternate Host FQDN should resolve to Internal Port IP Address.
- For one arm deployments, Host FQDN is host name of Network Port and Alternate Host FQDN is host name of Virtual Port. On public DNS servers, both Host FQDN and Alternate Host FQDN should resolve to Network Port IP Address. In local DNS servers, Alternate Host FQDN should resolve to Virtual Port IP Address.

Configuring VPN Connection Profiles

VPN Connection Profiles are used to assign tunneling IP's to client machines using DHCP servers or Global Address Pools during VPN tunnel establishment. You can also configure a split tunneling policy to send only the authentication, authorization, and compliance check traffic to PCS and application data directly to the cloud. Tunneled Resources list captures list of resources, which needs to be tunneled through PCS. This list is a combination of resources IP address and FQDN host names.

1. Select VPN Connection Profiles section.
2. Enter the Internal IP Address/subnet and Internal DNS Server under **Tunneled Resource List** and click **Add**.
3. Under **IP Address assignment type**:
    a. Select **DHCP** and give DHCP Server's IP address and click Add or
    b. Select **Manual** and give IP Address pool and click Add.
4. Click OK.

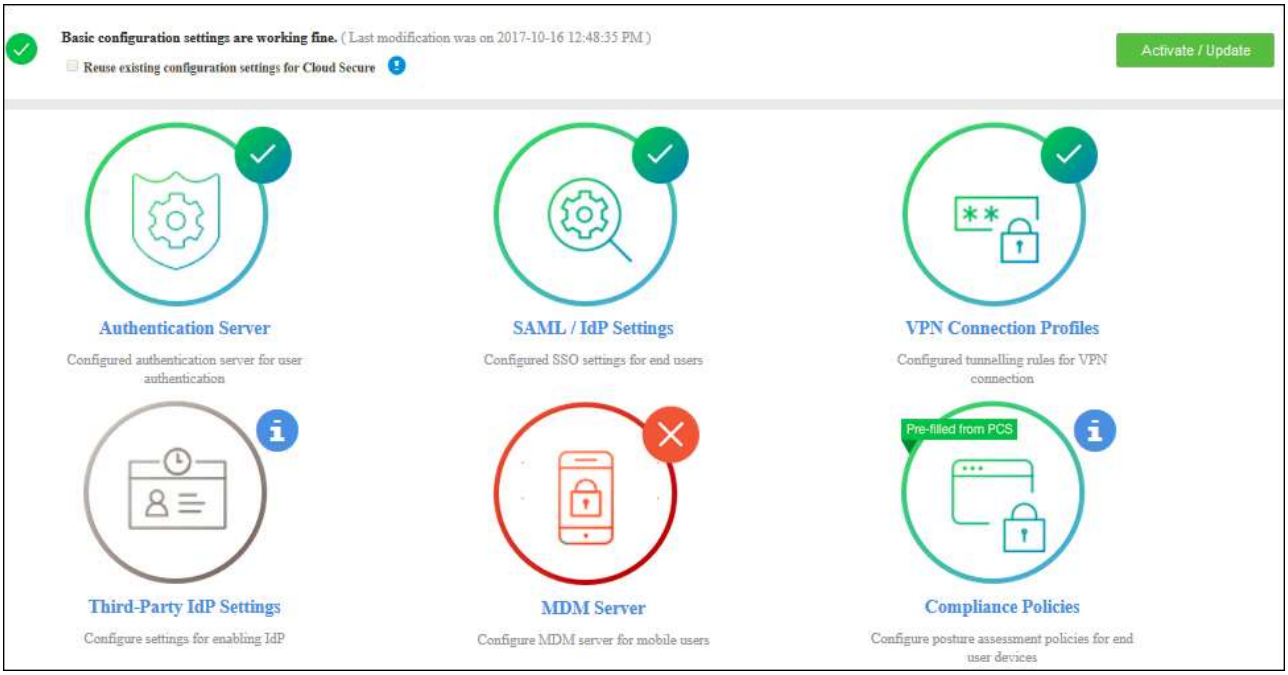
Figure: UX: VPN Connection Profiles



Note: Internal IP Address or FQDN hostnames need to be added in the **Tunneled Resource List**. This enables SSO access to the cloud resource by leveraging re-use VPN functionality when client machine having VPN tunnel accesses the cloud resource.

The following screen is displayed after completing the basic configurations on PCS. Click **Activate/Update** to enable Cloud Secure. After activating, the administrator will be redirected to Applications page. Click **Open** to go back to basic configuration page.

Figure: UX: Basic Configurations



Note: The icons in the configuration page indicate the status of configuration.

- Green Tick mark refers that this section is configured correctly.
- If the configuration section is in grey color, it indicates that the section is not configured.
- Red cross mark refers there is a connection problem with Authentication/MDM server.
- Pre-filled from PCS refers that the Admin can reuse the existing configurations from PCS.

Advanced Configurations (Optional)

The following configurations are optional.

- Configuring Third-Party IdP Settings
- Configuring MDM Settings
- Configuring Compliance Policies

Configuring Third-Party IdP Settings

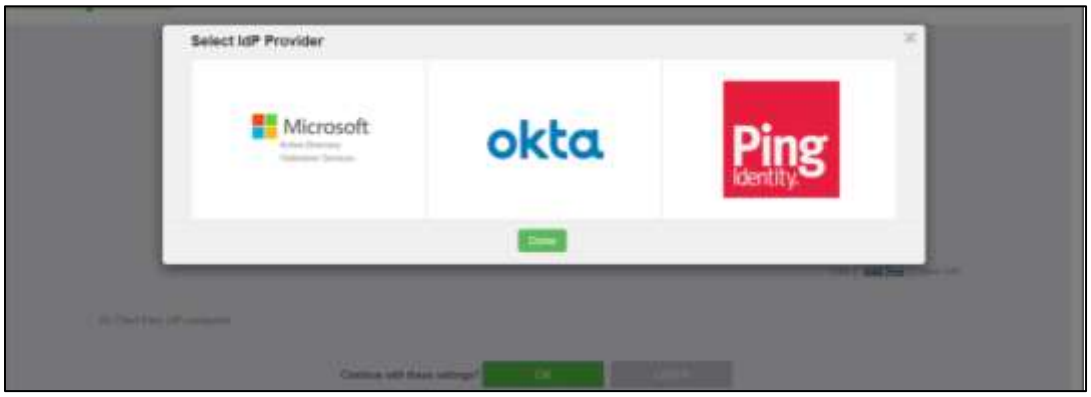
SAML allows cloud services to delegate user authentication to IdP. The IdP can also delegate the authentication to another IdP, which is called IdP federation. Cloud Secure supports IdP federation with PingOne, Okta, and Microsoft AD FS.

ADFS as Third-Party IdP

To add ADFS as third-party IdP provider:

1. Click **Add New** and select the **Third-party IdP** as Microsoft ADFS.

Figure: UX: Third-Party IdP



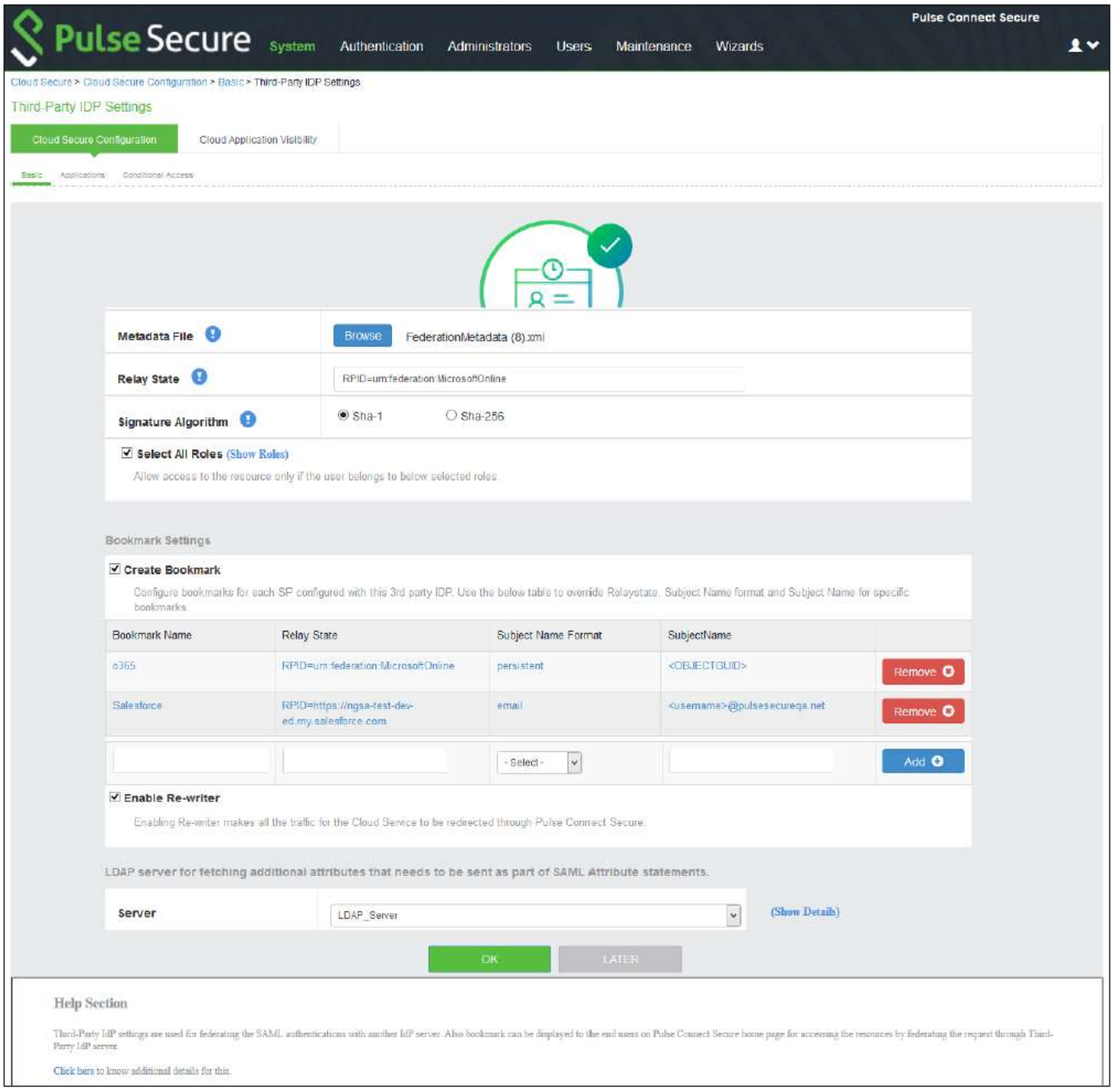
2. Click **Done.**
3. Under User Identity, select **Subject Name Format**.
4. Enter **Subject Name.**
5. Click **Browse** and upload the metadata file.
6. Enter the relay state.
7. Set the signature algorithm to **Sha-1** or **Sha-256**.
8. Select the desired roles.
9. Under **Bookmark settings**, enable the checkbox for **Create Bookmark** to configure bookmarks for each SP configured with the third-party IDP.

   You can configure multiple bookmarks for each SP configured with the Microsoft Active Directory Federation Service (ADFS) server.

   a. Enter the bookmark name.
   b. Enter the relay state.
   c. Enter the subject name format.
   d. Enter the subject name.
   e. Click **Add**.
10. Enable the checkbox **Enable Re-writer** to redirect all the Cloud Secure traffic through PCS.
11. Configure the LDAP server for fetching the additional details.

12. Click **OK**.

Figure: UX: Third-Party IdP - ADFS Settings



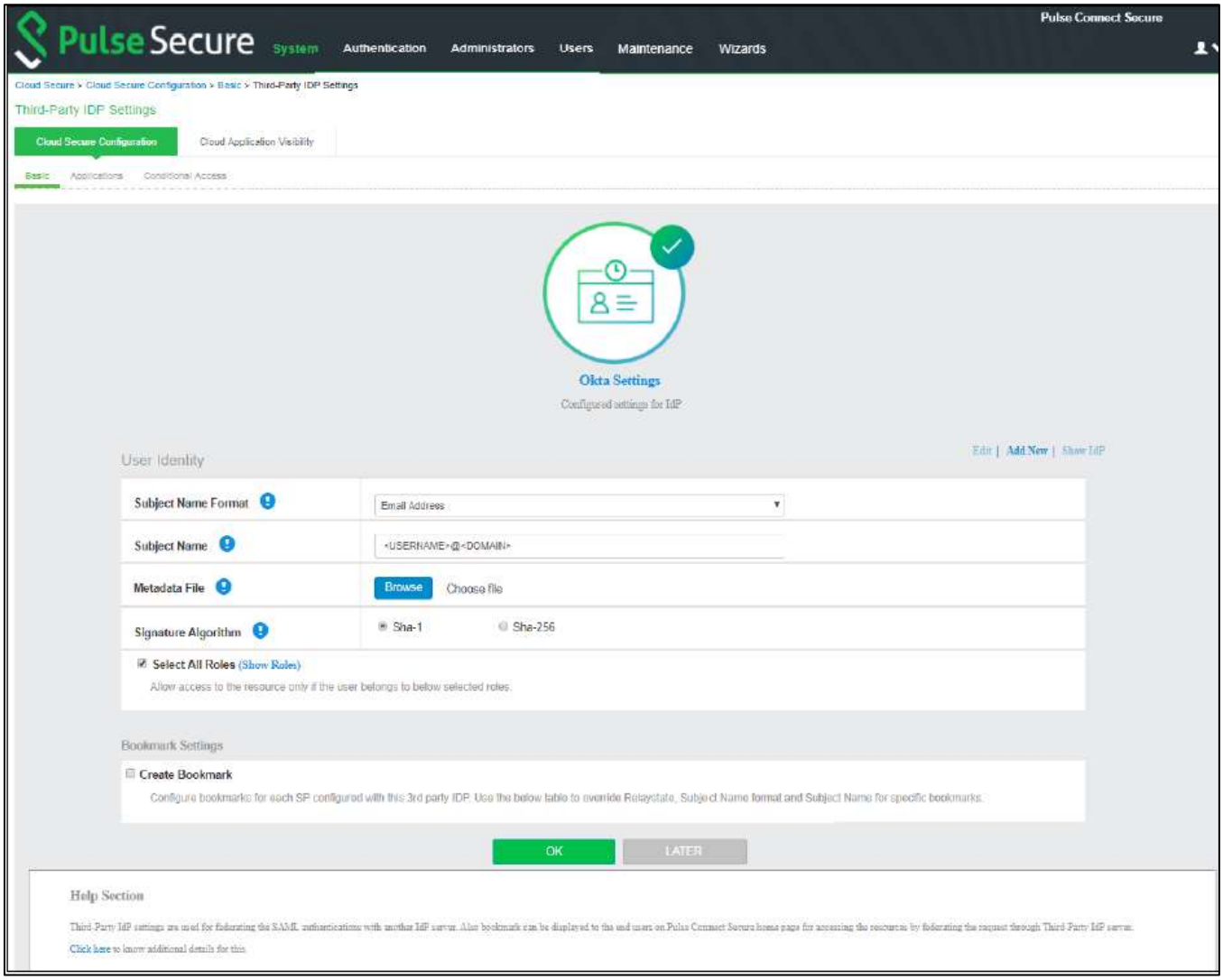
PingOne/Okta as Third-Party IdP

Under **Third-Party IdP Settings** section:

1. Click **Add New** and select the **Third-Party IdP** (PingOne/Okta).
2. Click **Done**.
3. Enter the Subject Name Format.
4. Enter the Subject Name
5. Click **Browse** and upload the metadata file (UX allows configuring Third party IdPs only through metadata file).
6. Set the signature algorithm to **Sha-1** or **Sha-256**.
7. Select the desired roles.

8. Click **OK**.

Figure: UX: Third-Party IdP



Note: Click **Show IdP** to view the details of the configured Third-Party IdP servers.

Configuring MDM Settings

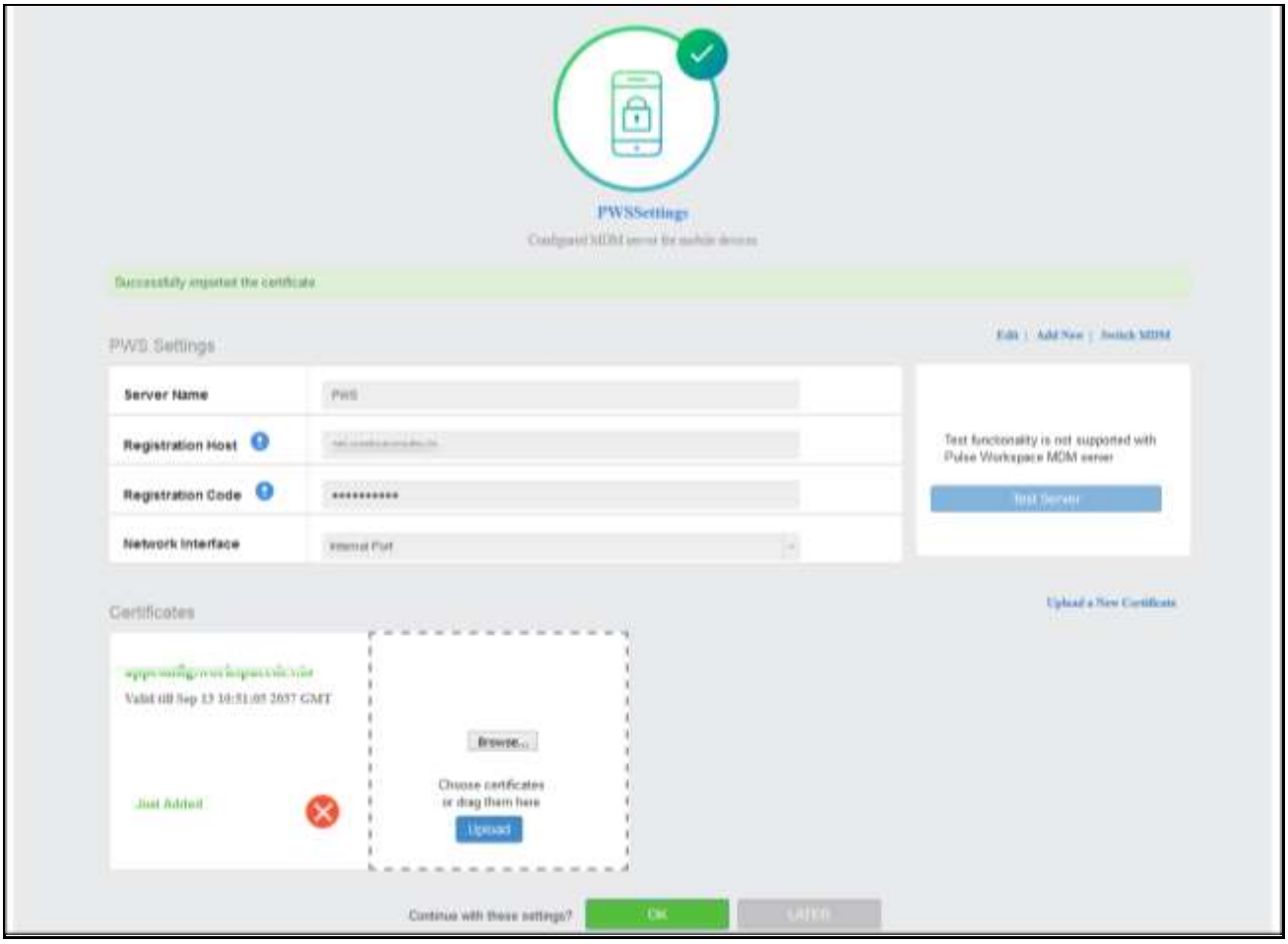
Mobile Device Management (MDM) Server is used to perform compliance check for managed mobile devices. The authentication is based on the certificate installed on the mobile device when the user enrolls the device with the MDM.

Cloud Secure Solution integrates with multiple MDM servers (Pulse Workspace, AirWatch, and MobileIron) for mobile device management and compliance checks.

Select **MDM Server** section:

1. Click **Add New** and select the PWS as MDM server and click Done.
2. Enter **Server name**.
3. Enter Registration host and Registration code details from **Step 9** of Pulse Workspace Configuration.
4. Click **Browse** and upload a PWS VPN certificate. See VPN Cert of Pulse Workspace Configuration.
5. Click **OK**.

Figure: UX: Pulse Workspace MDM Settings



To configure Airwatch/MobileIron MDM Server:

1. Under MDM Server, click **Add New** and select **Airwatch/MobileIron** as MDM server.
2. Enter **Server Name**.
3. Enter **Server URL**.
4. Enter **Viewer URL**.
5. Enter **Username** and **password** for communicating with the MDM server.
6. Enter **Tenant Code** [Not Applicable for MobileIron].

7. Click **Browse** and upload MDM certificate.
8. Click **OK**.

Figure: UX: AirWatch MDM Settings

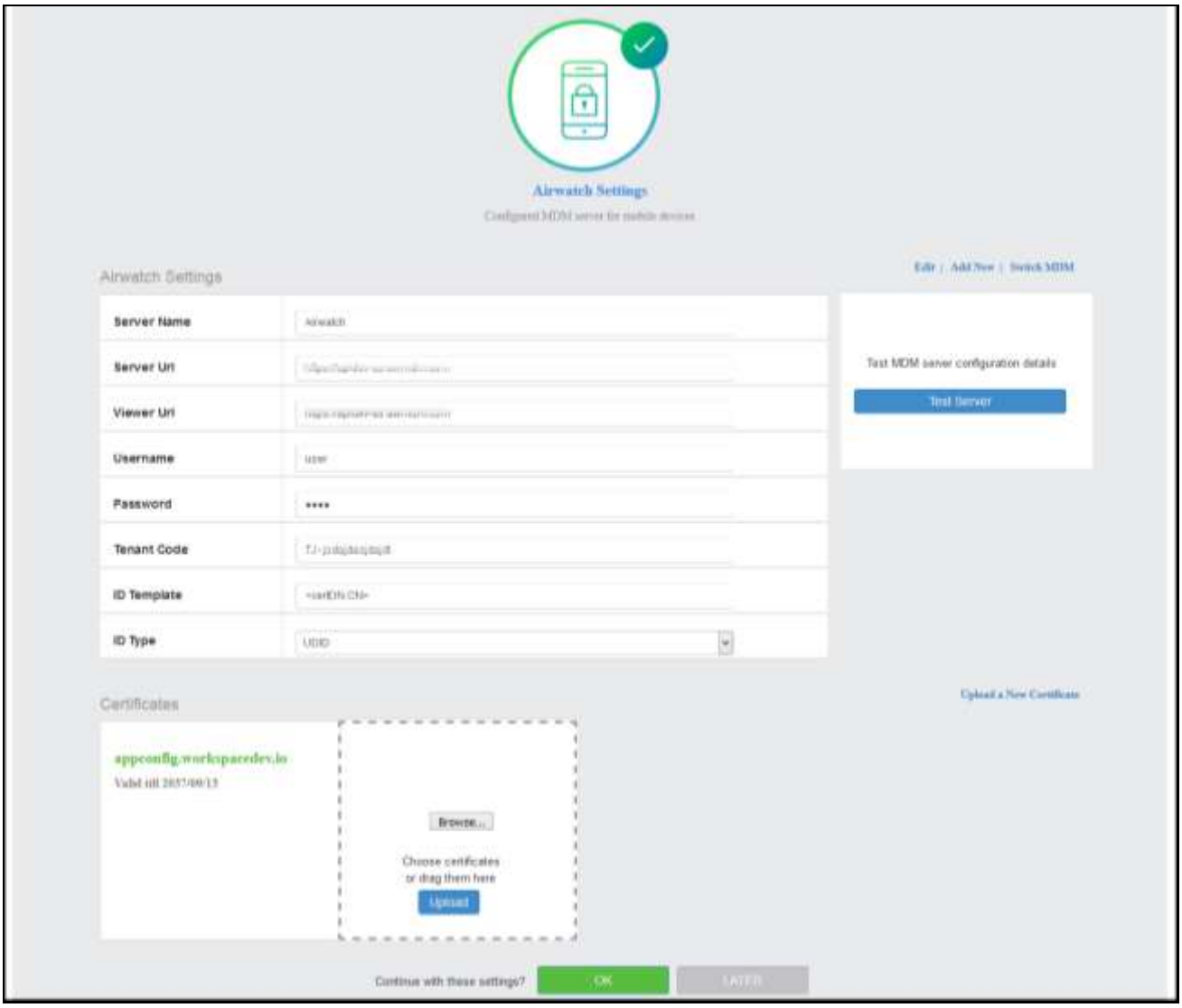
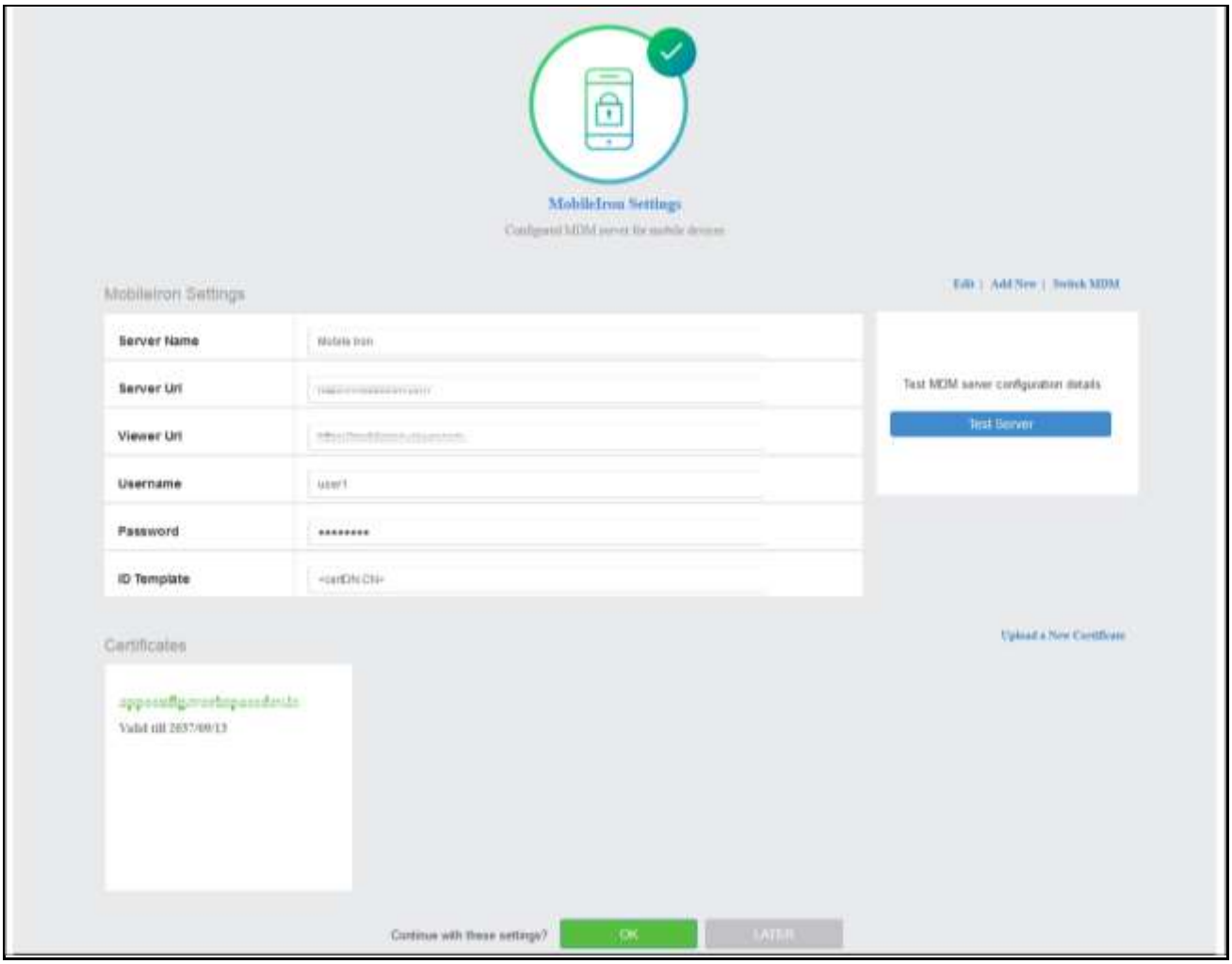


Figure: UX: MobileIron MDM Settings



Note:

- Cloud Secure UX allows validating the configurations and connections. “Test Server” verifies the connection between PCS and MDM server.
- Cloud Secure UX allows using the existing MDM configuration in PCS. Select Switch MDM to switch between already configured MDM servers or to add a new MDM server.

Configuring Compliance Policies

Cloud Secure supports compliance for Windows and Macintosh desktops/laptops through Host Checking capabilities and for mobile devices through MDM servers. The mobile compliance policies are based on device attributes retrieved from MDM server.

To configure the compliance policies for Desktops.

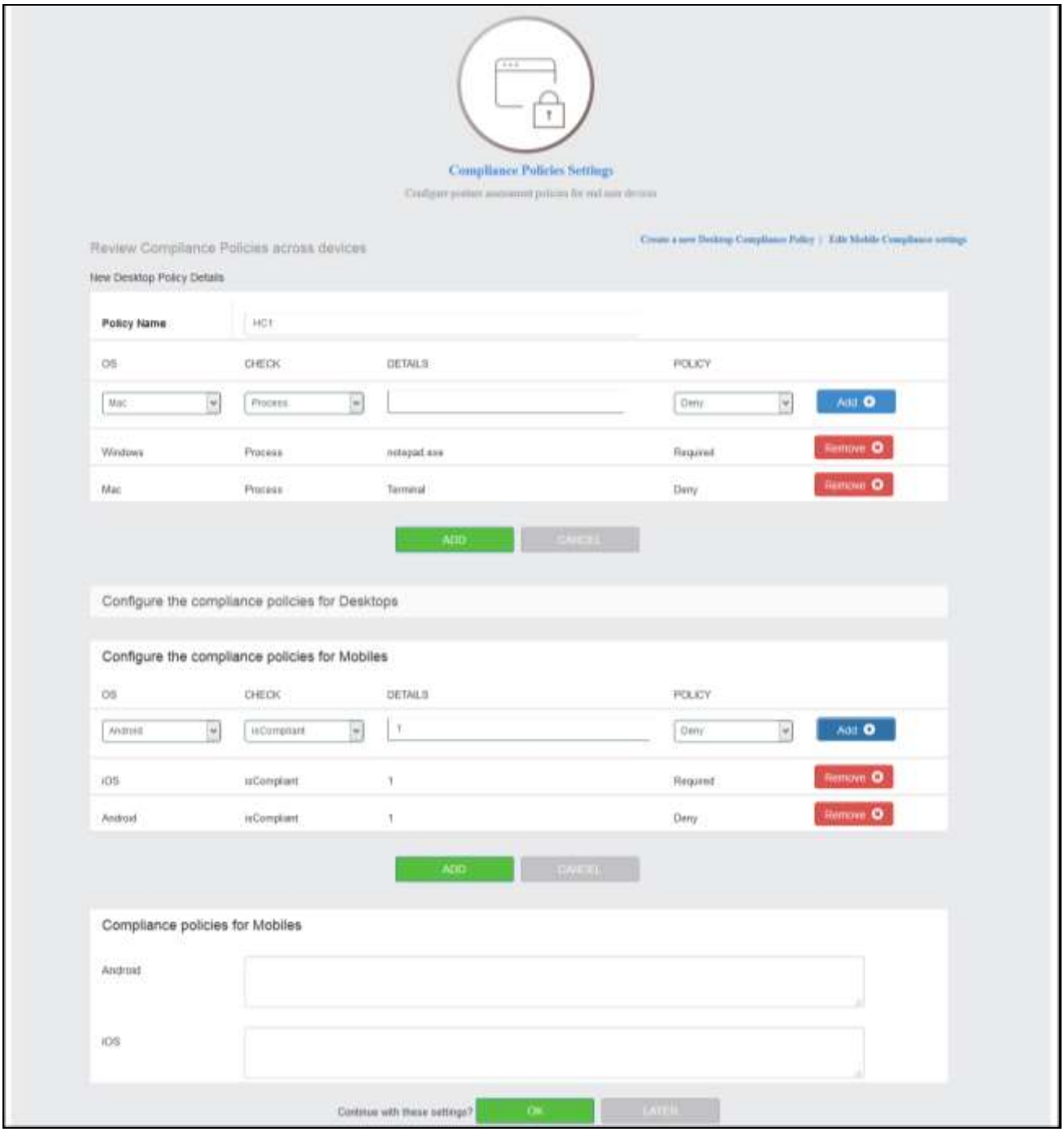
1. Select Compliance Policies section.
2. Under **Compliance Policies > Create a New Desktop Compliance Policy**.
   a. Enter **Policy Name**. Select the OS and Compliance check from the respective drop down and specify the details.
3. Click **ADD**.
4. Click **OK.**

Note: Cloud Secure UX allows reusing existing Host Checker Policies by enabling the checkbox from the pre-filled compliance policies. For desktops, only Antivirus, Firewall, and Process Host Checker policies are supported.

To configure the compliance policies for Mobiles:

1. Under **Compliance Policies > Edit Mobile Compliance settings**. Select the OS and Compliance check from the respective drop down and specify the details.
2. Click **ADD.**
3. Click **OK.**

Figure: UX: Compliance Policies

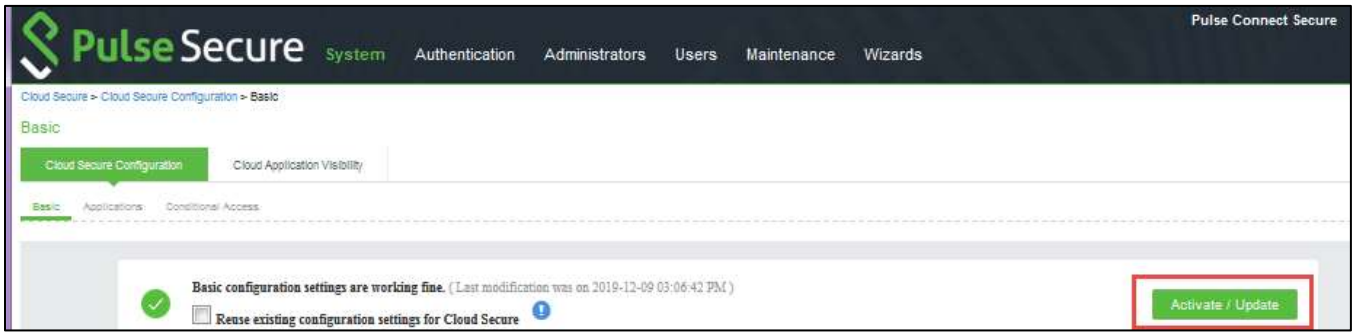


Note: Multiple Attributes can be configured for Compliance Checks. Admin can also create custom expression for mobile compliance checks in the Expression Field manually.

The mobile compliance policies are based on device attributes retrieved from PWS. Refer to Configuring **Pulse Workspace for Mobile Compliance Policies** for understanding how the compliance policies are retrieved/evaluated in PWS.

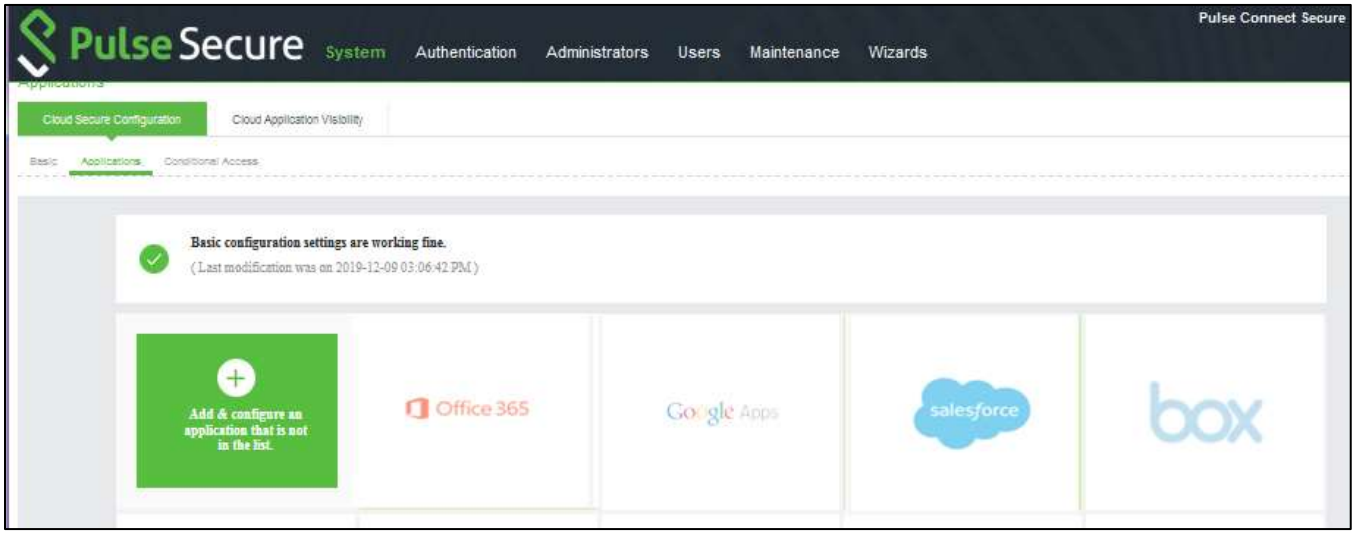
Click **Activate/Update** after the advanced configurations are completed. After activating, the administrator will be redirected to **Applications** page. Click **Basic** to go back to basic configuration page.

Figure: UX: Summary



Configuring Applications

The Admin can configure Cloud Applications as Peer SP once the basic configurations are completed and activated. Once the basic configurations are activated, Admin can click Applications tab to go to Applications configuration page. The widely used applications (O365, Google Apps, salesforce, box, and Zendesk) are available by default and come with pre-populated application settings for ease of configuration. The Administrator can also choose to add new applications by clicking **+ Add & configure an application that is not in the list**.



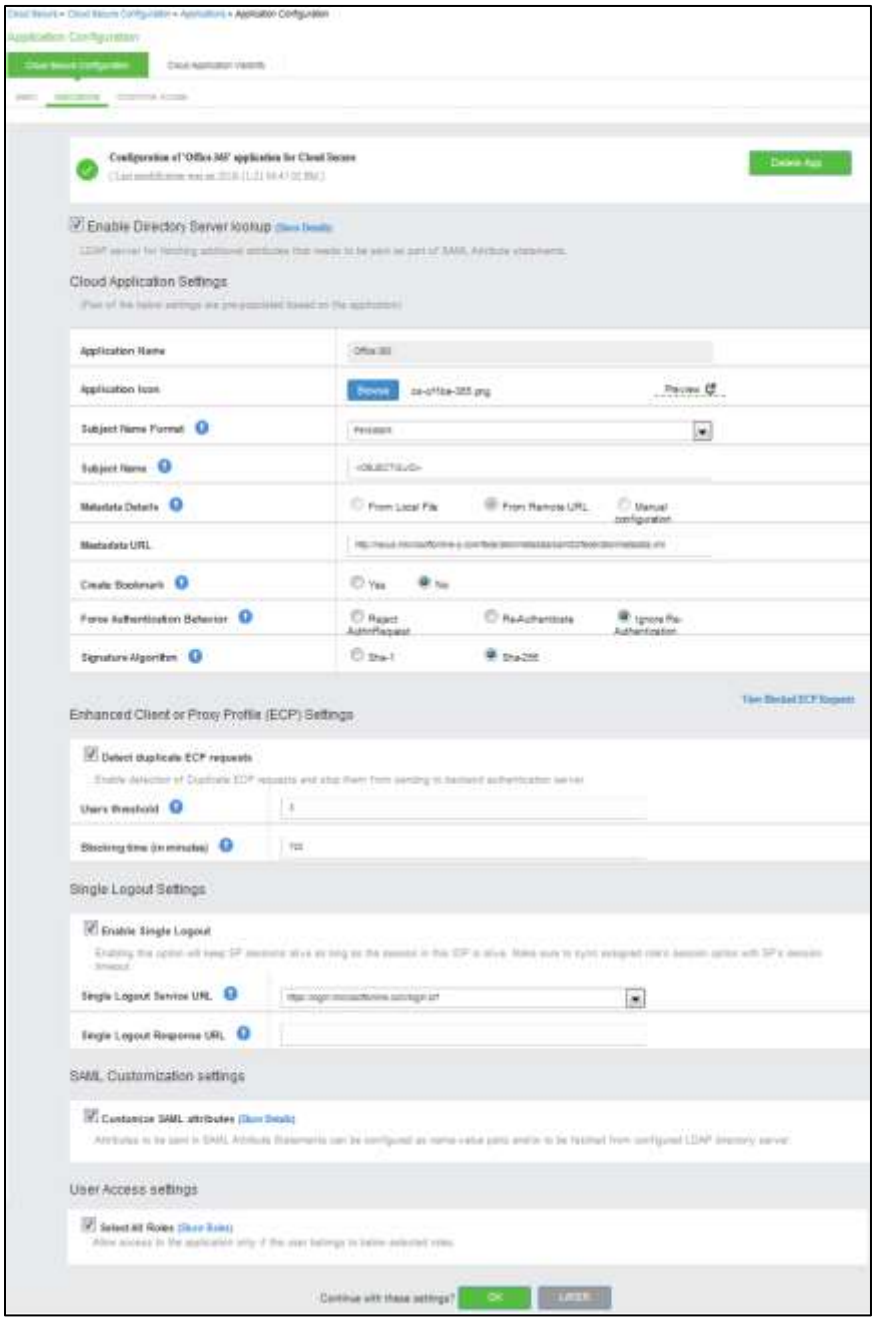
To configure O365 application:

1. Click the **Office 365** icon to configure the application.
2. Select **Enable Directory Server lookup** to enable LDAP server for fetching additional attributes. If the LDAP server is already configured the details will be pre-populated. Admin also has a provision to create a new LDAP server in the same section.
3. Under Cloud Application Settings:
   a. Enter the application name.
   b. Click Browse and select the application icon.
   c. Enter the Subject Name Format.
   d. Enter the Subject Name.

e. Under Metadata details, the metadata file is uploaded from a remote URL by default. The Admin can also choose to upload the metadata file from a local file or through manual configuration by entering the Entity ID and Assertion Consumer Service URL.
f. (Optional) Set **Create Bookmark** to **Yes** to support IdP initiated SSO.
g. Set the Force Authentication Behaviour to **Ignore Re-Authentication**.
h. Set the Signature Algorithm to Sha-1 or Sha-256.

4. Under Enhanced Client or Proxy Profile (ECP) Settings.
   a. Enable **Detect duplicate ECP request** to detect and stop from sending any duplicate ECP requests to backend AD server.
   b. Enter the user threshold.
   c. Enter the blocking time in minutes.
5. Under **SAML Customization & User Access settings**, Assign the application to applicable roles.
6. Click **OK**.

Figure: Application Configuration



The following screen with a green tick mark on the Office 365 application is displayed after a successful configuration.

Figure: O365 Configuration Completed

Note: The Administrator can also choose to delete an application using the **Delete App** option on the Application Configuration page.

Configuring IdP Initiated Single Logout

With Single Sign On service, users with role-based access are able to log into and access all SP provided services. The Single Logout feature allows the administrator to deny user access to services and initiate Single Logout in the following scenarios:

- machine goes out of compliance during a session.
- session times out.
- administrator deletes the session in PCS configured as Identity Provider (IdP).
- user logs out from PCS (configured as IdP) landing page.

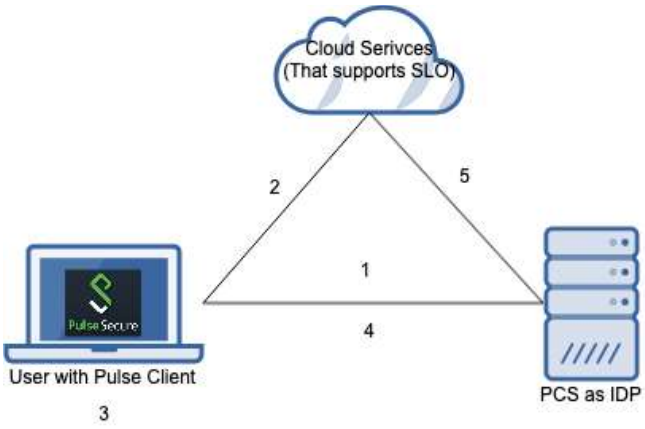
Note:

- When Single Logout is initiated by PCS configured as IdP, all the SPs linked to the session will be sent SLO requests.
- The IdP session is not affected by the SP's logout.
- IdP SAML session timeout can be either role-based or configured via Identity Provider page.
- Maximum timeout of SAML sessions could be increased, so that it matches with or be greater than the SP's Max Session timeout to get a seamless experience.

Prerequisites

- SP should be configured for Single Logout option even before uploading the SP's metadata to IdP. Otherwise, the metadata will not have the Single Logout details.
- If the user is using the same SP with multiple devices, it is recommended to have multi-user session enabled in PCS.

Figure: Flow Diagram



Scenario 1: When the machine goes out of compliance while user is accessing SPs

1. Pulse Client establishes connection to PCS (as IdP) with full access or partial access.
2. From the same machine, user accesses SPs that support SLO.
3. After some time, Pulse Client goes out of compliance.
4. Pulse Client reports the compliance check in server and switches to a remediate role that does not have access to SPs.
5. PCS (as IdP) sends an SLO to SP's Logout URL and there by user needs to SSO again to access the resource.

Since the Remediation role do not have access to the SPs, SSO will be denied and hence the user will be denied access.

Scenario 2: When the user session times out

1. Pulse Client establishes connection to PCS (as IdP) with full access.
2. From the same machine, user accesses SPs that support SLO.
3. User session times out.
4. PCS deletes the user session.
5. PCS (as IdP) sends an SLO to all the SPs that are associated with the user session.

Scenario 3: When the administrator deletes the user session from the PCS (as IdP) active user page

1. Pulse Client establishes connection to PCS (as IdP) with full access.
2. From the same machine, user accesses SPs that support SLO.
3. User gets access to SP through SSO.
4. Administrator deletes the user session from the active user's page.
5. PCS (as IdP) sends an SLO to all the SPs that are associated with the user session.

Scenario 4: When the user disconnects from PCS (as IdP)

1. Pulse Client establishes connection to PCS (as IdP) with full access.
2. From the same machine, user accesses SPs that support SLO.
3. User disconnects the Pulse session.
4. PCS deletes the user session.
5. PCS (as IdP) sends an SLO to all the SPs that are associated with the user session.

Note: After SLO is sent, the response is handled and logged in user access log and policy tracing.

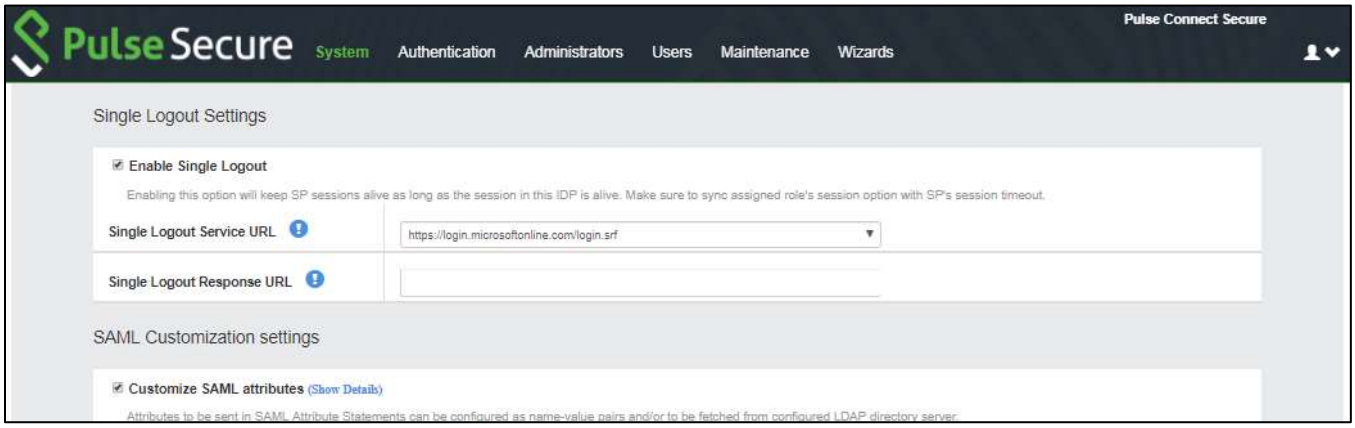
Configuring Single Logout

The administrator can configure the Single Logout option for the applications.

To configure Single Logout:

1. Select **Cloud Secure > Cloud Secure Configuration > Applications**.
2. Click the application icon to configure the application.
3. In the Single Logout Settings section, select the **Enable Single Logout** option.

Figure: Single Logout



4. Use one of the following to configure Single Logout:

- **Metadata upload from local file** - Administrator needs to configure SP for both SAML SSO and SLO. The metadata from SP needs to be provided to PCS which is acting as IDP.
- **Manual configuration** - Administrator needs to enter the SLO URL of SP manually along with other SSO configurations.
- **Using Remote URL** - Administrator needs to configure SP for both SAML SSO and SLO. The SP's metadata will be parsed from the online URL directly. The SLO details will be automatically populated.

End User Workflow

Browser based flow (SP initiated)

In the SP initiated case, when the user logs into an SP by authenticating with PCS, the user is allowed SSO to other SPs from the same browser. If the user logs out of the SP, then SLO is sent to all other SPs associated with the IdP.

Browser based flow (IdP initiated)

In the IdP initiated case, it is bookmark flow. This has two scenarios - with rewriter enabled and without rewriter enabled. In both the cases, when the user session gets logged out, the SLO is sent to all the SPs in which it was already logged in.

Note: If the bookmark is created from 3rd Party IdP page, then this SLO is not applicable.

Single user signed in with multiple devices with multi-users session enabled in PCS

Multiuser session is enabled in Users > User Roles > RoleName > General > Session Options. If multiuser session is not enabled for SLO, then user can use only one device/session.

Pulse Desktop based flow

User can perform Single Sign on using Pulse Desktop client. When Pulse Desktop client is connected to PCS as IdP, users can access any SP for which the role has access. The user can sign into SP directly as long as the connection exists. If the user logs out from Pulse Desktop client, then an SLO will be sent to all those SPs to which SSO was granted there by clearing all the SPs associated with the PCS SSO session.

Single user signed in with multiple devices without multi-users session enabled in PCS

In the scenario where user performs multiple logins with a single user session, only one device can be used by the user at any given time. The user cannot use multiple devices with the same user name. Because, when the user tries to use another device, when SSO happens on the 2nd device, the first device will be sent an SLO. which means, the session is teared down and re-created in PCS. So, only one device can be active for one user session at any given point of time.

Single user session in PCS and multiple logins from a single device

Through Pulse Desktop client connection, the user can sign into same SPs from different browsers or apps as many times as the SSO is in place. But, if the user tries to use two different browsers or use a browser-based login and another app-based login without Pulse Desktop client, then only one will be given access at any given point of time.

Note: By default, SLO is not enabled for any new peer SPs. Administrator has to manually configure it.

Configuring Pulse Policy Secure for On-Premise/Location Awareness

Cloud service SSO for On-Premise users is achieved by sharing PPS session information to PCS and using this imported IF-MAP session information to generate SAML response. Configure Pulse Policy Secure as Federation Client and associate it to a Federation Server.

PPS retrieves mobile device attributes from MDM server and uses it for compliance assessments whereas in desktops, native Host Checker is used for compliance checks.

This section describes the following tasks:

- Configuring Pulse Policy Secure as IF-MAP Client
- Configuring Pulse Policy Secure as IF-MAP Federation Server
- Configuring Pulse Connect Secure as IF-MAP Client

Configuring Pulse Policy Secure as IF-MAP Client

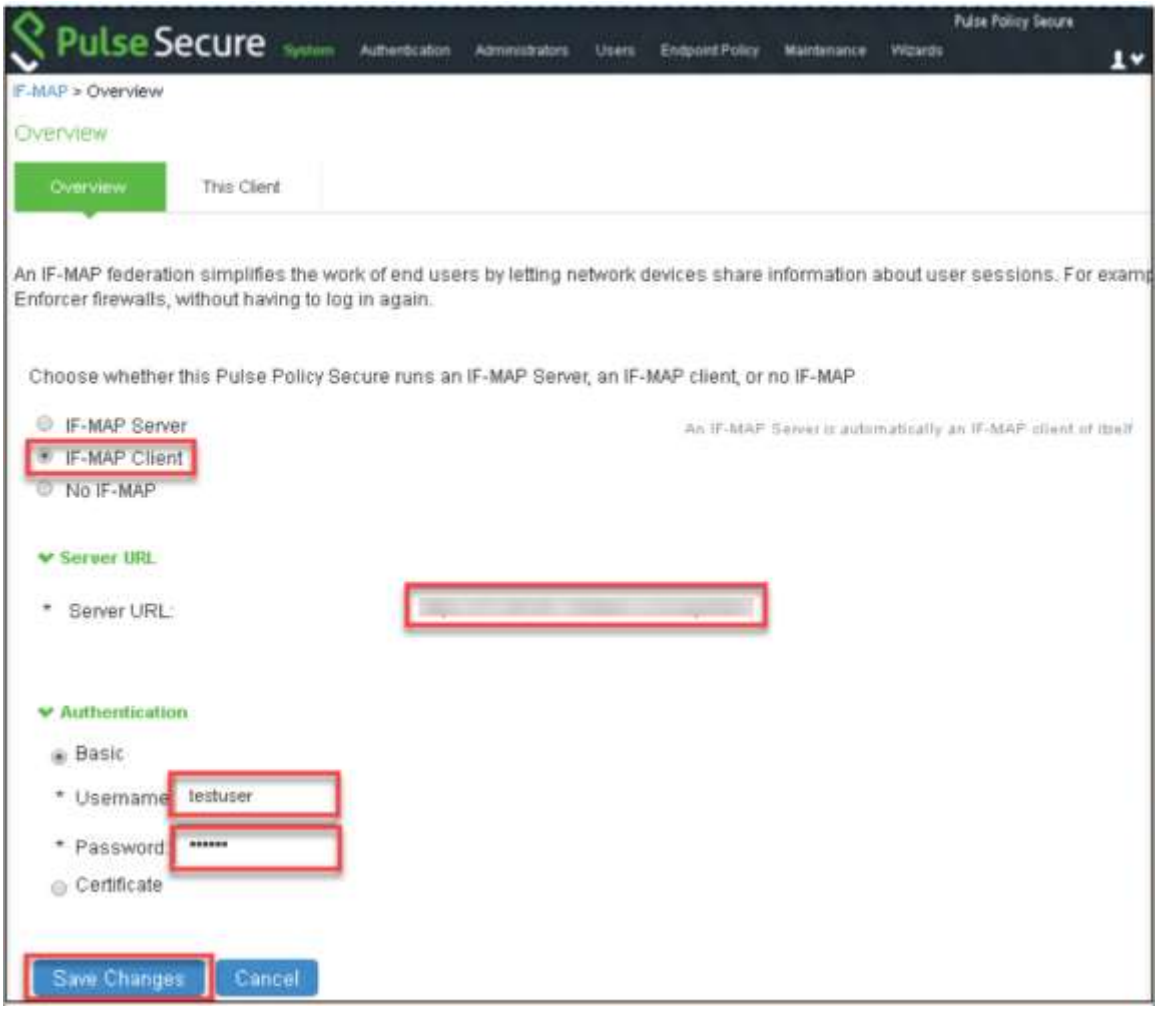
Follow below steps to configure Pulse Policy Secure as Federation Client, enable 802.1x and configure MDM Server:

1. Log into Pulse Policy Secure admin console Environment Details.
2. Navigate to **System > Configuration > Certificates > Trusted Server CAs**.
3. Click **Import Trusted Server CA...**.
4. Click **Browse** and select the CA certificate file.
5. Click **Import Certificate**.

Figure: Import Trusted Server CA on PPS

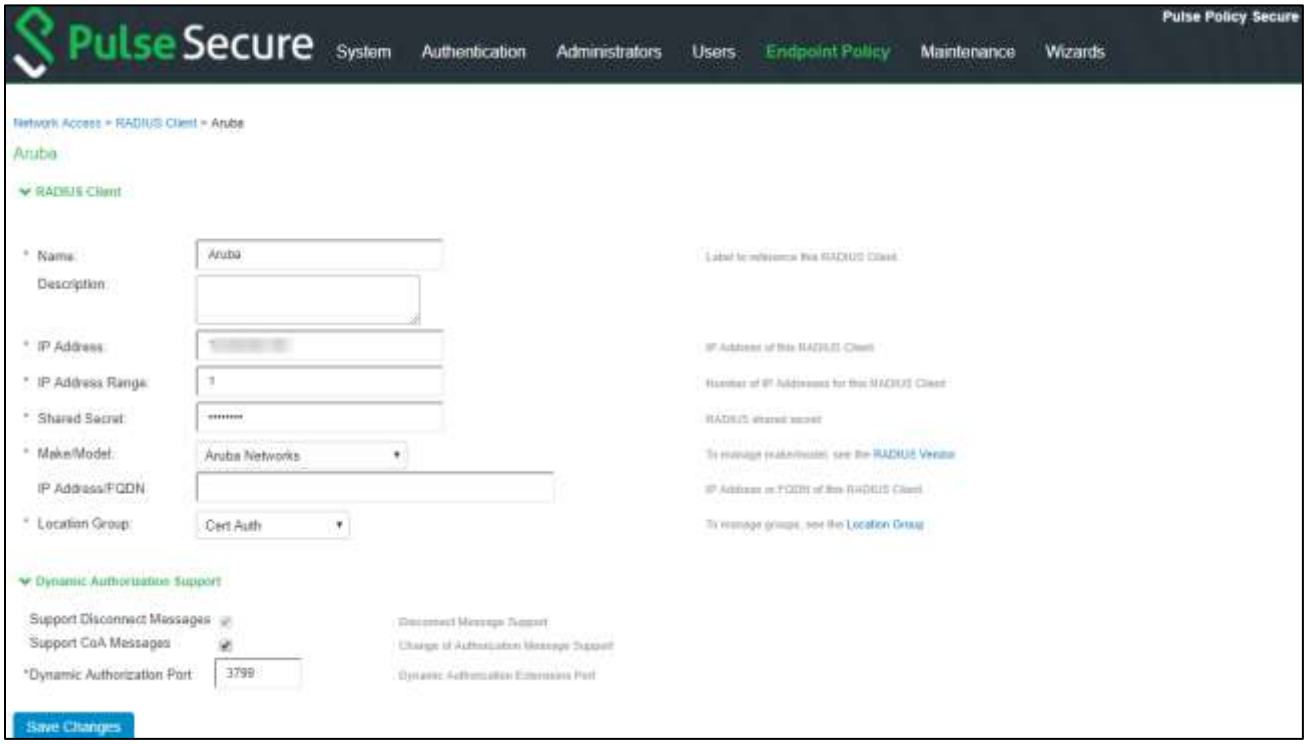
6. Navigate to **System > If-MAP Federation > Overview**.
7. Select **IF-MAP Client** and provide the following details:
   a. Under Server URL, provide **IP address** of Federation Server.
   b. Select **Basic** under Authentication and provide same **Username** and **Password** provided in Step 4 of IF-MAP Federation Server configuration.
   c. Click **Save Changes.**

Figure: Enable IF-MAP Client on PPS



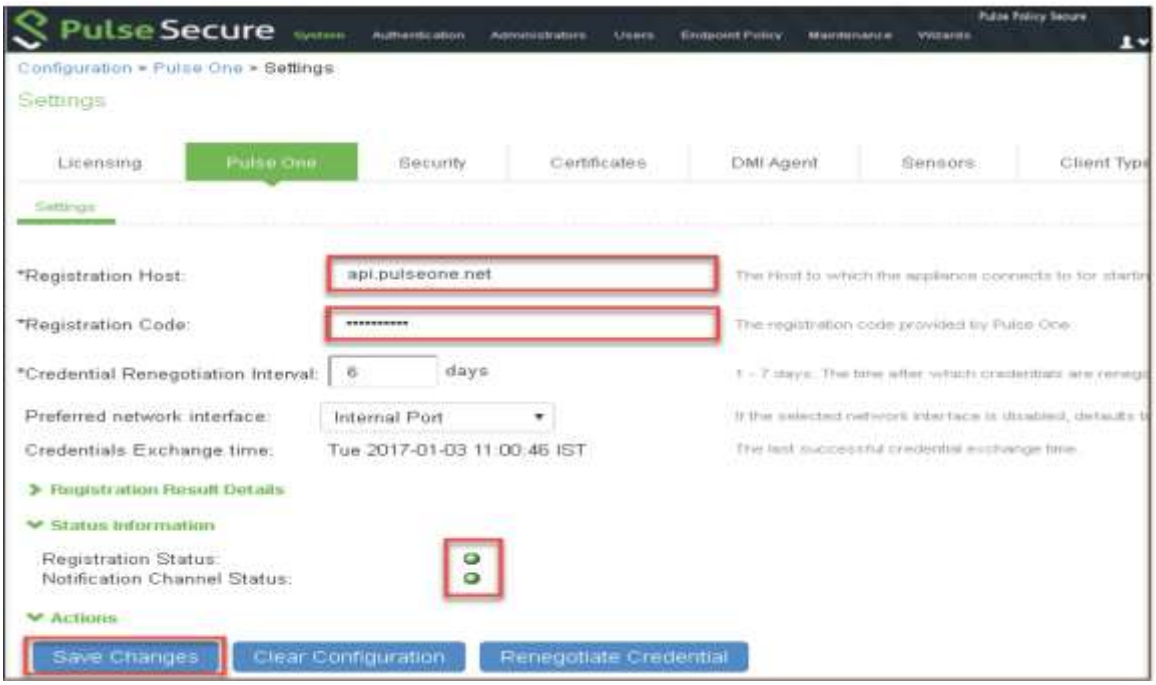
8. Navigate to **Endpoint Policy > Network Access > RADIUS Client**.
9. Click **'New RADIUS Client...'** and provide the following details:
    a. Enter **Name.**
    b. Enter the **IP Address** of RADIUS Client.
    c. Enter **Shared Secret**.
    d. Select **Make/Model**.
    e. Select **Location Group**.
    f. Select **Support Disconnect Messages** and/or **Support CoA Messages** (Optional)
    g. Enter the port value for dynamic authorization.
    h. Click **Save Changes**.

Figure: Configure Radius Client



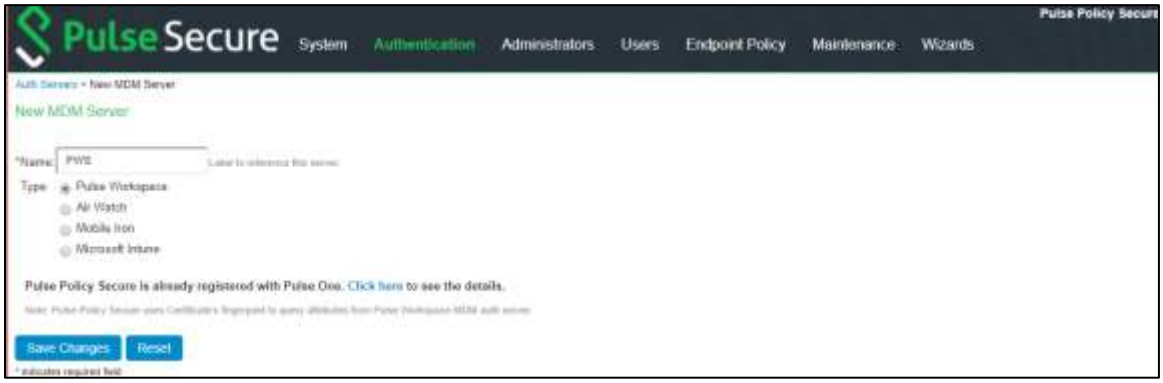
10. Navigate to **System > Configuration > Pulse One > Settings** to register PPS with Pulse One and provide the following details
    a. Enter **Registration Host** and **Registration Code** details from **Step 9** of Pulse Workspace Configuration.
    b. Click **Save Changes**.
    c. Registration Status and Notification Channel Status under Status Information section should turn green after few seconds.

Figure: Pulse One Settings



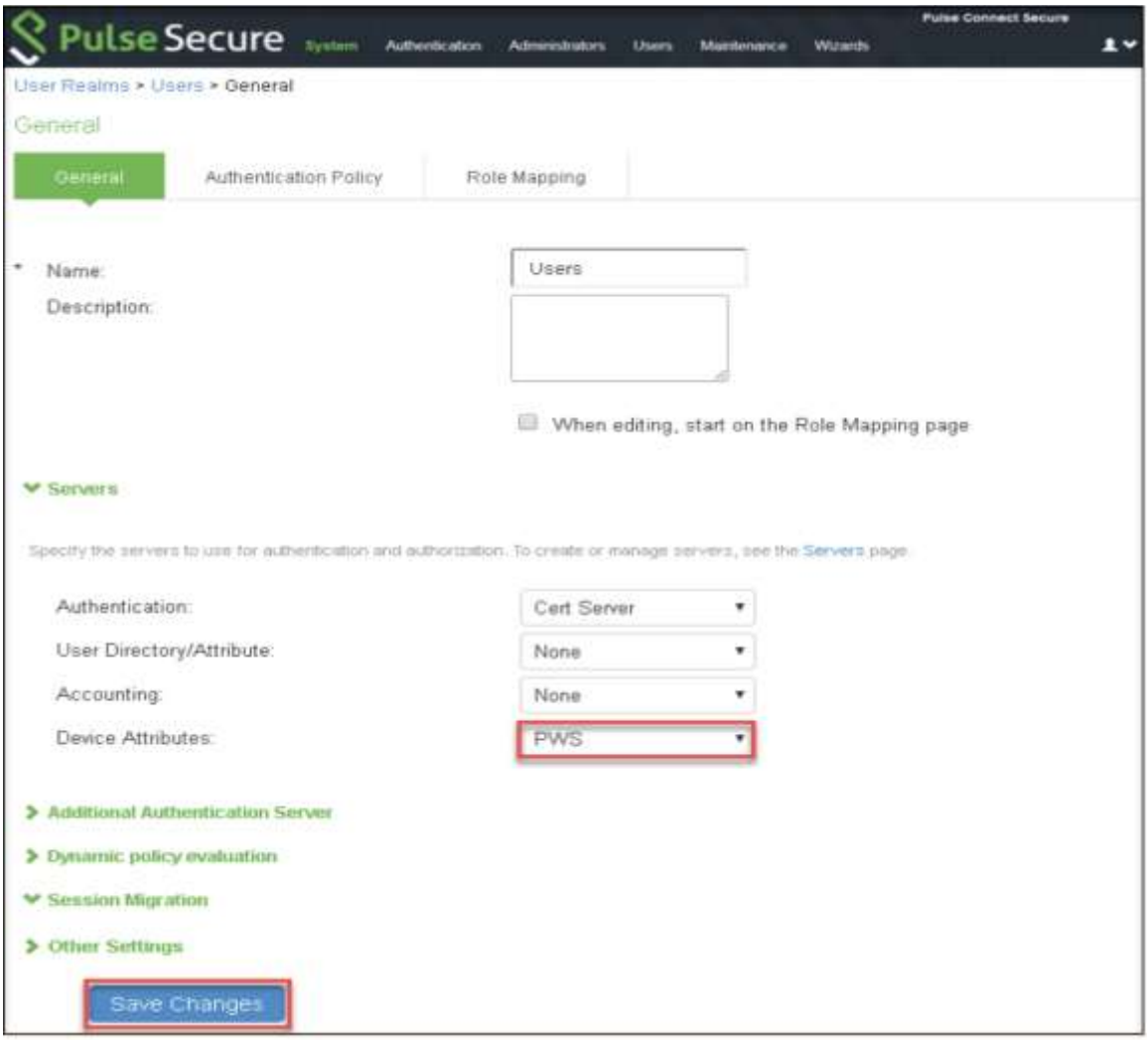
11. Navigate to Authentication > Auth Servers to create Pulse Workspace MDM Authentication Server.
12. Select New Server of Type **'MDM Server'** and Click New Server.
    a. Enter **Name**
    b. Select **Pulse Workspace**.
    c. Click Save Changes.

Figure: MDM Server



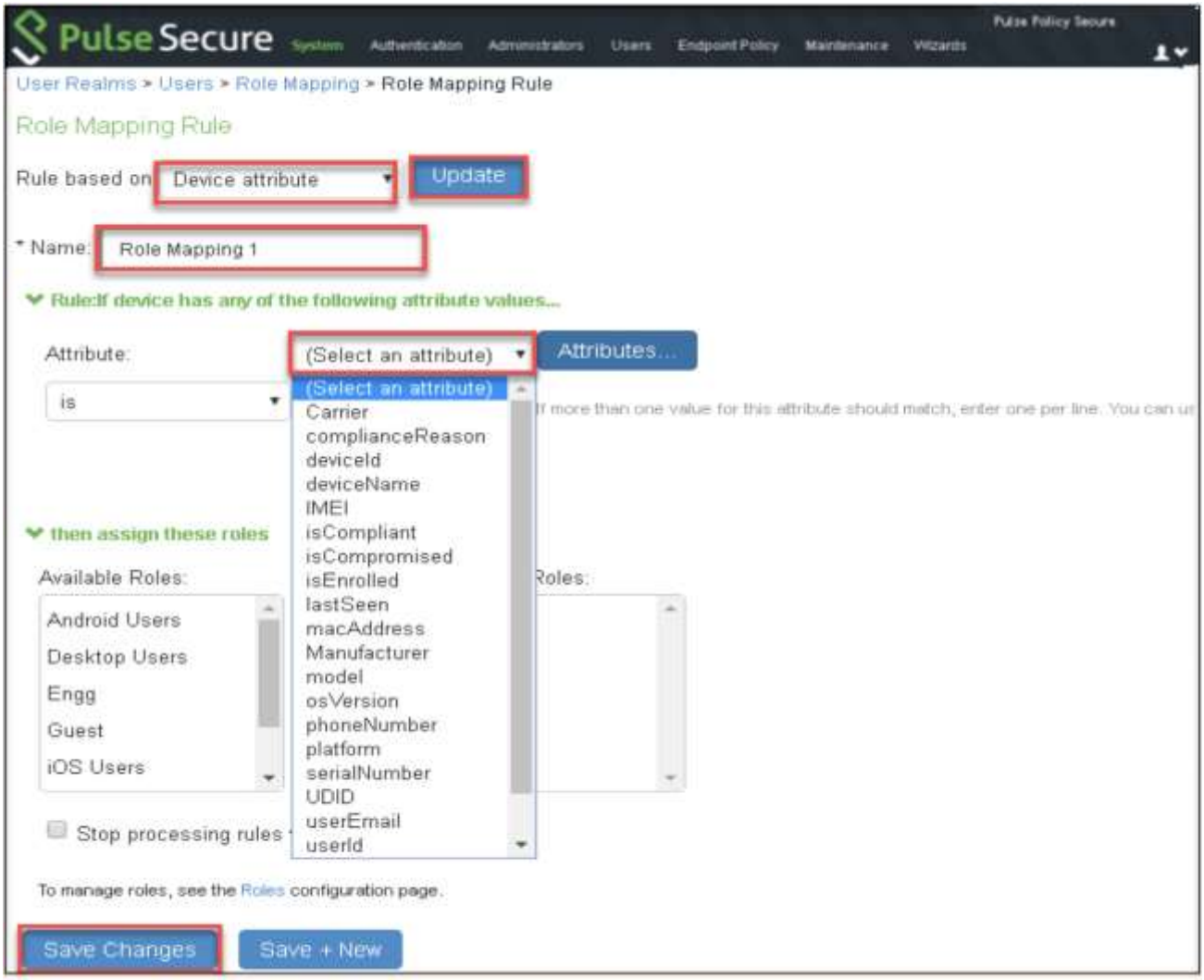
13. Navigate to Users > User Realms. Select the desired realm, configure PWS MDM Server created in Step 6 above as Device Attribute Server and click Save Changes.

Figure: Configure User Realm



14. (Optional) Navigate to **Role Mapping tab** of the user realm to create role mapping rules. Click **'New Rule...'** and provide following details:
    a) Select **Rule based on Device attribute** and Click **Update.**
    b) Enter **Name.**
    c) Select an Attribute and provide a value.
    d) Assign required roles.
    e) Click **Save Changes.**

Figure: Configure Role Mapping Rules



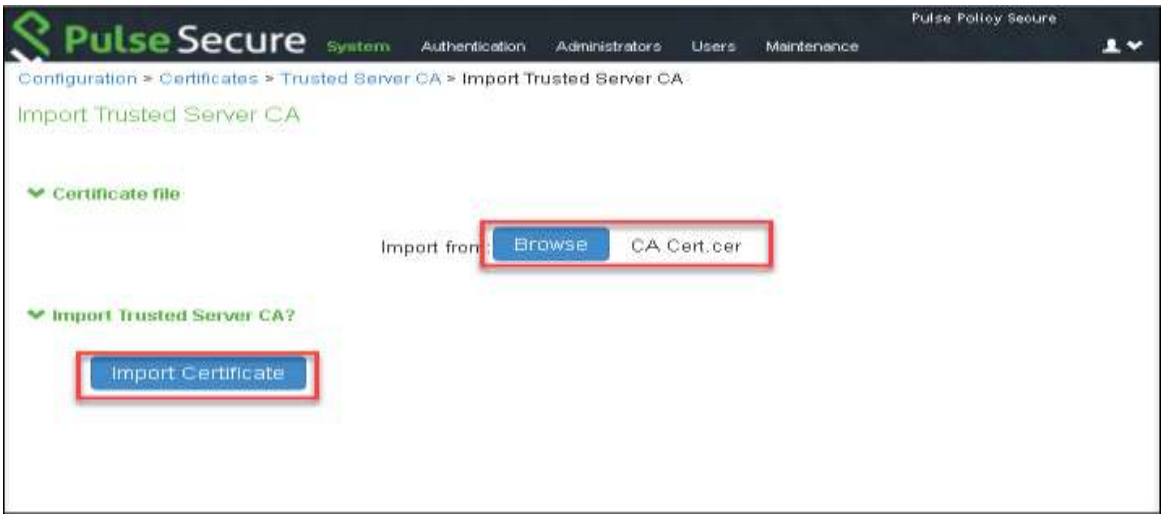
Note: Compliance check for mobile users will be done by MDM Server (PWS/MobileIron/ AirWatch). For desktop users, PCS/PPS uses Host Checker functionality for compliance check.

Configuring Pulse Policy Secure as IF-MAP Federation Server

Follow below steps to configure PPS as IF-MAP Federation Server:

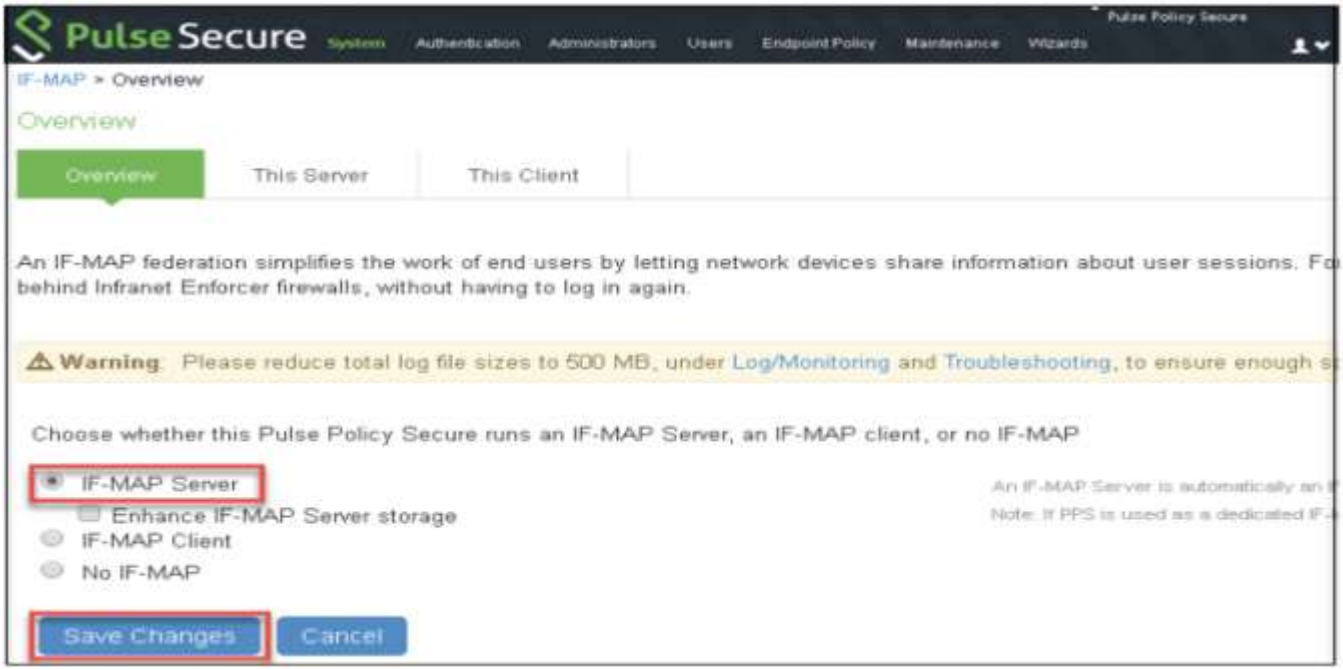
1. Log into Pulse Policy Secure admin console.
2. Navigate to **System > Configuration > Certificates > Trusted Server CAs**.
   Click **'Import Trusted Server CA...'**. Browse CA certificate file and click **'Import Certificate'.**

Figure: Import Trusted Server CA on Fed Server



3. Navigate to **System > If-MAP Federation > Overview**. Select **IF-MAP Server** and **Save Changes.**

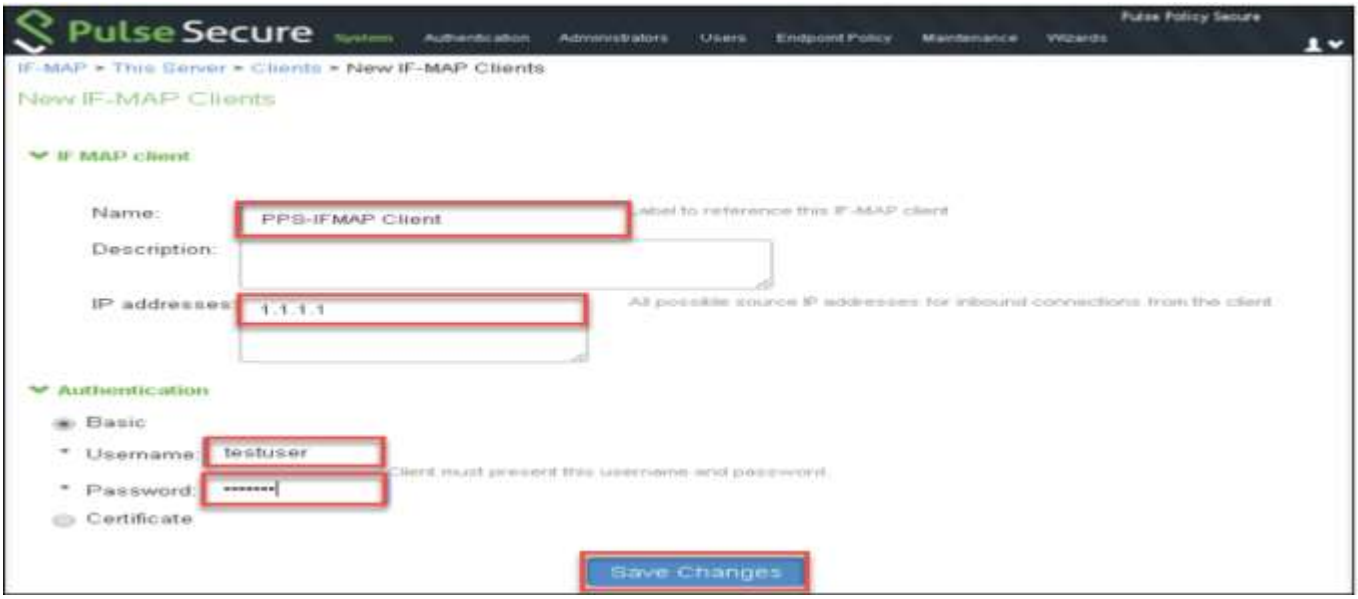
Figure: Enable IF-MAP Server



4. Navigate to **System > IF-MAP Federation > This Server > Clients.** Click **'New Client...'** and provide following details to configure PCS/PPS as Federation Client (Configure both PCS and PPS as Federation Clients).
   a) Provide **Name.**
   b) Provide **IP address** of PCS/PPS.
   c) Select **Basic** under Authentication and provide **Username** and **Password.**

5. Click **Save Changes.**

Figure: Add IF-MAP Client



Configuring Pulse Connect Secure as IF-MAP Client

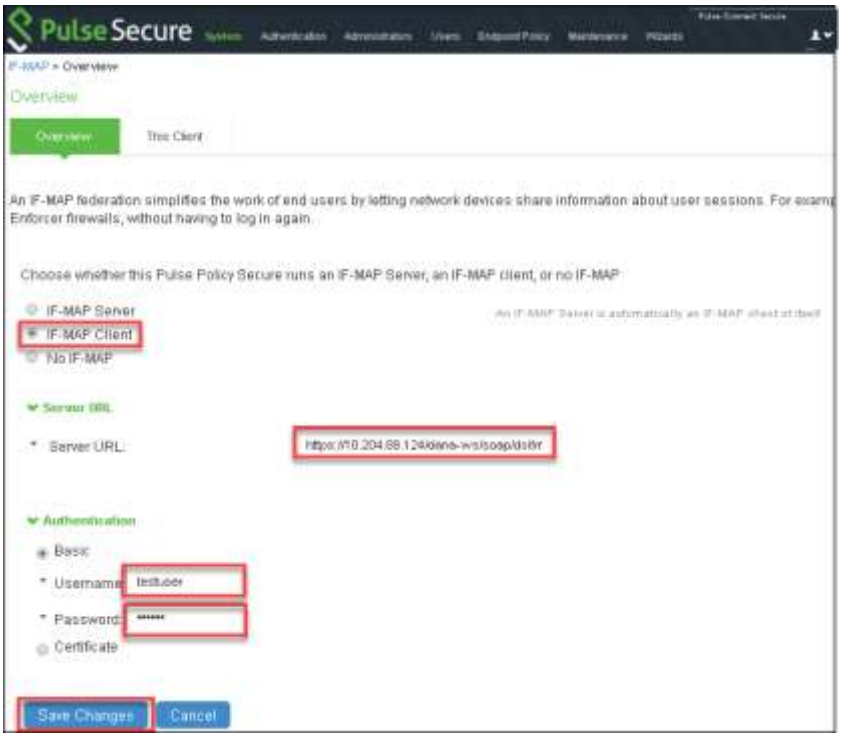
Follow below steps to configure Pulse Connect Secure (SAML IDP) as Federation Client: and enable Re-use existing IF-MAP session option:

1. Log into Pulse Connect Secure admin console
2. Navigate to **System > Configuration > Certificates > Trusted Server CAs**. Click **'Import Trusted Server CA...'**. Browse to the CA certificate file and click **'Import Certificate'.** Ensure that the certificate of the CA that signed the IF-MAP server certificate is added.

Figure: Import Trusted Server CA on PCS

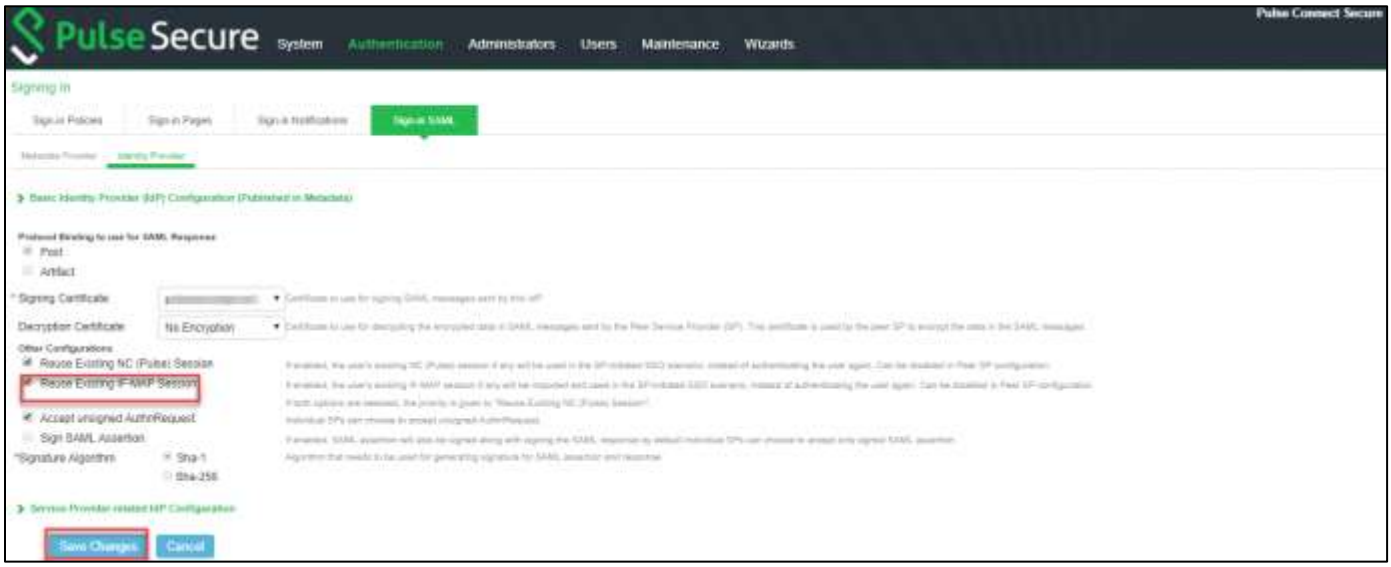
3. Navigate to **System > If-MAP Federation > Overview**. Select **IF-MAP Client** and provide following details:
   a. Under Server URL, provide **IP address** of Federation Server
   b. Select **Basic** under Authentication and provide same **Username** and **Password** provided in Step 4 of Federation Server configuration
   c. Click **Save Changes**

Figure: Enable IF-MAP Client on PCS



4. Navigate to **Authentication > Signing In > Sign-in SAML > Identity Provider.** Select **'Re-use Existing If-MAP Session'** option, specify the signature algorithm and click **Save Changes**

Figure: Enable Re-use Existing IF-MAP Session



5. Select desired Peer SP configured, enable **'Re-use Existing If-MAP Session'** option and click **Save Changes.**

Note: Once both PCS and PPS are enabled as IF-MAP Clients, verify that the status for both the clients is green on Federation Server.

Configuring Pulse Workspace

Pulse Workspace acts as Mobile Device Management (MDM) Server to manage mobile devices and to evaluate compliance posture of the devices.

- Configuring Pulse Workspace
- Configuring Pulse Workspace for Mobile Compliance Policies
- Configuring Pulse Workspace for Location Awareness
- Configuring On-Demand VPN for Android devices

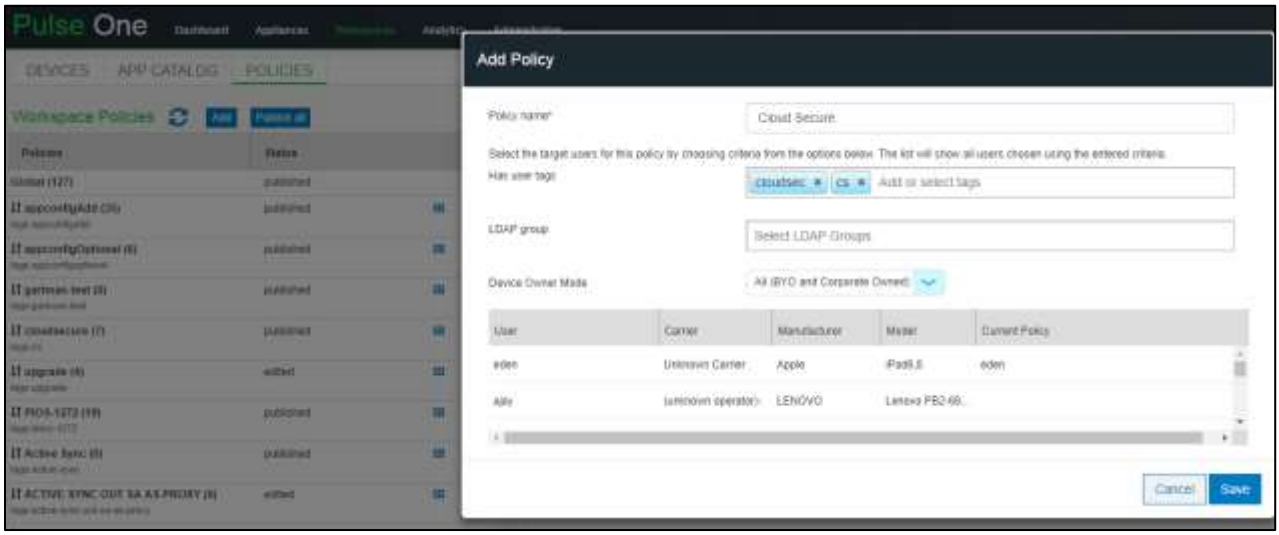
For Cloud Secure solution, Pulse Workspace should be configured with:

- Policy configured with VPN properties and iOS/Android applications enabled with Per app VPN.
- Workspace user.
- PCS appliance.
- Configure Wi-Fi profile and add PPS appliance for On-Premise solution.

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

1. Log into the Pulse One admin console.
2. Use existing Global policy or create a new policy. To create new policy, select **Workspaces > Policies > Add.**
    a. Enter the **Policy name.**
    b. Under **Has user tags,** Add or select tags.
    c. Click **Save**.

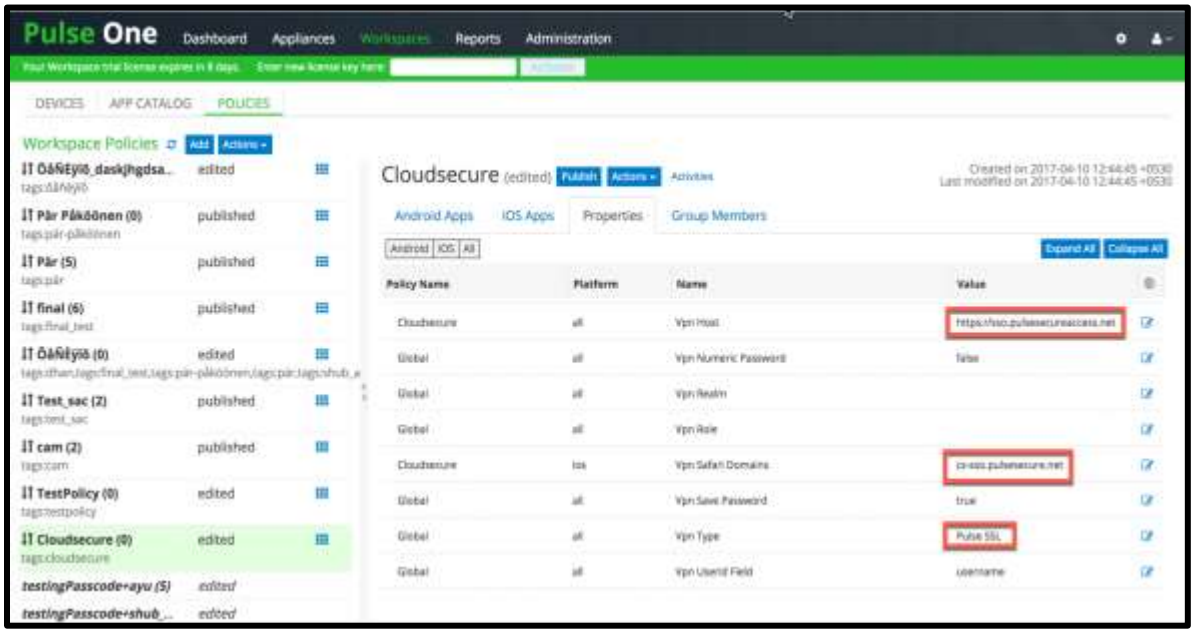
Figure: Add Policy



3. Modify the VPN properties of new policy or Global policy to support Per App VPN. Navigate to the **Properties** Tab. Scroll down to 'VPN' section, click the **Edit** icon against each field below and provide the following values:
    a. Set **Use L3 VPN** to true (in case of L3 VPN).
    b. VPN Host = https:// <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: Modify VPN Properties

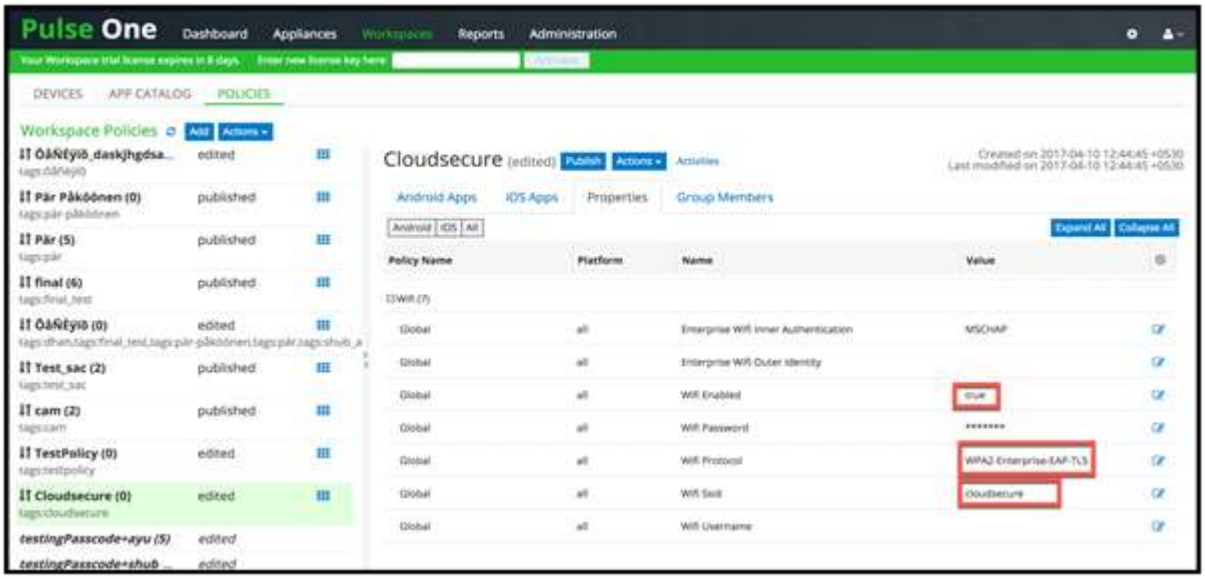


4. (Optional) Modify the 'Wifi' Properties of the new policy or Global policy. Navigate to **Properties** tab. Scroll down to 'Wifi' section, click the **Edit** icon against each field below and provide following details:

    a. Set **Wifi Enabled** to true.
    b. Select **WPA2-Enterprise-EAP-TLS** as Wifi Protocol.
    c. Provide Wifi Ssid.
    d. Click **Publish.**

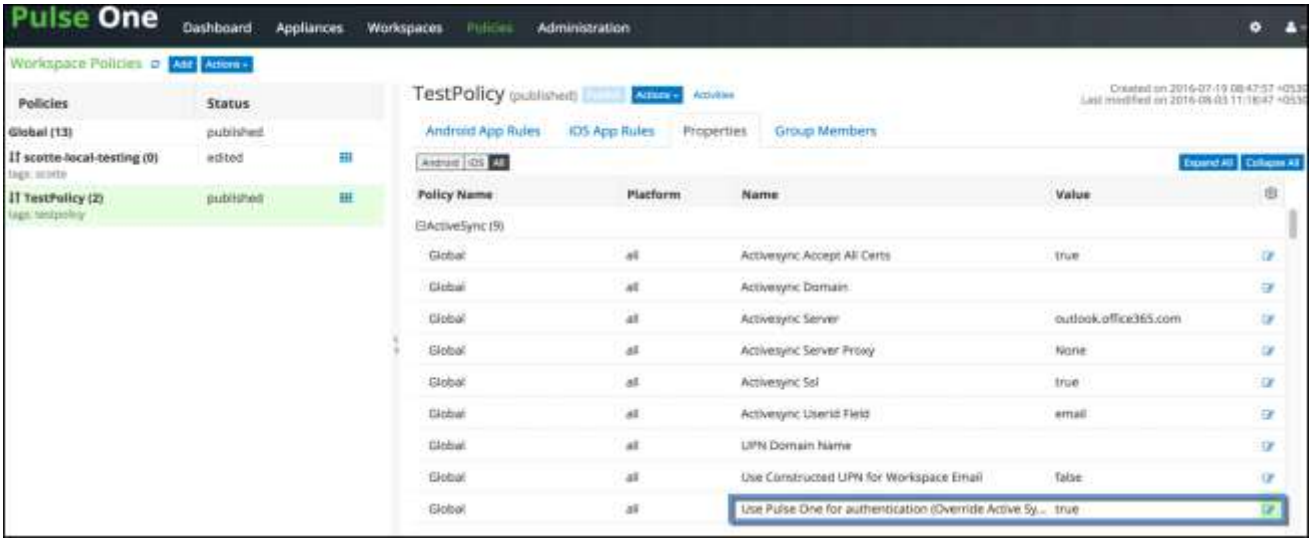
Note: SSO access to On-Premise Mobile Users requires Wifi Configurations.

Figure: Configure WiFi Profile



5. (Optional) Modify the Active Sync properties.
    a. Set Activesync Accept All Certs to Yes.
    b. Set Activesync Server to outlook.office365.com.
    c. Set **Use Pulse One for authentication** (Override Active Sync Server) to Yes.

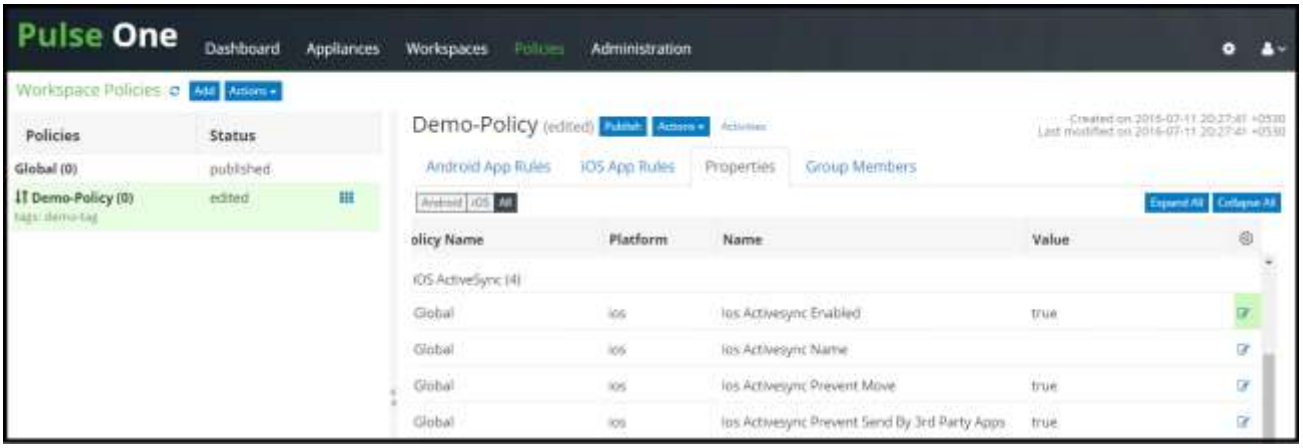
Figure: Modify Active Sync Properties



Note: The option 'Use Pulse One for authentication' enables Pulse One to push token to the registered mobiles which is used in authenticating the user for Email Access.

6. Modify the iOS ActiveSync properties. Set ios Activesync Enabled to **Yes**.

Figure: Modify iOS Active Sync Properties



Note: iOS Active Settings are applicable only to iOS devices.

7. Select the **iOS App / Android App** tab under the policy created.
    a. Click **Add App** to add a new application.
    b. Enter the application name in the search list (Salesforce1, Zendesk, Box etc.), select the

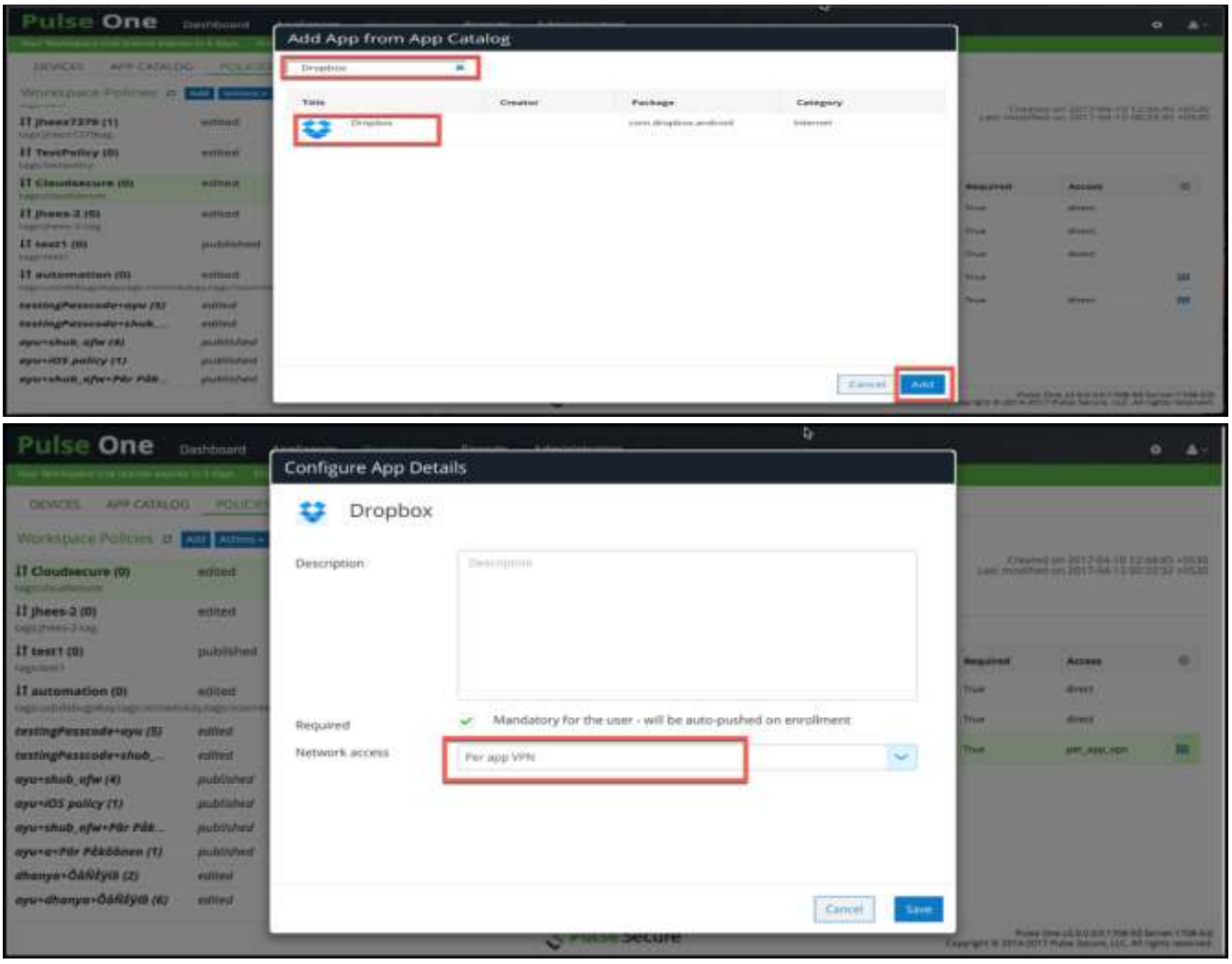
application and click **Add.**

c. Select the application added and click Edit app rule. Select '**Per app VPN'/'Require VPN'** for Network Access.

d. Click **Save**.

Note: Add applications to "App Catalog" before associating it to Workspace Policies. Refer PWS Administration guide for adding Applications to App Catalog.

Figure: Add Application



8. Navigate to the **Workspaces >Devices** tab. Click **Actions > Add User** to create a new user if user does not exist. Provide the following details:

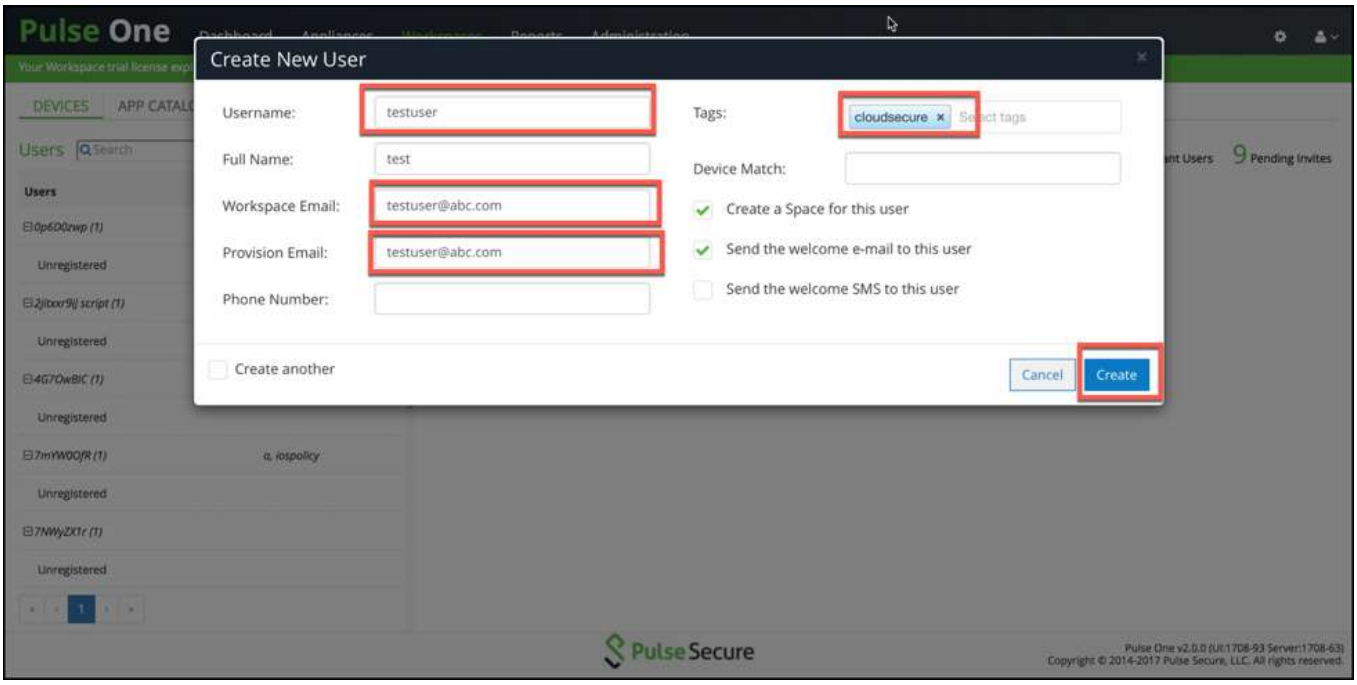
a. Enter **Username**.

b. Enter **Workspace Email**. Provision Email will get populated automatically.

c. Enter Policy name created in Use existing as Tags if required (else, Global policy will be assigned by default). See pwsstep2.

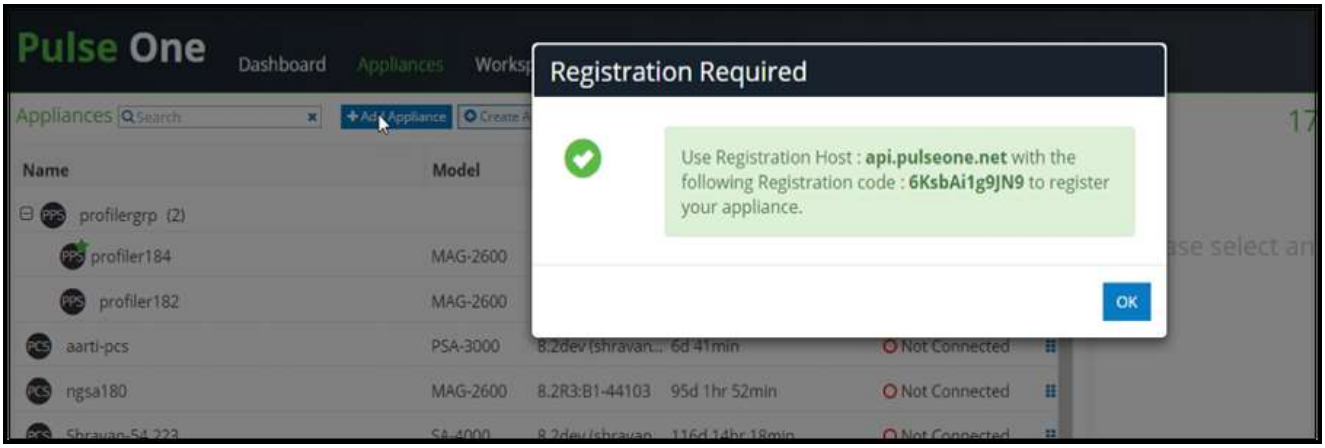
d. Click **Create.**

Figure: Create New User



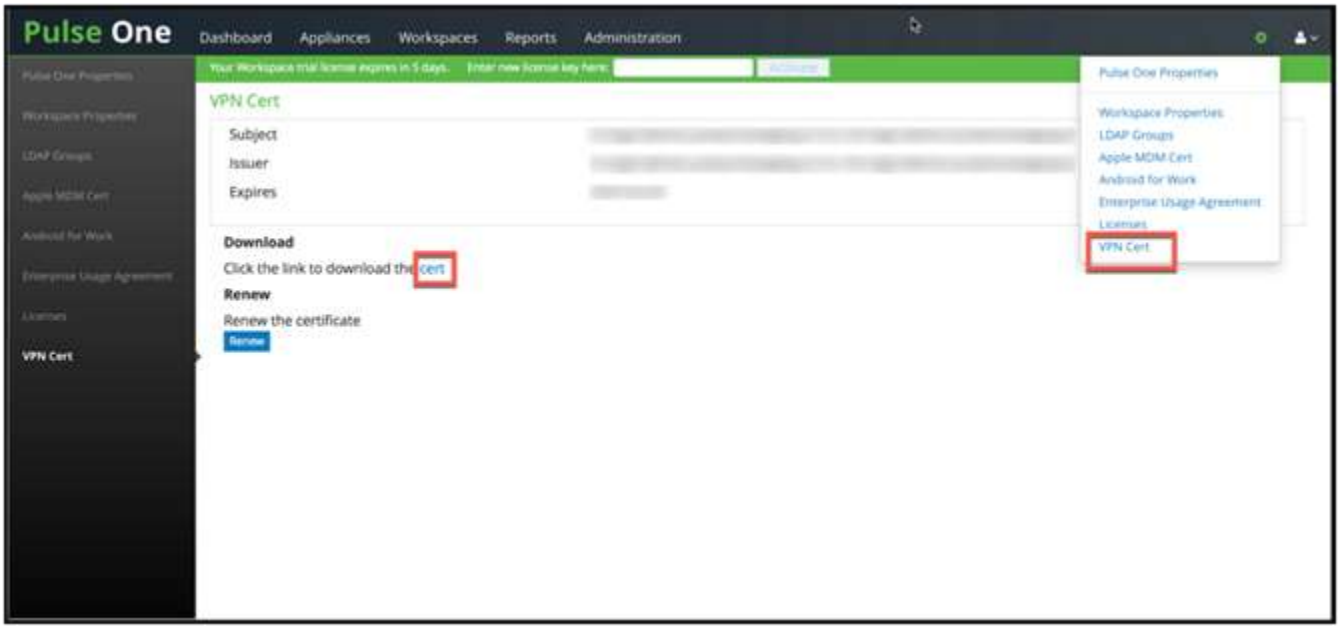
9. Select the **Appliances** tab. Click **Add Appliance** and provide a name to register Pulse Connect Secure /Pulse Policy Secure with Pulse One. Admin will be provided with Registration Host and Registration code details to be configured in PCS/PPS.

Figure: Register Appliance



10. Click the Settings gear on the top right corner of the page.
11. Click **VPN Cert** and then click the **cert** link to download Pulse One VPN certificate, which needs to be uploaded in PCS / PPS as Trusted Clients CA.

Figure: VPN Cert



Configuring Pulse Workspace for Mobile Compliance Policies

Pulse Workspace enables mobile compliance policy management for employees who bring their own devices (BYOD). To enable policy based access to mobile devices. The administrator can configure compliance policies for mobile devices based on the various device attributes, such as:

- Jail Break Detection-When compliance is set to Allow, "isCompliant" value sent from client is True. When compliance is set to Restrict VPN, "isCompliant" value sent from client is False. When compliance is set to Wipe, "isCompliant" value sent from client is False.
- Minimum OS version-Sets minimum OS version.
- Rooted Detection- Determines the action the client should take when it determines a device is Rooted. The options are allow, notify, lock or wipe.
- Non-Compliant OS Version Action-If user provisions the device that has Pulse Client version lower than that is set in Minimum Pulse Client Version policy, the device becomes non-compliant device. Actions for a non-compliant device can be one of the following:
  - Allow: User is allowed VPN access, and the device remains in the non-compliant state
  - Restrict VPN: User is restricted from VPN access
  - Wipe: Profile is wiped off from the user's device
- Minimum Pulse Client Version- Sets minimum Pulse Client version.

For more information on how to configure the compliance properties on PWS, see PWS Configuration Guide.

Configuring Pulse Workspace for Location Awareness

The location awareness feature enables the PWS managed iOS devices to suppress the VPN connections based on the user location. This enables On-Premise users to get access to cloud applications without establishing a VPN connection.

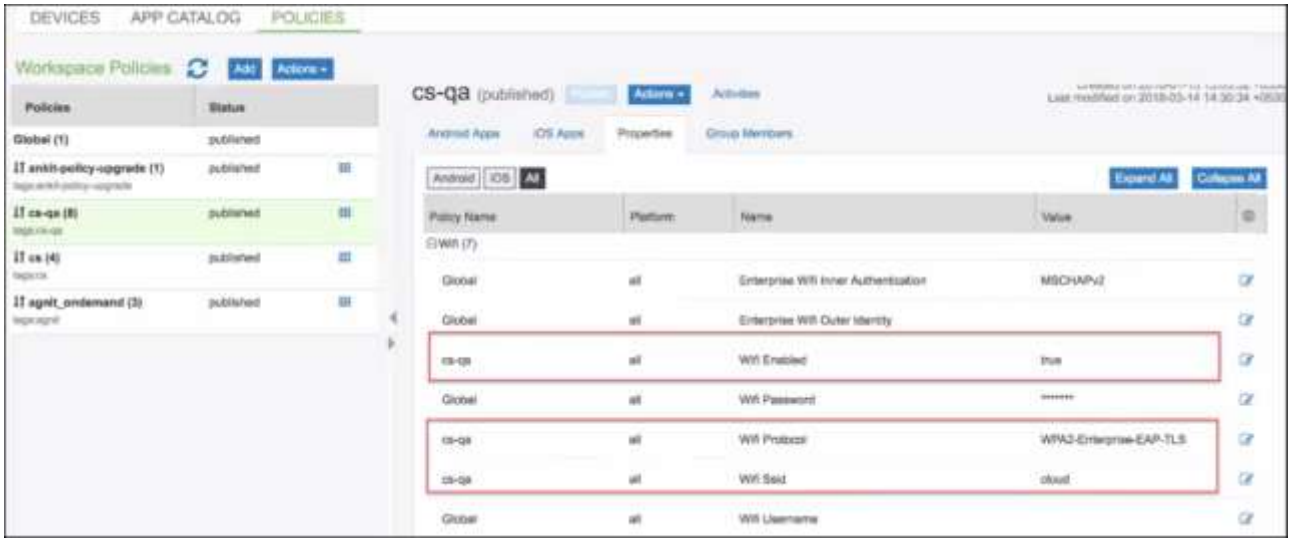
For location awareness, Pulse Workspace should be configured with:

- Wi-Fi profile and add PPS appliance for On-Premise solution. For configuration, see Configuring Pulse Workspace.
- Configure PCS for reusing the existing session through IF-MAP. For configuration, see Step 4 in Configuring Pulse Connect Secure as IF-MAP Client.

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

1. Log into the Pulse One admin console.
2. Modify the 'Wifi' Properties of the new policy or Global policy. Navigate to **Properties** tab. Scroll down to 'Wifi' section, click the **Edit** icon against each field below and provide following details:
    a. Set **Wifi Enabled** to true.
    b. Select **WPA2-Enterprise-EAP-TLS** as Wifi Protocol.
    c. Provide Wifi Ssid.

Figure: Modify Wifi Properties



3. Modify the VPN properties of new policy or Global policy to support Location Awareness. Navigate to the **Properties** Tab. Scroll down to 'VPN' section, click the **Edit** icon and Set **Enable Location Awareness** to true. For Android, under VPN configure the following.
   a. On Demand VPN Timeout (minutes): 5 (optional)
   b. Stealth Mode: true (mandatory)
   c. Vpn Connection Type: OnDemand (mandatory)

Figure: VPN Properties for iOS

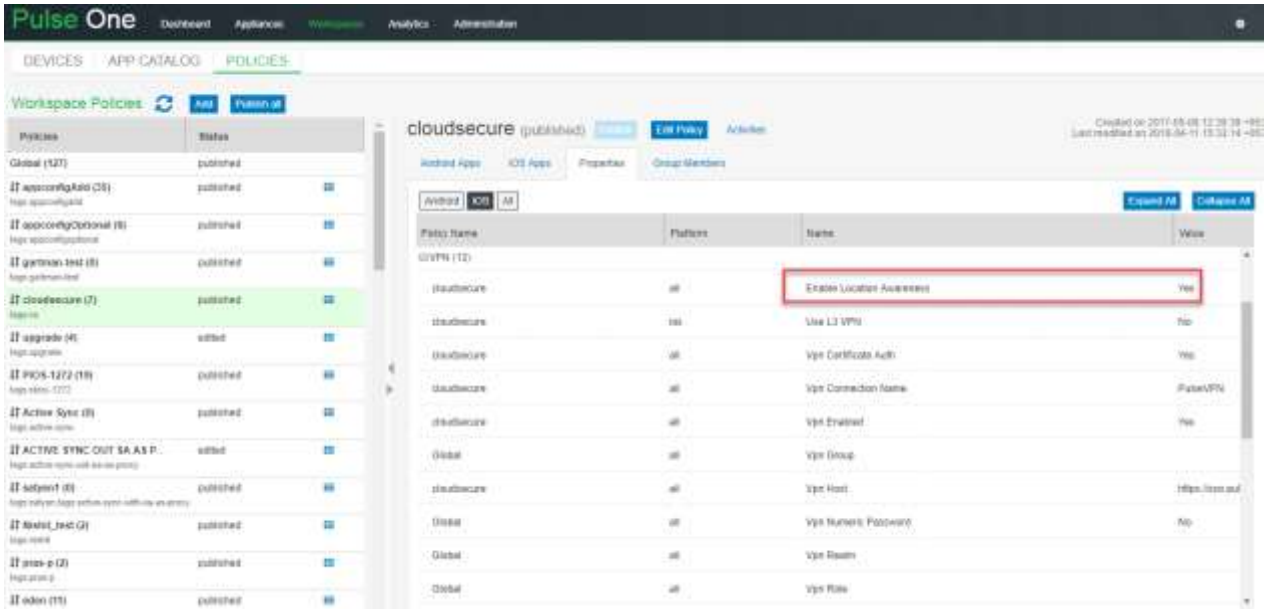
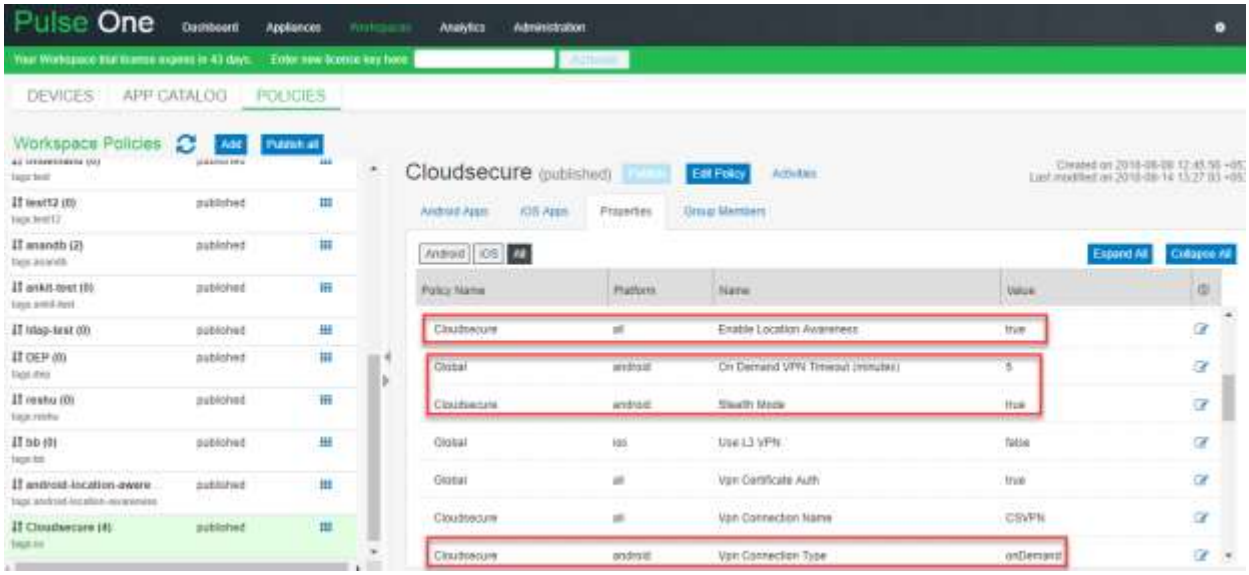


Figure: VPN Properties for Android



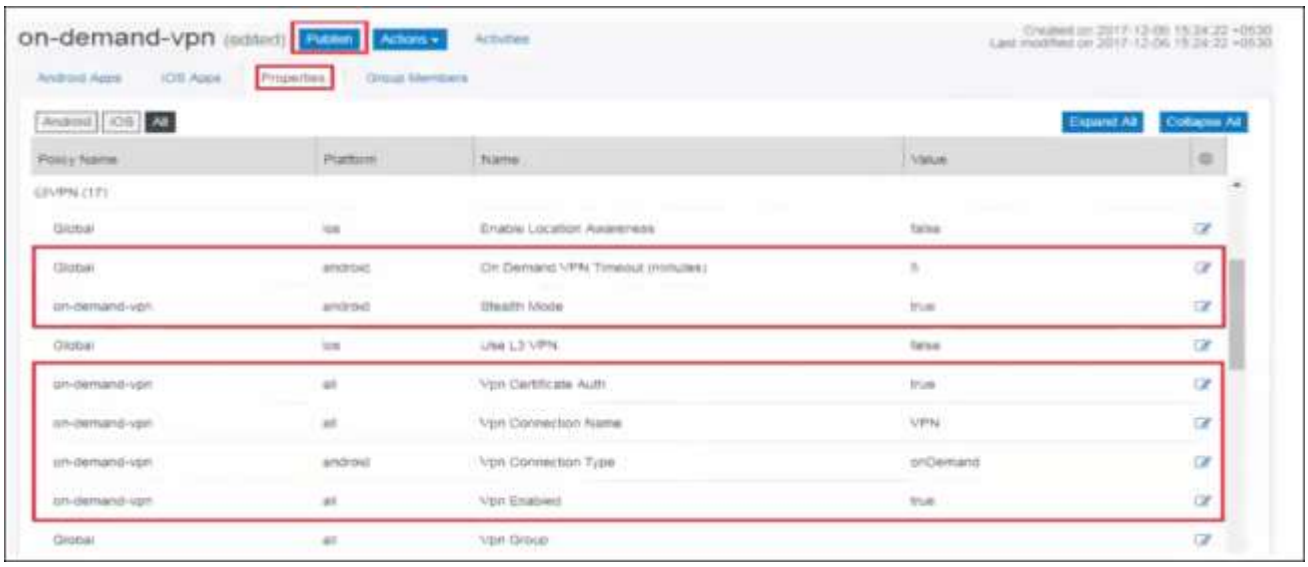
Configuring On-Demand VPN for Android devices

The On-Demand VPN feature enables the VPN connection to be triggered dynamically on accessing applications managed by Pulse Workspace (PWS). Cloud Secure re-uses the VPN session information for providing SSO access to applications.

To enable On-Demand VPN for PWS managed applications, perform the following configuration on PCS:

1. Log into Pulse One Admin console.
2. Navigate to **Policies > <policy_name>** for which you would like to add On-Demand configuration and click the **Properties** tab.
3. Under VPN, configure the following:
    a. On Demand VPN Timeout (minutes): 5 (optional)
    b. Stealth Mode: true (mandatory)
    c. Vpn Certificate Auth: true (mandatory)
    d. Vpn Connection Name: **VPN** (mandatory)
    e. Vpn Connection Type: OnDemand (mandatory)
    f. Vpn Enabled: true (mandatory)
4. Click **Publish**.

Figure: On-Demand VPN



For more information, see PWS Configuration Guide.

Redesigned End-User Pages

Cloud Secure enables end-users to access Cloud Applications seamlessly and securely. While accessing the cloud applications, different end-user pages are shown for performing various actions such as user login, Host Checker, SAML Authorization and so on.

The end-user pages are redesigned to improve the user experience. This includes users who access the cloud services using the web browser and applications across various platforms such as Windows, Mac, Android and iOS.

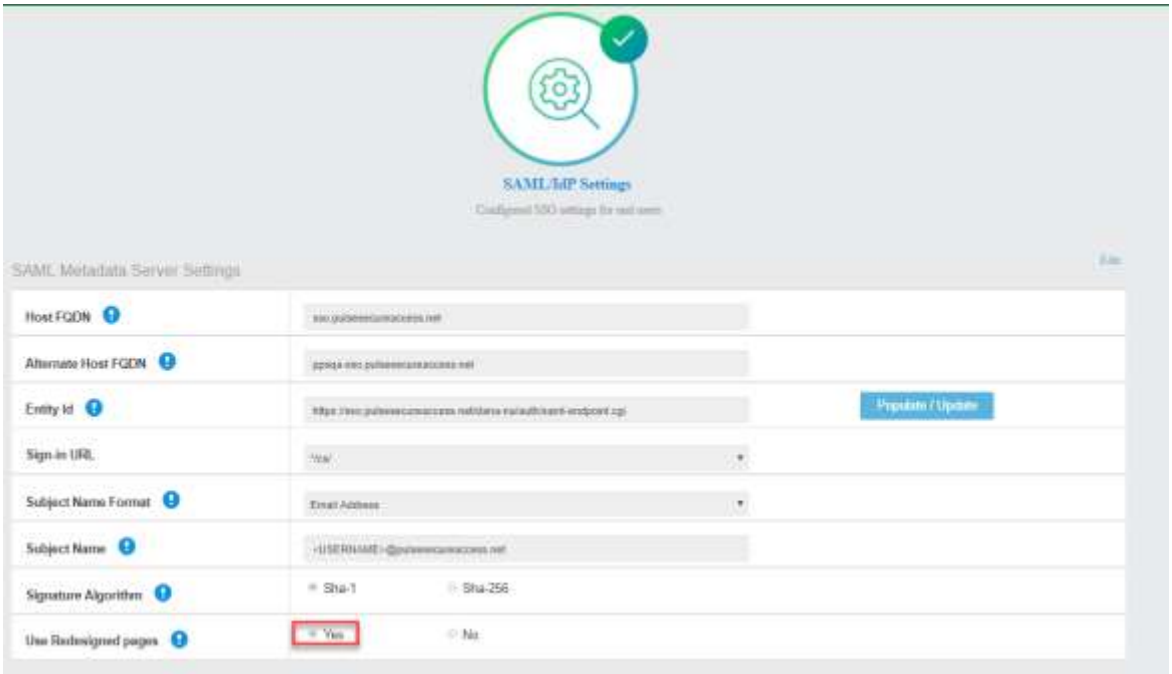
The new redesigned user pages can be enabled from both the existing PCS sign-in policy page and the new Cloud Secure UX home page.

Cloud Secure UX page

To enable the usage of redesigned pages for Cloud Secure from new Cloud Secure UX configuration page:

1. Navigate to **System > Cloud Secure > Cloud Secure Configuration** and select the SAML/IdP Settings section from the UX Home Screen.
2. Under SAML Metadata Server Settings, Click **Yes** to Use Redesigned Pages.

Figure: Cloud Secure Configuration- New UX

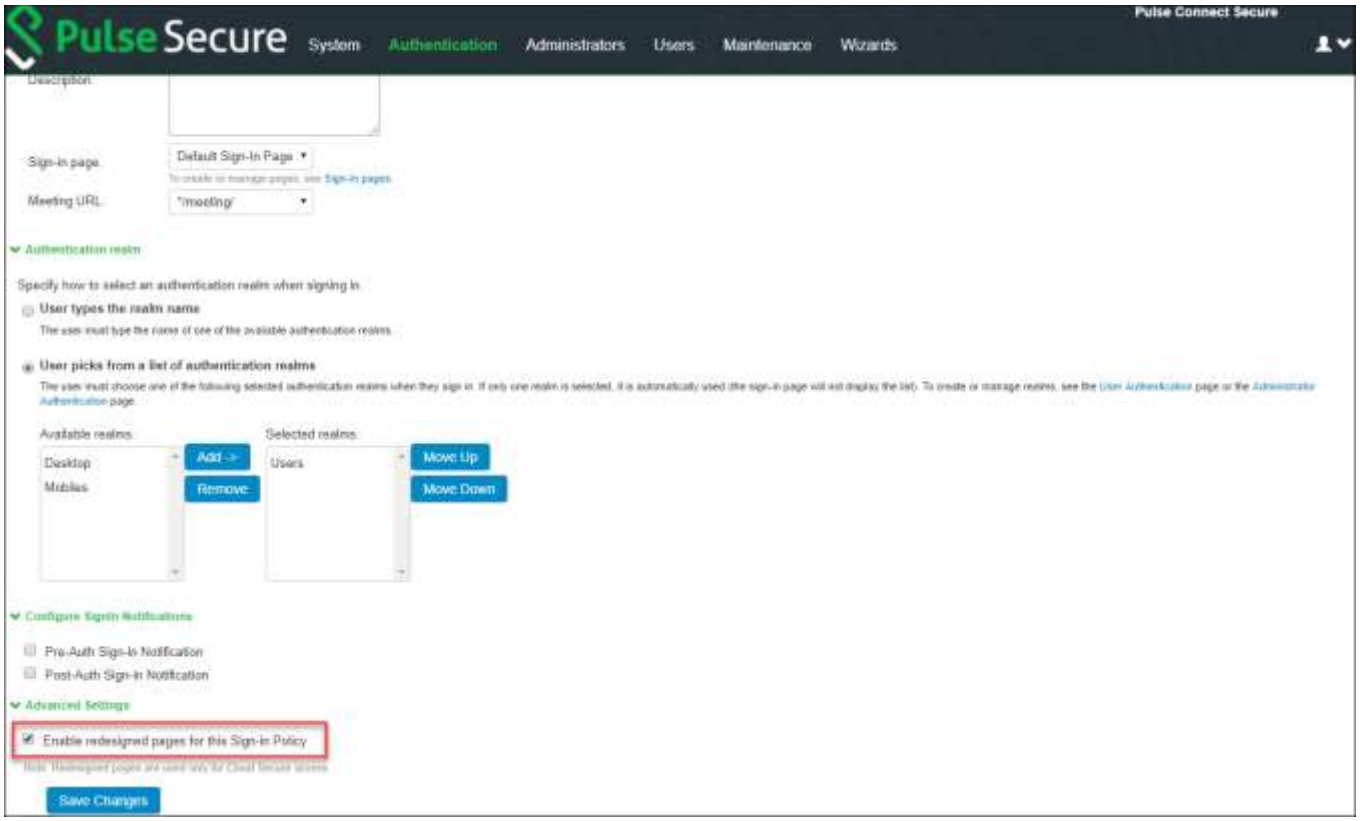


Existing PCS Sign-In Policy Page

To enable the usage of new redesigned user pages using the existing sign-in policy page:

1. Select **Authentication > Signing In > Sign-In Policies** and click New URL to create a new sign-in policy.
2. Under Advanced Settings, click the checkbox for **Enable redesigned pages for this sign-in policy**.

Figure: Pre Sign-In Notification



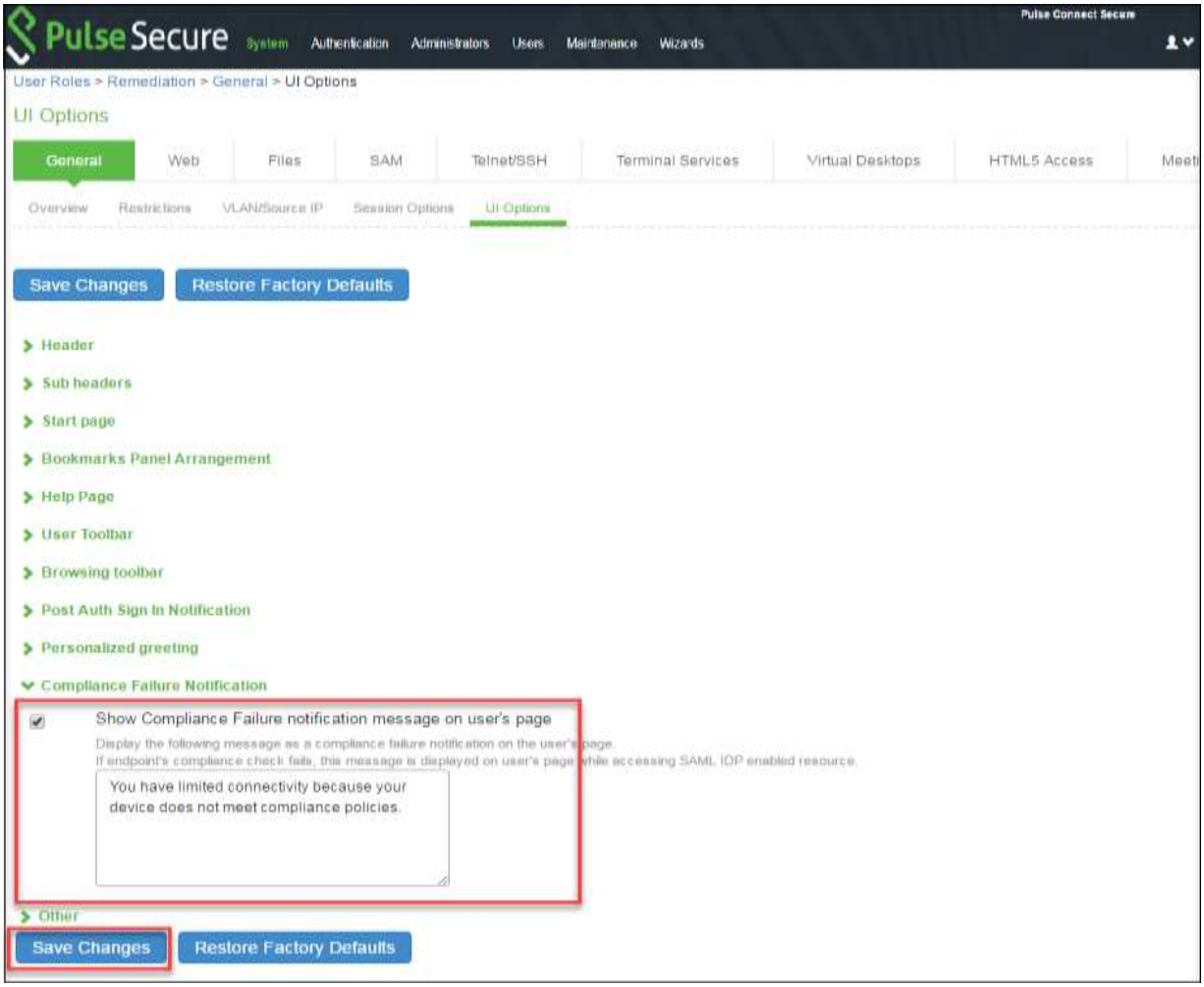
Compliance Failure Notification

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 compliance failure notification, perform the following configuration on PCS:

1. Navigate to **Users > User Roles**. Create a new Remediation role and enable all the options.
2. Navigate to the **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: Compliance Failure Notification



4. Navigate to Users > User Realms > <REALM> > Role Mapping.
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.

ECP Throttling

ECP throttling provides a mechanism to identify and stop all duplicate ECP requests being sent to AD server for authentication thus preventing the user from AD account lock out.

For example, User changes AD password and if there are devices using ECP to access mail or other service from Service Provider (O365), which is not updated with the new password, then the ECP request is sent with old password.

The AD authentication fails and the IDP (PCS) gets flooded with ECP requests containing old password. The AD server locks the user account when it exceeds the number of configured wrong password attempts since all the requests are sent to AD.

As a result of AD account lock out, all other services will also get affected. To avoid this the admin can enable ECP throttling in IDP(PCS), which prevents users from sending their duplicate password credentials to AD thus avoiding the user from getting locked out.

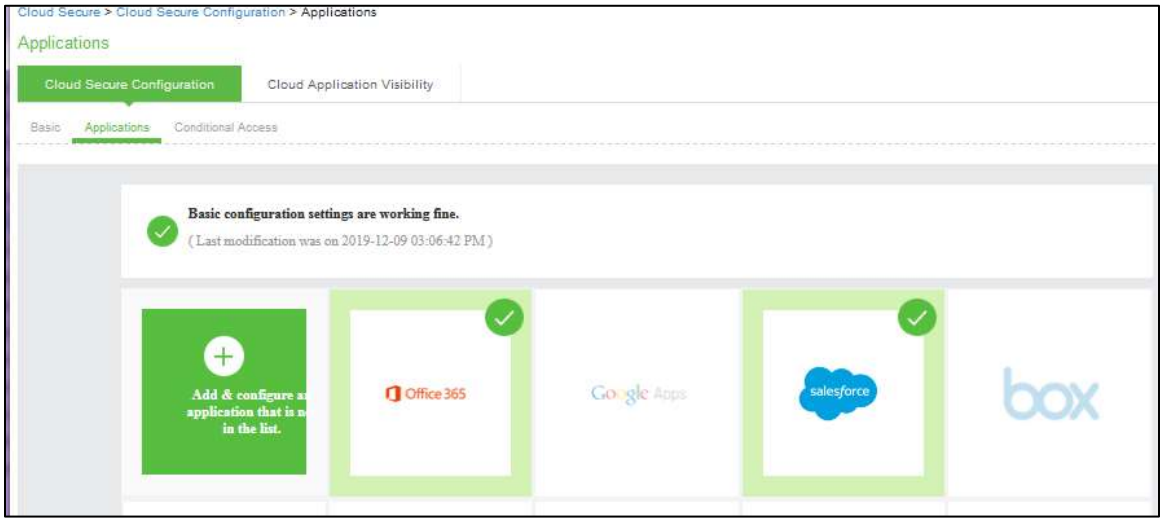
IDP(PCS) will also maintain a table of such blocked ECP requests. In case of any brute force attack, the AD account will still be locked and thereby IDP(PCS) ensures capturing of such brute force attacks and blocking the user.

Enabling ECP Throttling

To enable ECP throttling:

1. Select **System > Cloud secure > Cloud Secure Configuration > Applications.**
2. Click Office 365.

Figure: ECP Throttling



3. Under Enhanced Client or Proxy Profile (ECP) Settings, Enable Detect duplicate ECP requests.
4. Enter the threshold limit for the user. This specifies the maximum number of duplicate ECP requests that can be blocked for a user.

   For example, if a user has n devices both sending the same old password (for example, pass1), then this is considered as one duplicate ECP request.

   Similarly, if there are n devices and if one of the device is continuously sending wrong password (for example, pass2) and the other devices are sending an another wrong password (pass1), then this is considered as 2 duplicate ECP requests.

5. Enter the blocking time in minutes. On repeating multiple failed login attempts the user will be blocked for the specified amount of time.

Viewing Blocked ECP users

This report shows all the blocked ECP requests, which can be used to determine if the attack is due to a brute force attack or due to duplicate password requests.

It also gives information on the device through which the request is received so that the user can be notified to change the password in that device.

The Admin also has an option to unblock the user from the blocked ECP requests page. This option is very useful, if the password entered in the device is new but the AD failed to sync the new password because of any time synchronization issue.

Select **Reports > Blocked Users Report** to view the blocked ECP users.

Figure: Blocked ECP Users

The below table describes the columns in the Cloud Secure blocked ECP users report.

Column	Description
User Name	Specifies the name of the user accessing the cloud application.
Blocked Since	Specifies the day, month, date, time and year since the user is blocked.
Most Recent Request Time	Specifies the most recent request time.
Request Count	Specifies the number of requests.
Blocked till	Specifies the time till the user is blocked.
Recent ECP Request from	Specifies the device details from which the request originated.
Realm	Displays the user realm for the blocked user.

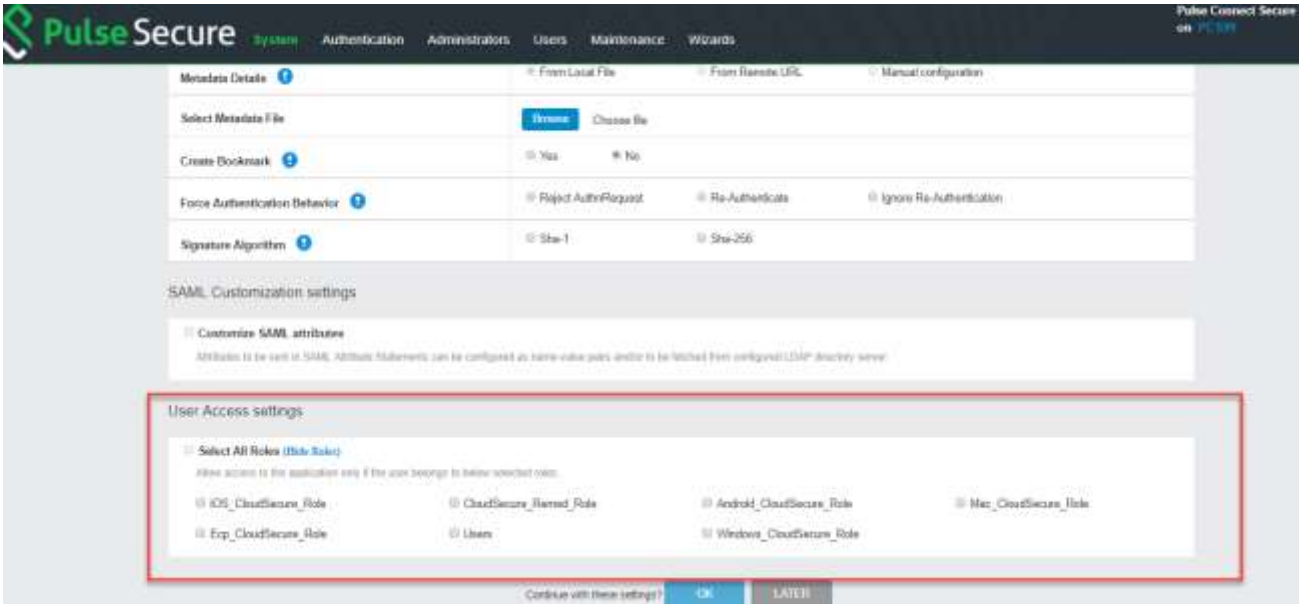
Role Based Access Control

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 **Cloud Secure Configuration > Applications > Application Configuration**.
2. Access the Service Provider configured, for example, Salesforce, and configure the Roles under User Access Settings.
    a. **Select 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: Configure desired roles to restrict access to the cloud service only if any of the user roles configured are assigned.

Figure: Role Based Access Control



Conditional Access

Conditional Access for Cloud Secure provides a mechanism to enforce access control policies based on user, device type, device compliance and location parameters by defining policies for applications. The Conditional Access policy control is evaluated on top of the existing Role based Access Control on applications. If the Role based Access Control denies access to an application, then irrespective of conditional access control policies the application access would be denied by PCS.

A Conditional Access policy has following three components:

- **Condition** for Conditional Access policy based on:
  - User group - based on LDAP/AD group membership
  - Device compliance - based on host checker policies or MDM parameters
  - Device type
  - Location
- **Applications**: A conditional access policy can be applied on one or more Cloud Secure applications.
- **Actions**: A conditional access policy results in one of the following configurable actions:
  - Allow
  - Deny
  - Multi Factor Authentication (MFA)

Conditional Access policies are evaluated during application access time while roles are mapped to the session during the session creation time.

Note: In case you have a Fresh Installation of PCS/PPS, then it will NOT have UEBA package by default with it. Please add the UEBA package at Behavioral Analysis page before using Geolocation Based Conditional Access. In case of Upgrade of PCS/PPS from R7 or earlier to R8 or later, then UEBA package is carried forwarded as is and you can still update it to latest version by uploading new package. You may download latest UEBA package from Pulse Secure Support Site. (my.pulsesecure.net).

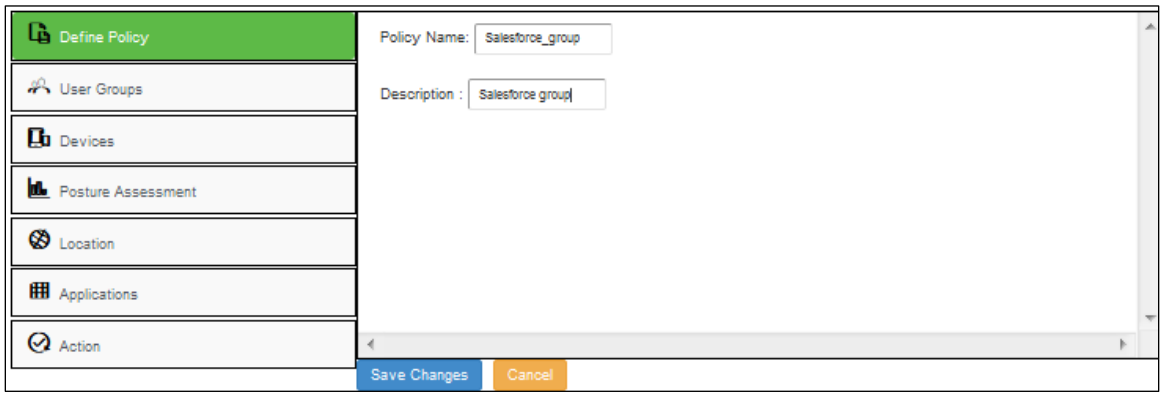
Note: Conditional Access policies are not evaluated for federated sessions.

Conditional Access Policy

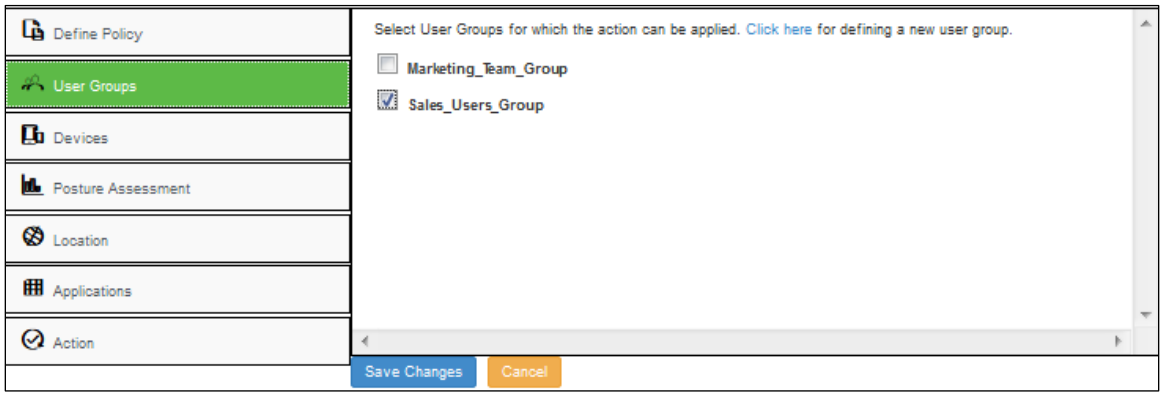
Before defining Conditional Access policy, ensure that Cloud Secure is configured with all applications and basic configurations.

To define a Conditional Access policy, do the following:

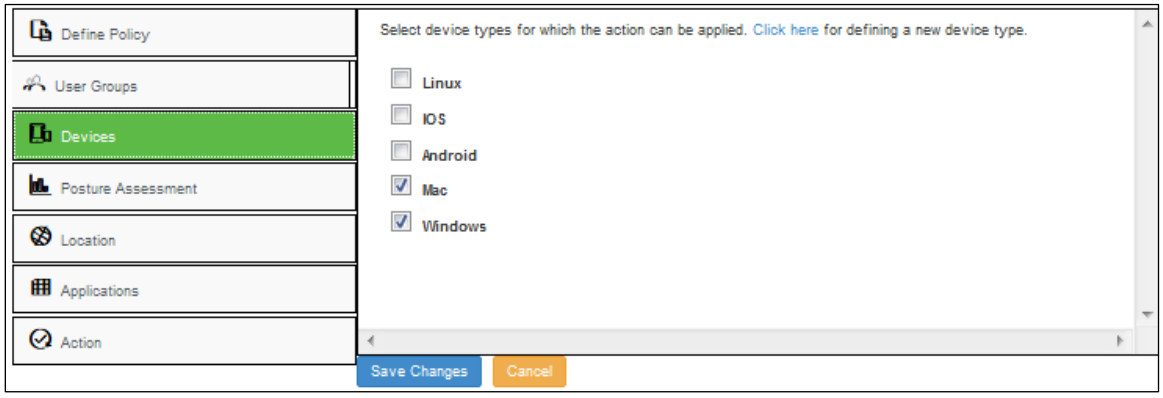
1. In the PCS admin console, select **System > Cloud Secure > Cloud Secure Configuration > Conditional Access**.
2. Select the **Policies** tab. A list of policies is displayed if already defined.
3. Click **Add New** to define a new policy.
4. Define policy by entering **Policy Name** and **Description**.



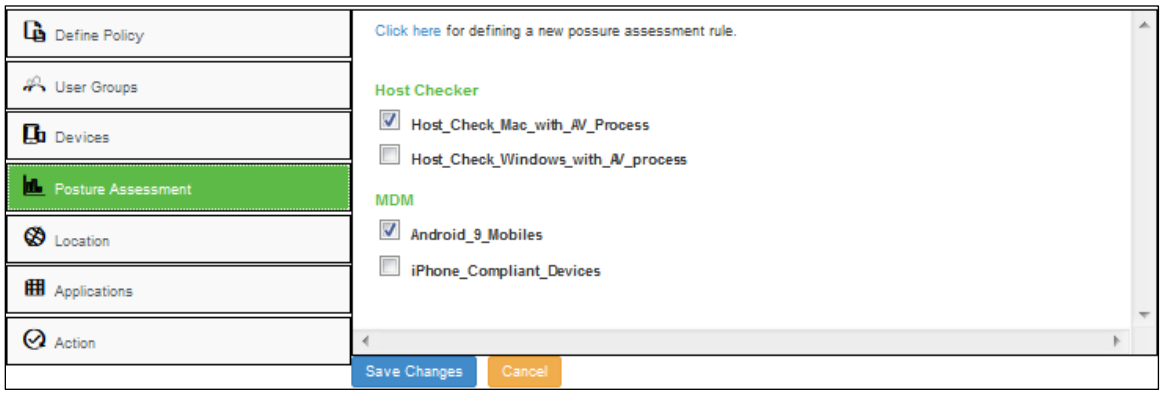
5. Select **User Groups** and choose the user groups to which the action needs to be applied. To add a user group, click the **Click here** link and follow the instructions.



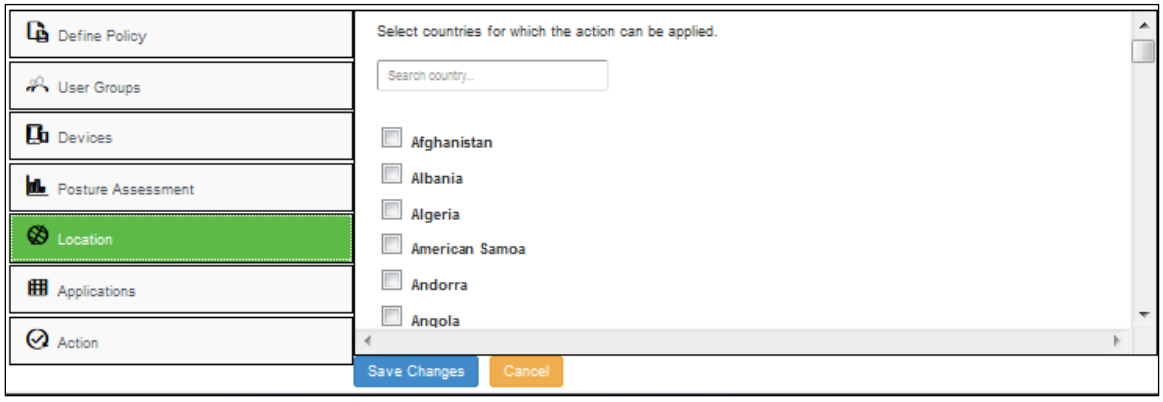
6. Select **Devices** and choose the device types to which the action needs to be applied. To add a device type, click the **Click here** link and follow the instructions.



7. Select **Posture Assessment** and choose the Host Checker policy for desktop and MDM policy for mobile devices to which the action needs to be applied.



8. Select **Location** and choose the countries to which the action needs to be applied.

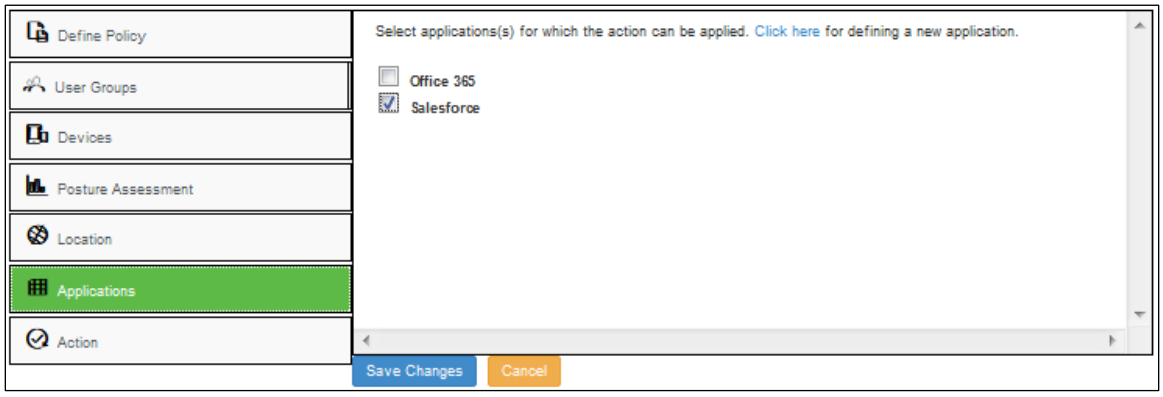


The list of countries supported:

Afghanistan	Cameroon	French Polynesia	Kazakhstan
Aland Islands	Canada	French Southern	Kenya
Albania	Cape Verde	Territories	Kiribati
Algeria	Cayman Islands	Gabon	Korea
American Samoa	Central African Republic	Gambia	Kuwait
Andorra	Chad	Georgia	Kyrgyzstan
Angola	Chile	Germany	Lao People's Democratic
Anguilla	China	Ghana	Republic
Antarctica	Christmas Island	Gibraltar	Latvia
Antigua and Barbuda	Cocos (Keeling) Islands	Greece	Lebanon
Argentina	Colombia	Greenland	Lesotho
Armenia	Comoros	Grenada	Liberia
Aruba	Congo	Guadeloupe	Libyan Arab Jamahiriya
Asia/Pacific Region	Cook Islands	Guam	Liechtenstein
Australia	Costa Rica	Guatemala	Lithuania
Austria	Cote d'Ivoire	Guernsey	Luxembourg
Azerbaijan	Croatia	Guinea	Macao
Bahamas	Cuba	Guinea-Bissau	Macedonia
Bahrain	Curacao	Guyana	Madagascar
Bangladesh	Cyprus	Haiti	Malawi
Barbados	Czech Republic	Heard Island and	Malaysia
Belarus	Denmark	McDonald Islands	Maldives
Belgium	Djibouti	Holy See (Vatican City	Mali
Belize	Dominica	State)	Malta
Benin	Dominican Republic	Honduras	Marshall Islands
Bermuda	Ecuador	Hong Kong	Martinique
Bhutan	Egypt	Hungary	Mauritania

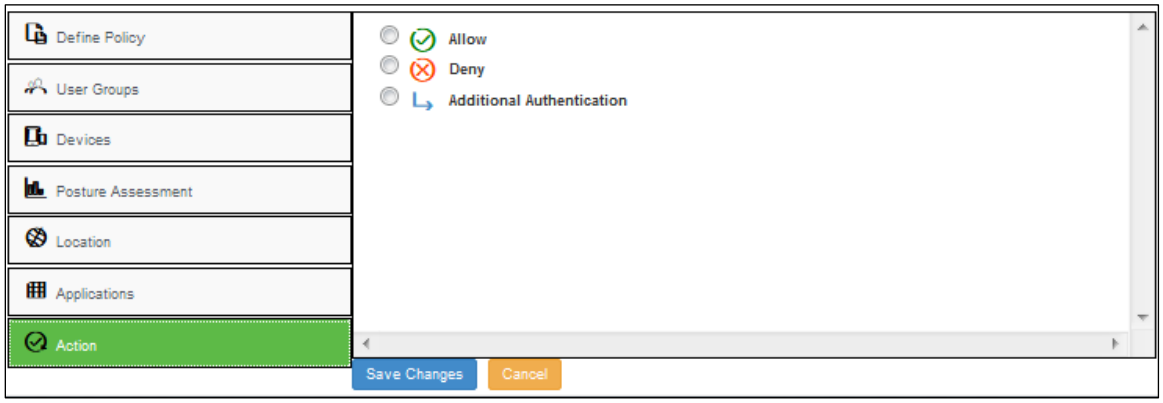
Bolivia Bonaire Bosnia and Herzegovina Botswana Bouvet Island Brazil British Indian Ocean Territory Brunei Darussalam Bulgaria Burkina Faso Burundi Cambodia	El Salvador Equatorial Guinea Eritrea Estonia Ethiopia Europe Falkland Islands (Malvinas) Faroe Islands Fiji Finland France French Guiana	Iceland India Indonesia Iran Iraq Ireland Isle of Man Israel Italy Jamaica Japan Jersey Jordan	Mauritius Mayotte Mexico Micronesia Moldova Monaco Mongolia Montenegro Montserrat Morocco Mozambique Myanmar Namibia
Nauru Nepal Netherlands New Caledonia New Zealand Nicaragua Niger Nigeria Niue Norfolk Island Northern Mariana Islands Norway Oman Pakistan Palau Palestinian Territory Panama Papua New Guinea Paraguay Peru Philippines Pitcairn Poland Portugal Puerto Rico	Qatar Reunion Romania Russian Federation Rwanda Saint Barthelemey Saint Helena Saint Kitts and Nevis Saint Lucia Saint Martin Saint Pierre and Miquelon Saint Vincent and the Grenadines Samoa San Marino Sao Tome and Principe Saudi Arabia Senegal Serbia Seychelles Sierra Leone Singapore Sint Maarten Slovakia	Slovenia Solomon Islands Somalia South Africa South Georgia and the South Sandwich Islands South Sudan Spain Sri Lanka Sudan Suriname Svalbard and Jan Mayen Swaziland Sweden Switzerland Syrian Arab Republic Taiwan Tajikistan Tanzania Thailand Timor-Leste Togo Tokelau Tonga Trinidad and Tobago	Tunisia Turkey Turkmenistan Turks and Caicos Islands Tuvalu Uganda Ukraine United Arab Emirates United Kingdom United States United States Minor Outlying Islands Uruguay Uzbekistan Vanuatu Venezuela Vietnam Virgin Islands Wallis and Futuna Western Sahara Yemen Zambia Zimbabwe

9. Select **Applications** and choose the applications to which the action needs to be applied. To add a new application, click the **Click here** link and follow the instructions.



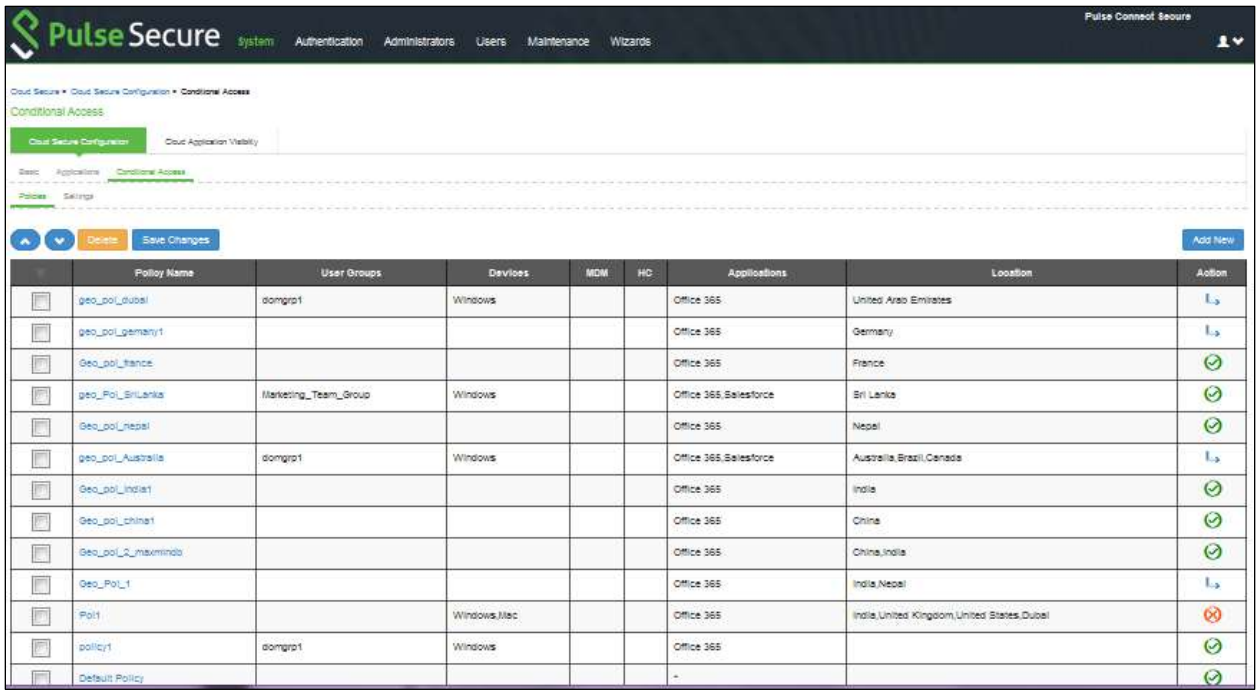
10. Select **Action** and choose one of the following actions for the policy:

- **Allow ( )** – This action ensures that the application access is granted.
- **Deny** ( ) – This action denies application access to the end user. An error page "Authorization Failed" is presented to the user.
- **MFA** ( ) – This action ensures that the application access is granted only after two levels of authentication.



11. Click **Save Changes**. The new policy is listed in the Conditional Access Policies page. This list of conditional access policies maintains an order.

- Use the Up/Down arrow heads ( ) if you want to reorder the policies and click **Save Changes**.
- Click the Policy Name link if you want to edit the policy.
- Select the check box associated with the policy and click **Delete** to remove a policy.

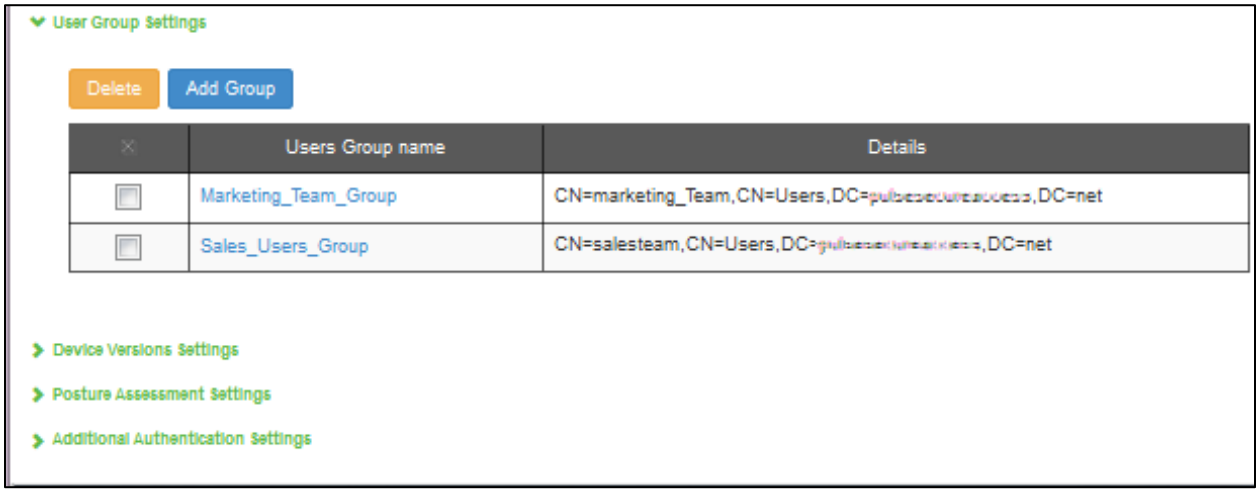


Conditional Access Settings

The Conditional Access Settings page provides you with additional settings to configure the conditions in detail.

Configuring User Group

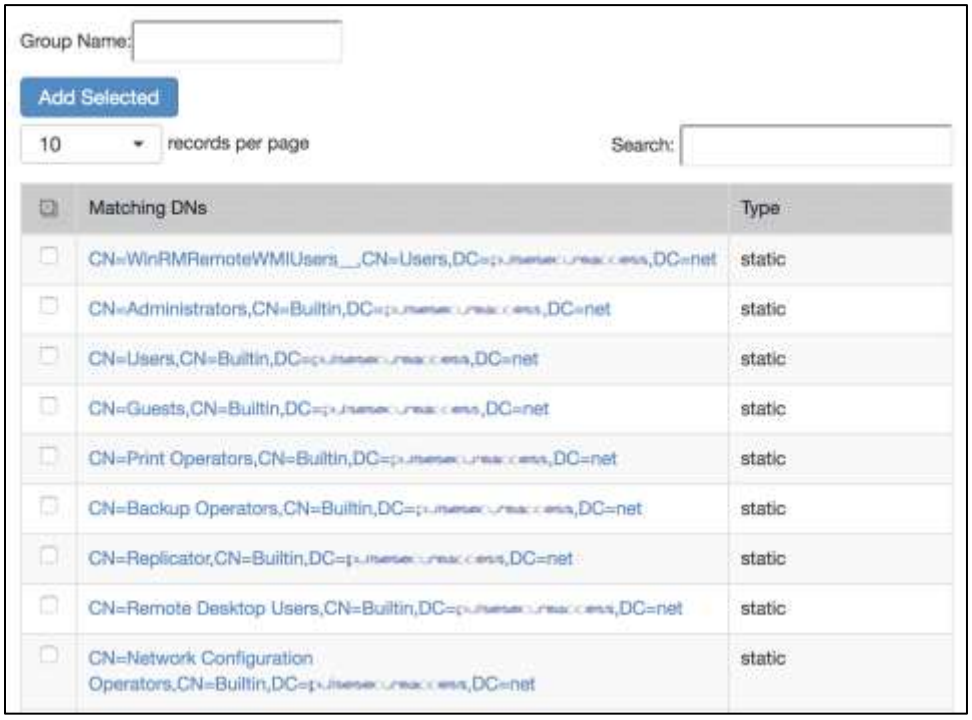
Under the User Group Settings section, you can group multiple LDAP/AD groups to mark them as a logical group.



The logical user group configuration has a workflow to fetch the groups from the LDAP/AD authentication server configured for Cloud Secure and select multiple groups into a logical group.

To add a User Group, do the following

1. In the User Group Settings section, click **Add Group**.
2. In the window displayed, type a name for the group, select one or more LDAP or AD groups from the list and click **Add Selected**.



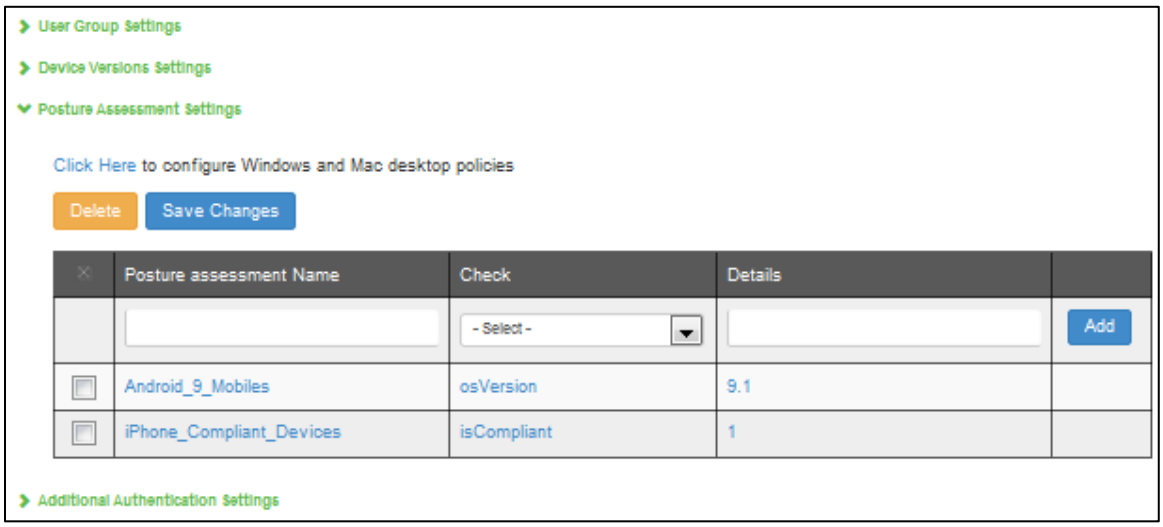
Note: Groups are fetched and listed from the configured Auth Server under Authentication Server of Basic Settings for Cloud Secure.

Configuring Device Versions Settings

Under the Device Versions Settings, define a device by entering a regular expression pattern against the user agent string.

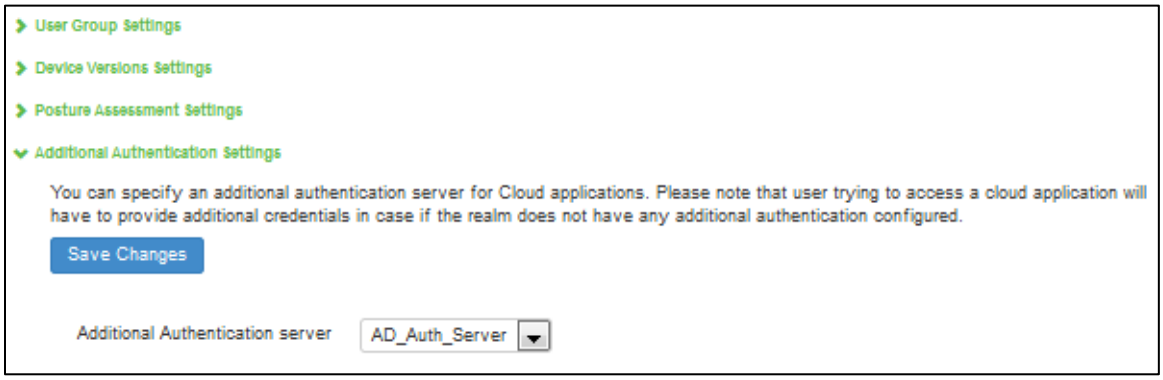
Configuring Posture Assessment Settings

Under Posture Assessment Settings section, define an MDM policy based on MDM attributes.



Configuring Additional Authentication Server

Under Additional Authentication settings section, specify Additional Authentication server from the drop-down list for cloud applications. This authentication server is used for MFA across all Conditional Access policies.



Note: In this release,

- the following servers are not supported as MFA authentication servers.
  - TOTP server
  - Certificate server
  - SAML server
- MFA is applicable only to SP-initiated workflow. For Bookmark-initiated workflow, MFA is not applicable and is equivalent to Deny access.

Clustering

Cloud Secure SSO solution is supported with Active/Active and Active/Passive Cluster Deployments. It requires load balancing of VPN connections and SAML requests across all the Cluster nodes. For generic Clustering Configurations, refer to PCS Administration Guide.

The deployment scenarios and configurations specific to Cloud Secure are described below:

- Cloud Secure Active/Active Cluster Deployment
- Cloud Secure Active/Passive Cluster Deployment
- DNS Server Configuration

Cloud Secure Active/Active Cluster Deployment

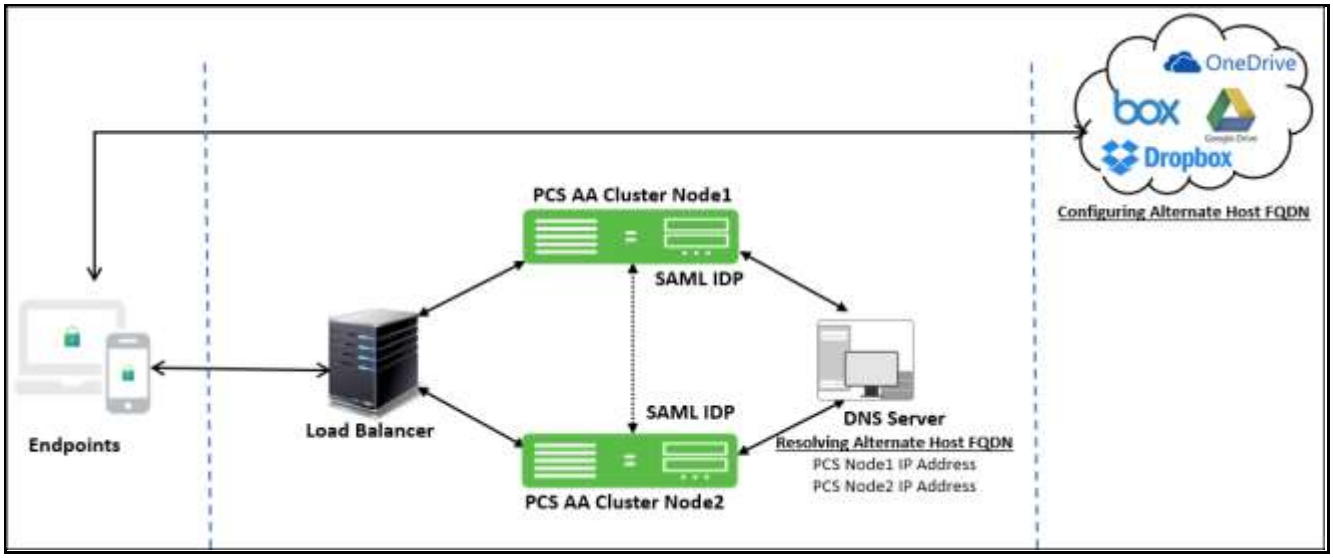
For Active/Active Cluster support, external Load balancer does load balancing of VPN connection requests to all the external interfaces of cluster nodes. The configurations on Internal DNS server is required for load balancing the SAML AuthN requests for L3 VPN. However, for L4 vpn the host entry configurations on respective PCS nodes are required for handling the SAML AuthN requests.

In an Active/Active PCS cluster the user sessions are synchronized across cluster nodes. Hence if a VPN connection is established with one cluster node, the session details are available on all the Active/Active cluster nodes. If a user has a VPN connection with one PCS node and SAML AuthN request is on another PCS node, the SSO to SAML SP is provided by using cluster synchronized session.

Note:

- SSO is not supported on Configuration-Only Cluster since the user sessions are not synchronized across cluster nodes.
- If one of the PCS cluster nodes (whose IP address is returned first in DNS response) fails, browser tries with second IP address. If it is reachable, SAML AuthN request is handed to second cluster node. This way in failover scenario, SSO is provided by other PCS node in Active/Active cluster.
- For Active/Active cluster, "Alternate Host FQDN" entry should be resolved to internal IP address of all cluster nodes by the internal DNS server for L3 VPN. In case of L4 VPN, host entries should be added for the respective PCS nodes to resolve the Alternate host FQDN to internal interface IP. Navigate to system >network >hosts for adding the host entries.
- For re-use VPN functionality to work in Active/Active cluster deployment, the internal IP addresses of all the cluster nodes should be added as split tunnel resources.

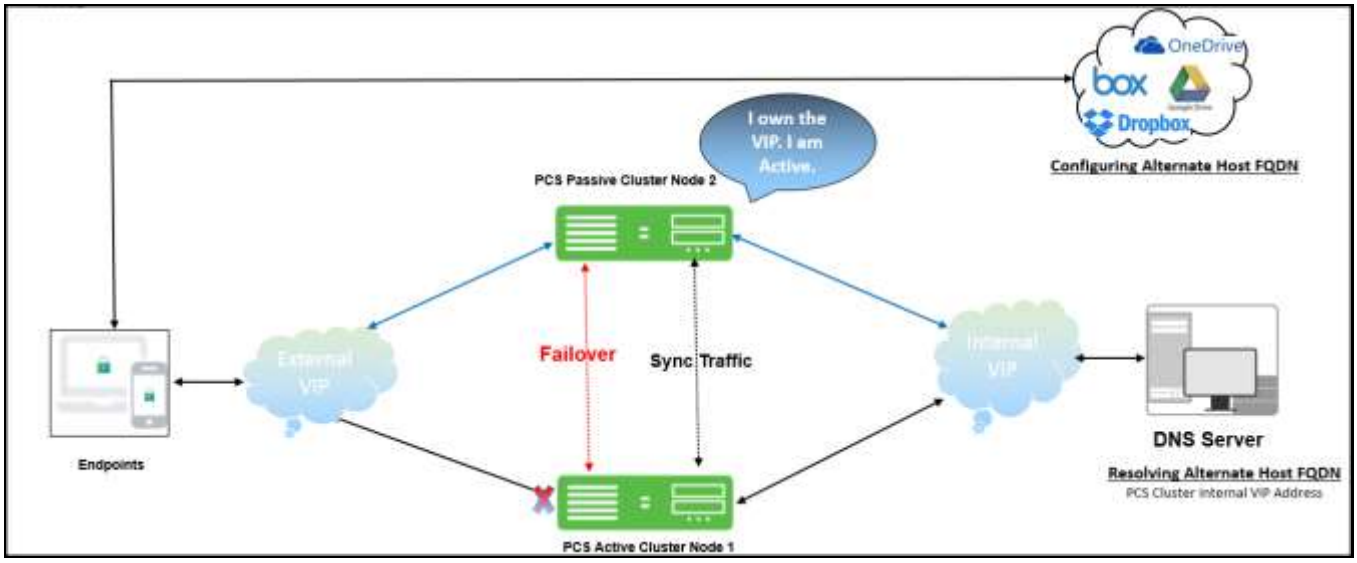
Figure: Cloud Secure Active Active Cluster



Cloud Secure Active/Passive Cluster Deployment

PCS uses a virtual IP (VIP) address to address the cluster pair. If the active node fails, the passive node takes over the VIP address and provides SSO access.

Figure: Cloud Secure Active/Passive Cluster



Note:

For re-use VPN functionality to work in Active/Passive cluster deployment, the internal VIP address should be added as split tunnel resource.

DNS Server Configuration

Admin should add the host entries on the Internal and External DNS server as described in the table below.

Table 1 DNS Server Configuration

	Cluster FQDN for SAML	Alternate Cluster FQDN for SAML
Active/Active Cluster		
External DNS	Load Balancer IP Address	Load Balancer IP Address
Internal DNS	NA	Internal IP Address of all nodes
Active/Passive Cluster		
External DNS	VIP External Address	VIP External Address
Internal DNS	NA	VIP Internal Address

Note:

For One Arm Deployment, Virtual Port IP address of all nodes should be added in the DNS server.

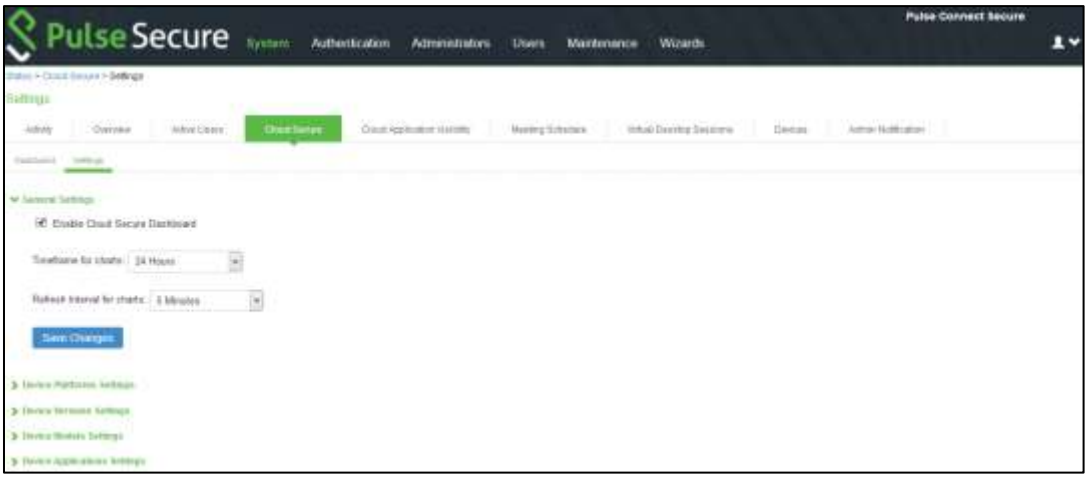
Dashboard

The Cloud Secure Dashboard captures the cloud secure applications that are getting accessed by users and the device platform from where these applications are getting accessed. It provides a consolidated view of the different applications being accessed 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. Select **System > Status > 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. Click **Save Changes**.

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

Figure 1 Dashboard Settings



Navigate to **System > Status > 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 and represents them in the 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.
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.
- Admin can click on the search icon at the top of the chart ( ) to view the Cloud Secure report. The drill down report for the corresponding chart is displayed.
- 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 chart by clicking on the chart in the dashboard.

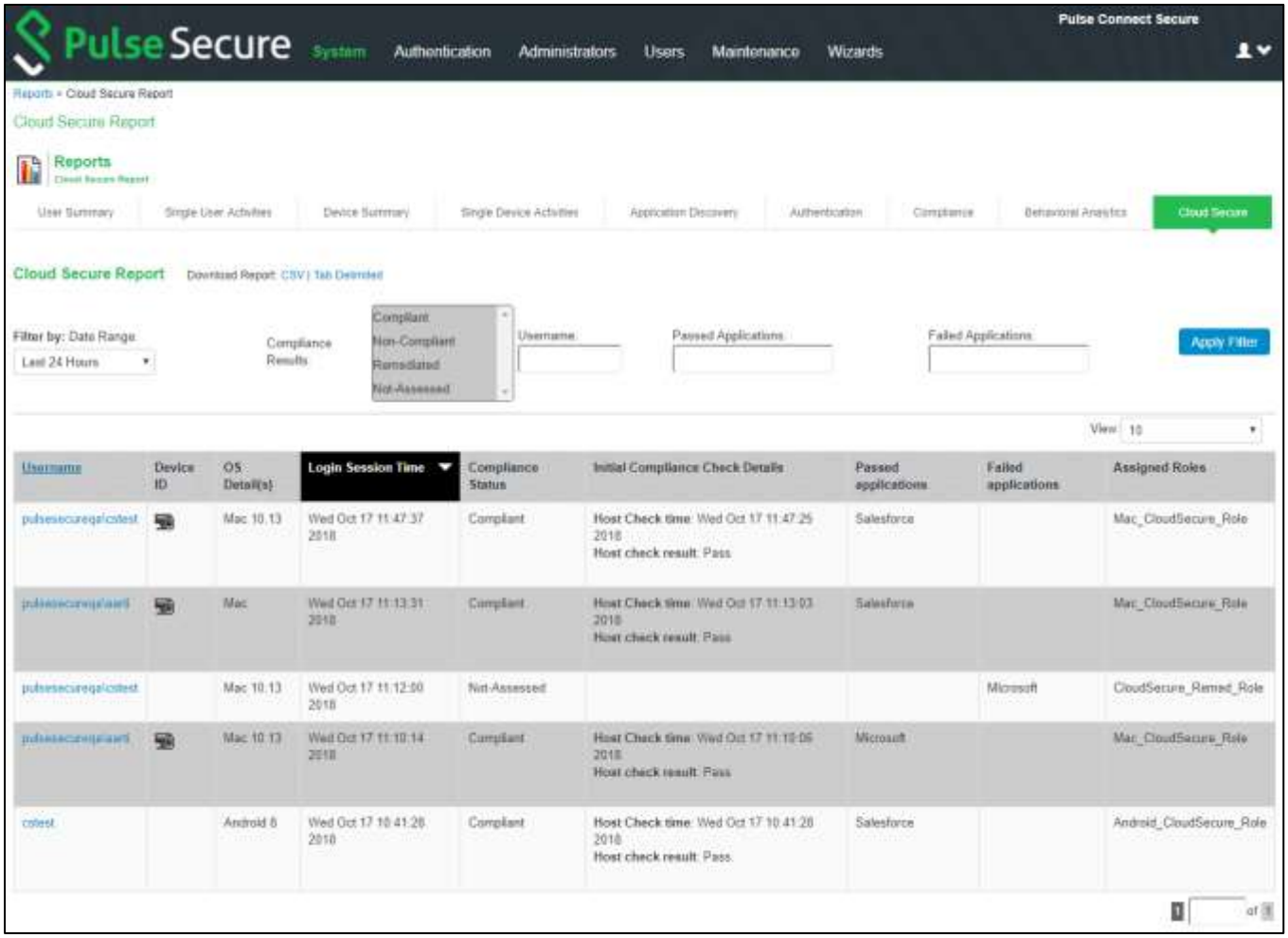
Figure: Dashboard

Reports

Cloud Secure Summary report provides information about the user's cloud application usage. It provides details such as user name, device ID, OS details, compliance status, login session time, compliance check details, passed and failed applications, and the assigned user roles.

To display the Cloud Secure Summary report:

1. Select System > Reports > Cloud Secure Summary.
2. Select one of the following periods from the Date Range list box:
   - Last 24 Hours– (Default) Refers to the last 24 hours from the current hour.
   - Last 7 Days– Refers to current day and the previous last 6 days.
   - Last 30 Days– Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
   - Compliance Results
   - Username
   - Passed Applications
   - Failed Applications
4. Click Apply Filter.



The below table describes the columns in the Cloud Secure summary report.

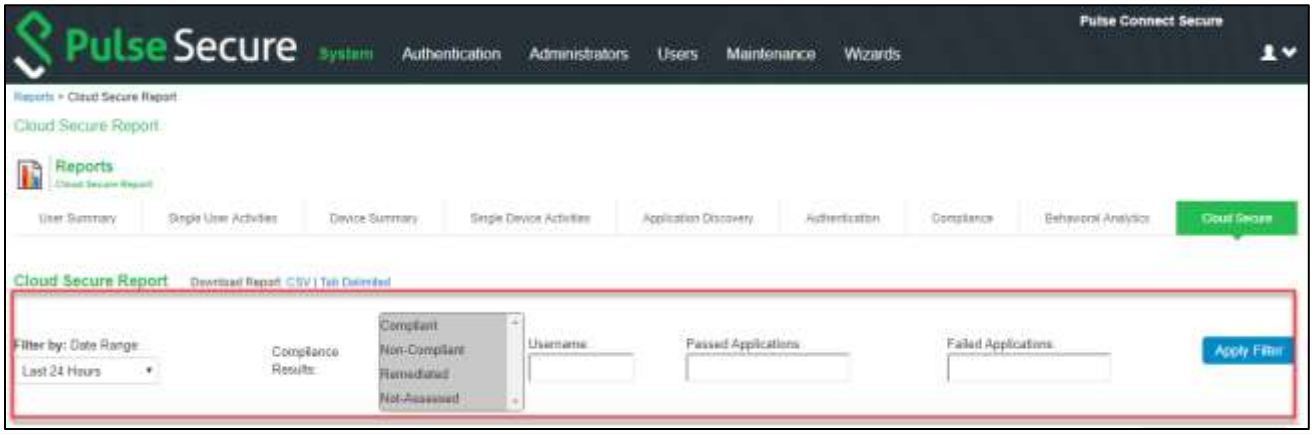
Column	Description
User Name	Specifies the name of the user accessing the cloud application.
Device ID	Specifies a unique identifier to identify the endpoint. Click the device ID icon to view a single device report.
OS Details	Specifies the Operating System of the device.
Login Session Time	Specifies the login time of the session.
Compliance Status	Specifies the Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated.
Initial Compliance Check Details	Specifies the compliance details when the session was first established.
Passed Applications	Provides the name of the applications, which passed.
Failed Applications	Provides the name of the applications, which failed.
Assigned Roles	Specifies the user role assigned.

Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Cloud Secure Summary**.
2. Select one of the following periods from the Filter by: Date Range list box:
   - Last 24 Hours– (Default) Refers to the last 24 hours from the current hour.
   - Last 7 Days– Refers to current day and the previous last 6 days.
   - Last 30 Days– Refers to current day and the previous last 29 days.
3. Enter search criteria in one or more of the following columns:
   - Compliance Status
   - Username
   - Passed Applications
   - Failed Applications
4. Click **Apply Filter**.

Figure: Data Filters



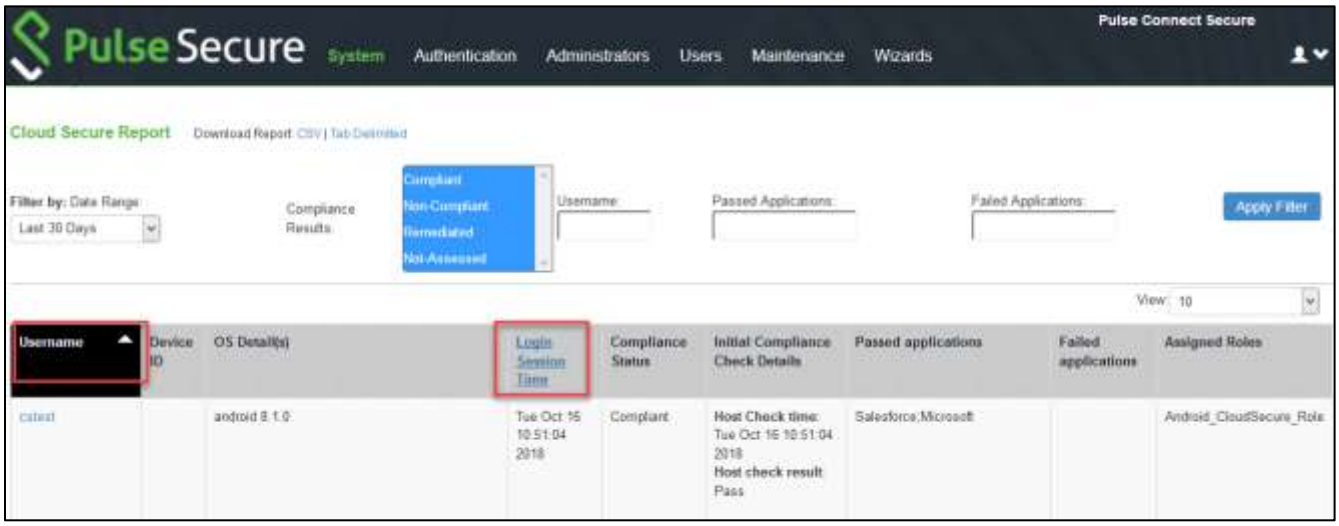
Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the Cloud Secure Summary report:

1. Select **System > Reports > Cloud Secure Summary.**
2. Select Login Session Time column and click either the ascending or descending order icon.

Figure: Sorting Records

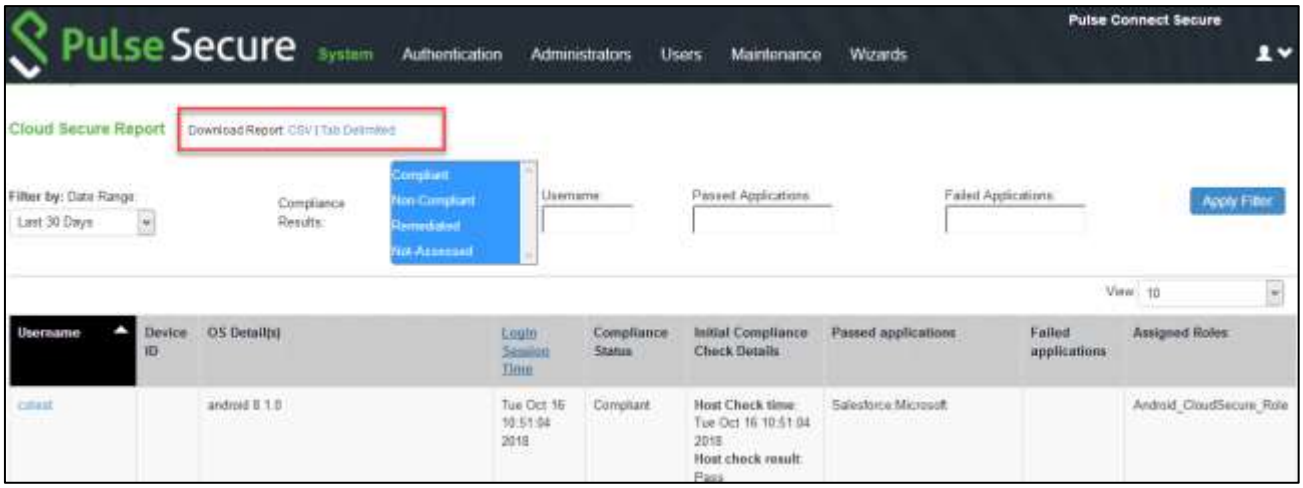


Exporting Cloud Summary Report

To export a Cloud Secure Summary report:

1. Select **System > Reports > Cloud Secure Summary**.
2. Select a Download Report option.
   - CSV– Exports the report in CSV format.
   - Tab Delimited– Exports the report in tab-delimited format.

Figure: Download Report



Cloud Application Visibility

Overview

In a cloud computing environment, loss of visibility can mean loss of control over several aspects of IT management and data security. Shadow IT is a great example of how IT can lose control when they have a blind spot in their cloud architecture. Administrators must be able to control which applications are being used, who is using them, and what data is being generated and shared within cloud environments.

Cloud Application Visibility feature enables you to secure and manage cloud applications. It also provides visibility of the cloud application used by the user and allows the Administrator's to set granular access and use policies to monitor the Cloud Application usage in real time.

Benefits

The Cloud Application Visibility page enables you to quickly investigate the cloud application usage and provides the following benefits:

- Real-time visibility to cloud applications, along with their category so that the Administrator can determine if one or more apps need to be blocked.
- Block access to certain cloud apps that may be risky or hog bandwidth so that the network operates with peak efficiency.
- View cloud applications by category, cloud applications by user, total number of cloud applications.
- Offers Application visibility and control regardless of location that is both on-premises using PPS and remote access using PCS.

Note: Cloud Application Visibility is currently supported only with Windows Pulse Client.

Configurations

- Enabling Cloud Application Visibility at Role Level
- Configuring Cloud Application Visibility Options
- Configuring Cloud Secure Application Policies
- Editing/Deleting Application

Pre-Requisite

Cloud Application Visibility is a licensed feature and you must install Cloud Secure license to enable it.

Summary of Configuration

A high-level overview of the configuration steps needed to set up Cloud Application Visibility is shown below. Click each step to directly jump to the related instructions.

Note:

- Cloud applications visited by the user are tracked and reported even when there may not be an active session to PCS/PPS. CAV does need the Pulse Client to be connected for the first time to a PCS/PPS to start sending information about the access to cloud applications and receive new policies.
- CAV looks ups the category of a URL by communicating with PPS/PCS server and then the resulting response is cached to improve performance.
- CAV is currently supported only with standalone PPS/PCS server.
- When the user connection changes from PPS to PCS for a CAV enabled role. Use "Preserve Client Side" proxy option in VPN connection profile to preserve the CAV proxy exception list.

Enabling Cloud Application Visibility at Role Level

To enable cloud application visibility for a role:

1. Select **User** > **User Roles** and Click the role name.
2. Under **Options**, select the checkbox for **Cloud Application Visibility.**

3. Click Options, to configure the Cloud Application Visibility options. See Configuring Cloud Application Visibility Options.
4. Click Application Policies, to configure the Cloud Secure Application Policies. See Configuring Cloud Secure Application Policies.
5. Click Save Changes

Figure: PPS User Roles Page

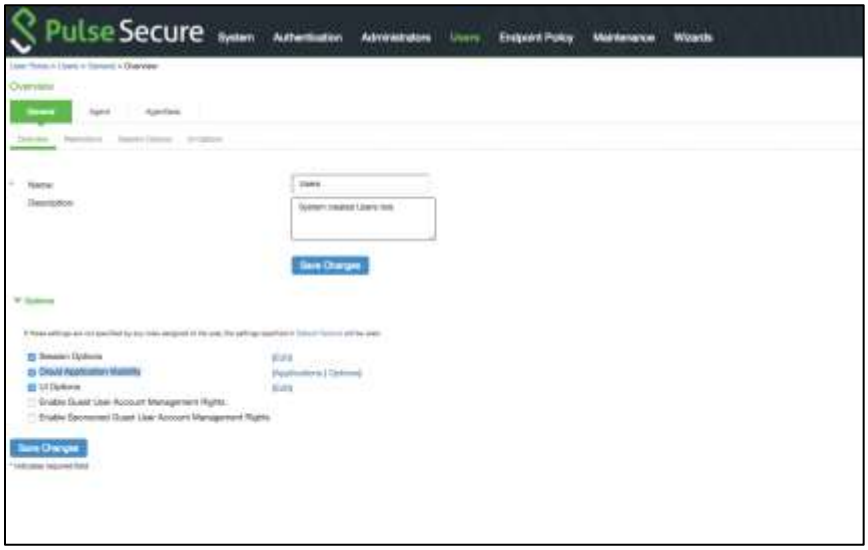
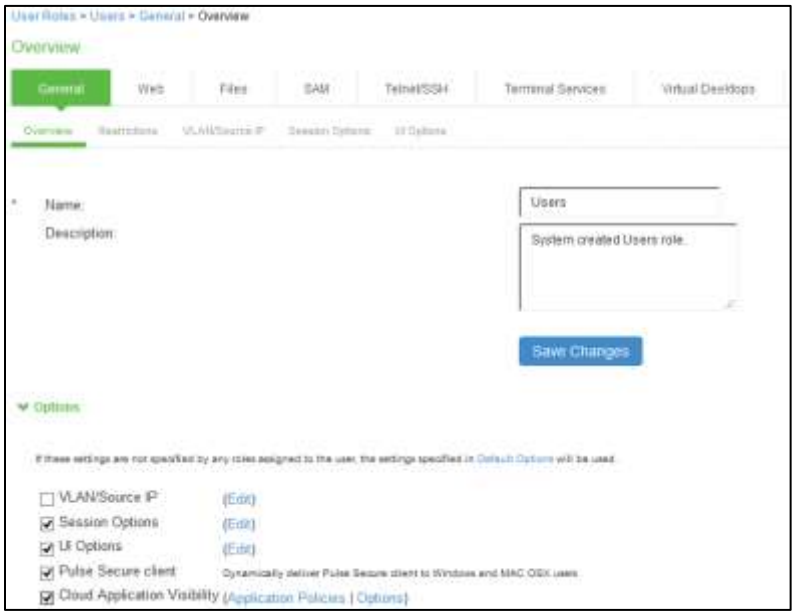


Figure: PCS User Roles Page



Configuring Cloud Application Visibility Options

Define the frequency that the Pulse Client checks with the PCS/PPS for new policies, upload the threatprint database and add the notification message to be displayed for blocked applications.

To configure application visibility options:

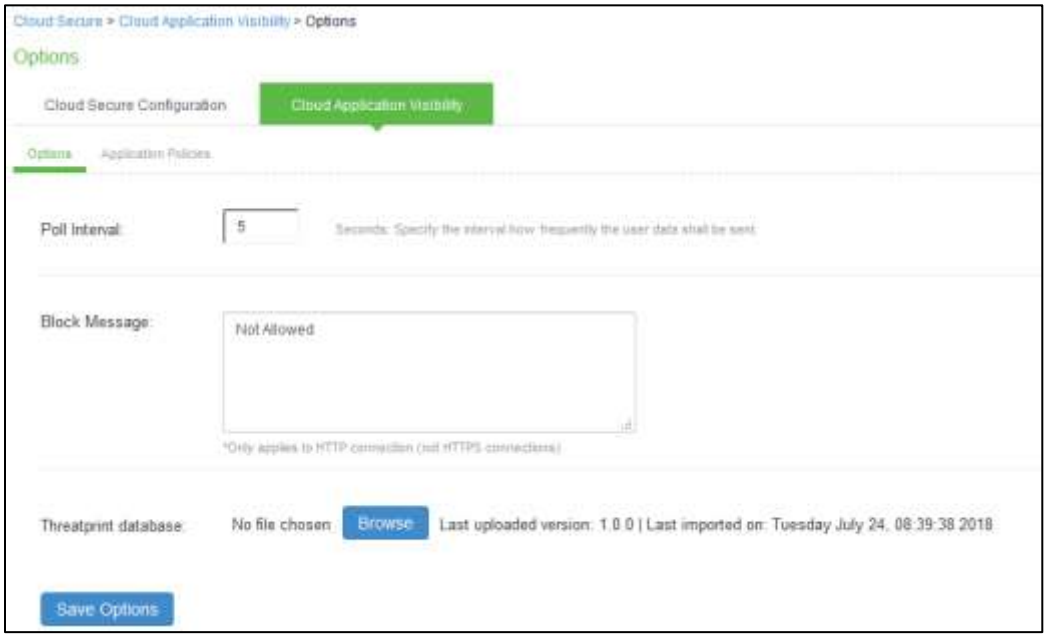
1. Select **System** > Cloud Secure > Cloud Application Visibility > Options.
2. **Under Poll Interval, enter the required time interval in minutes**.

3. Under **Threatprint database**, Click **Browse** and upload the categorization database. You can download the Threatprint database from the Pulse Secure support portal.

   Note: Pulse Client gets the categorization from the uploaded categorization DB, and it needs to be uploaded to PCS/PPS separately.

4. Under **Block Message**, enter the notification message to be displayed when the web application is blocked.

Figure: CAV Visibility Options Page



Configuring Cloud Secure Application Policies

Define the Cloud Secure application policy to control access to applications based on user role and application category.

To configure application policies:

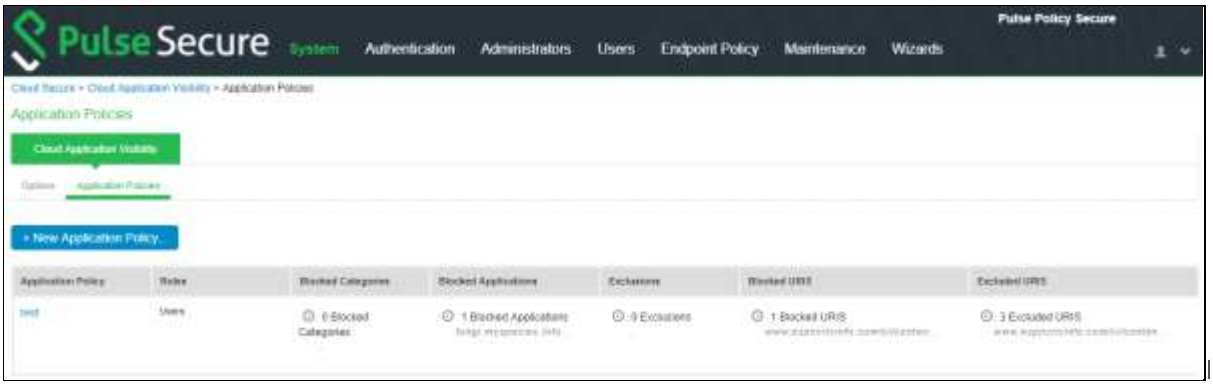
1. Select **System** > **Cloud Secure** > **Cloud Application Visibility** > **Application Policies.**
2. Click **New Application Policies** to create a new application policy, which allows/blocks cloud applications.
3. Enter the name for the application policy.
4. Under **Block Based on Categories**, select the application category needs to be blocked.

   The applications are categorized into different categories such as Social, News, Technology, Health, Business, Sports, Others, Entertainment, Weather, Finance, Education, Shopping, Adult and so on.
5. Under **Also block these cloud applications,** enter the domain name that needs to be blocked.
6. Under **Exclusions: Allow these applications even if they fall under blocked applications,** enter any of the specific applications that has to be allowed even though they are under blocked category or applications.
7. Click '+' button next to **URI Filtering** to expand URI configuration options.
8. Under **Block these URIs**, enter the URI that needs to be blocked (blacklisted). Administrator can also enter the keyword, and all the URIs containing that keyword will be blocked for the user.
9. Under **Exclusion: Allow these URIs even if they fall under blocked URIs**, enter the specific URIs

that have to be allowed even though they are under blocked URIs. Administrator can also enter the keyword, and all the URIs containing that keyword will be allowed for the user.

Note: **URI Filtering** is for http traffic only.

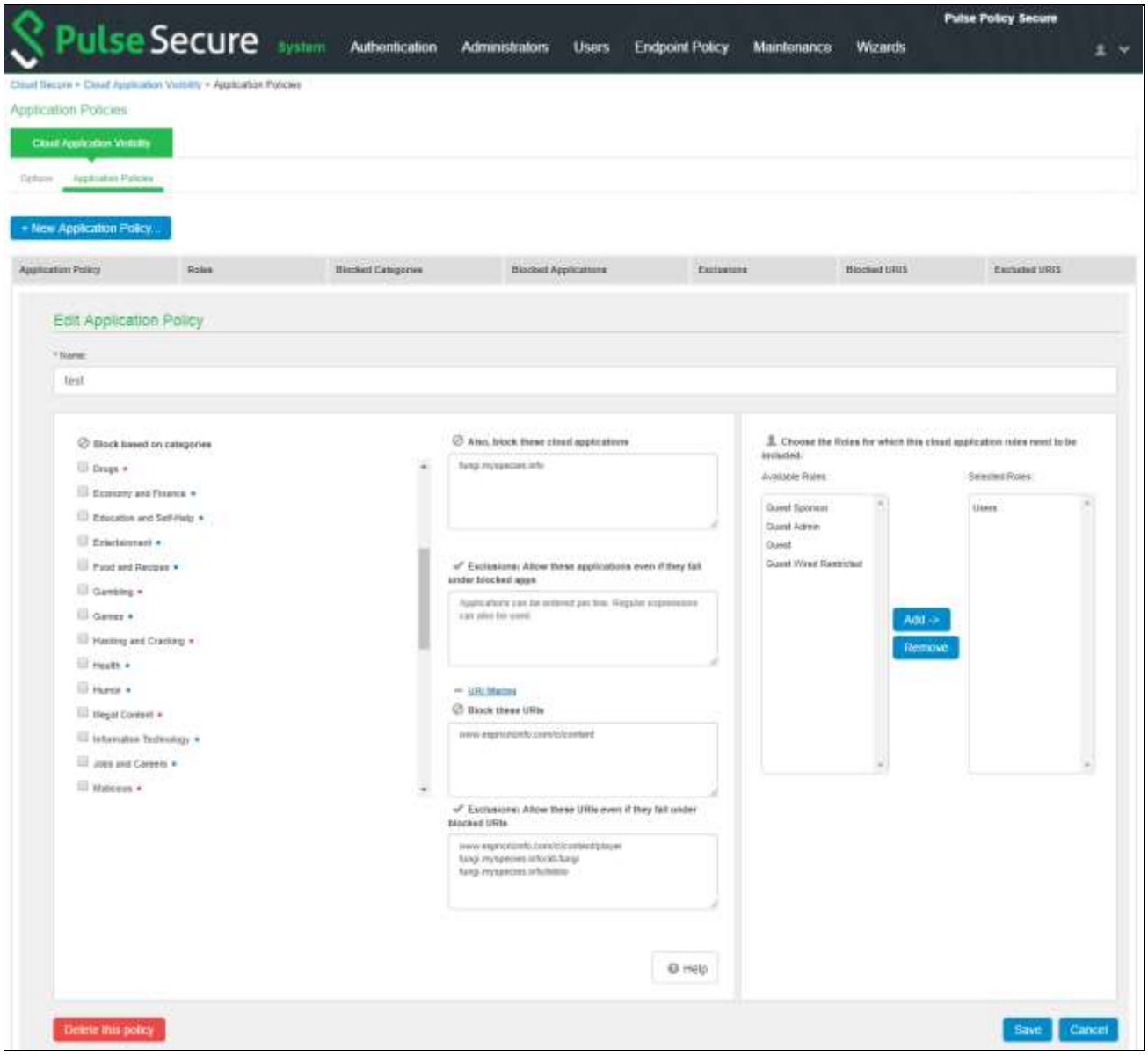
10. Choose the roles for which the cloud application policy has to be included.
11. Click **Save**. Once added, the list of allowed and blocked applications is displayed as shown below:



In the below example, URIs fungi.myspecies.info/all-fungi and fungi.myspecies.info/biblio are accessible by the user even though the domain fungi.myspecies.info is blocked.

Also, URI www.espncricinfo.com/ci/content/player is accessible by the user even though the URI www.espncricinfo.com/ci/content is blocked.

Figure: CAV Application Policies Page



Following table describes the sample configuration of this example:

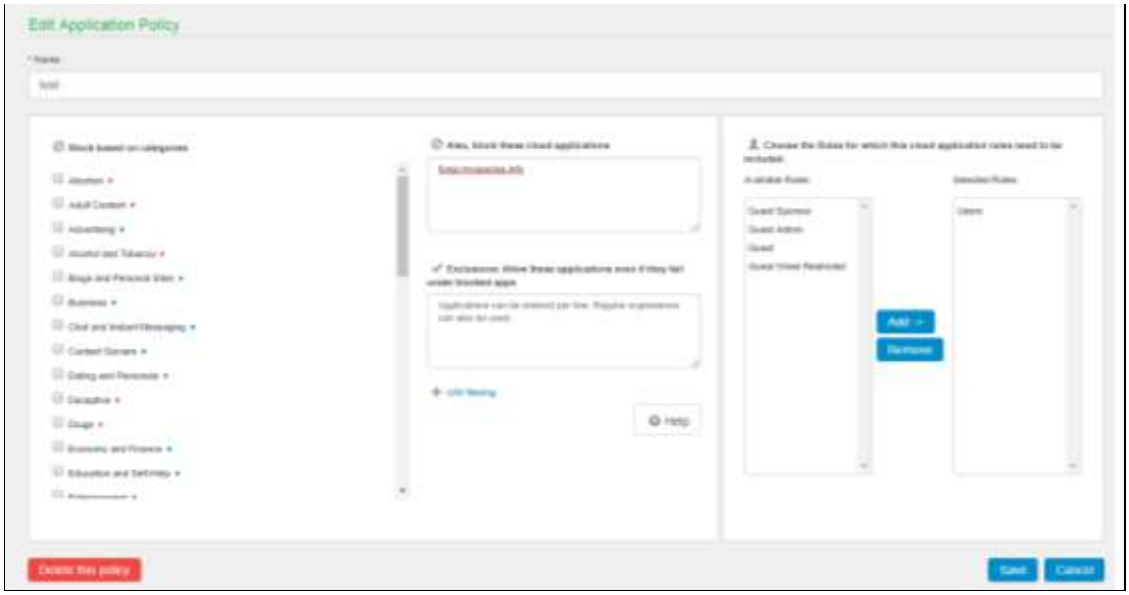
Field	Field Value
Also, block these cloud applications	fungi.myspecies.info
Exclusions: Allow these applications even if they fall under blocked applications	None
Block these URIs	www.espncricinfo.com/ci/content
Exclusion: Allow these URIs even if they fall under blocked URIs	www.espncricinfo.com/ci/content/player fungi.myspecies.info/all-fungi fungi.myspecies.info/biblio

Editing/Deleting Application Policy

To edit/delete the application policy:

1. Select the name of the application policy. The Administrator can edit the configuration by clicking the Name of the application set.
2. You can edit the application set Block based on categories, exclusions, roles and then click **Save.**
3. To delete the application set click **Delete this policy**.

Figure: CAV Editing/Deleting Application Policy



Cloud Application Visibility Dashboard

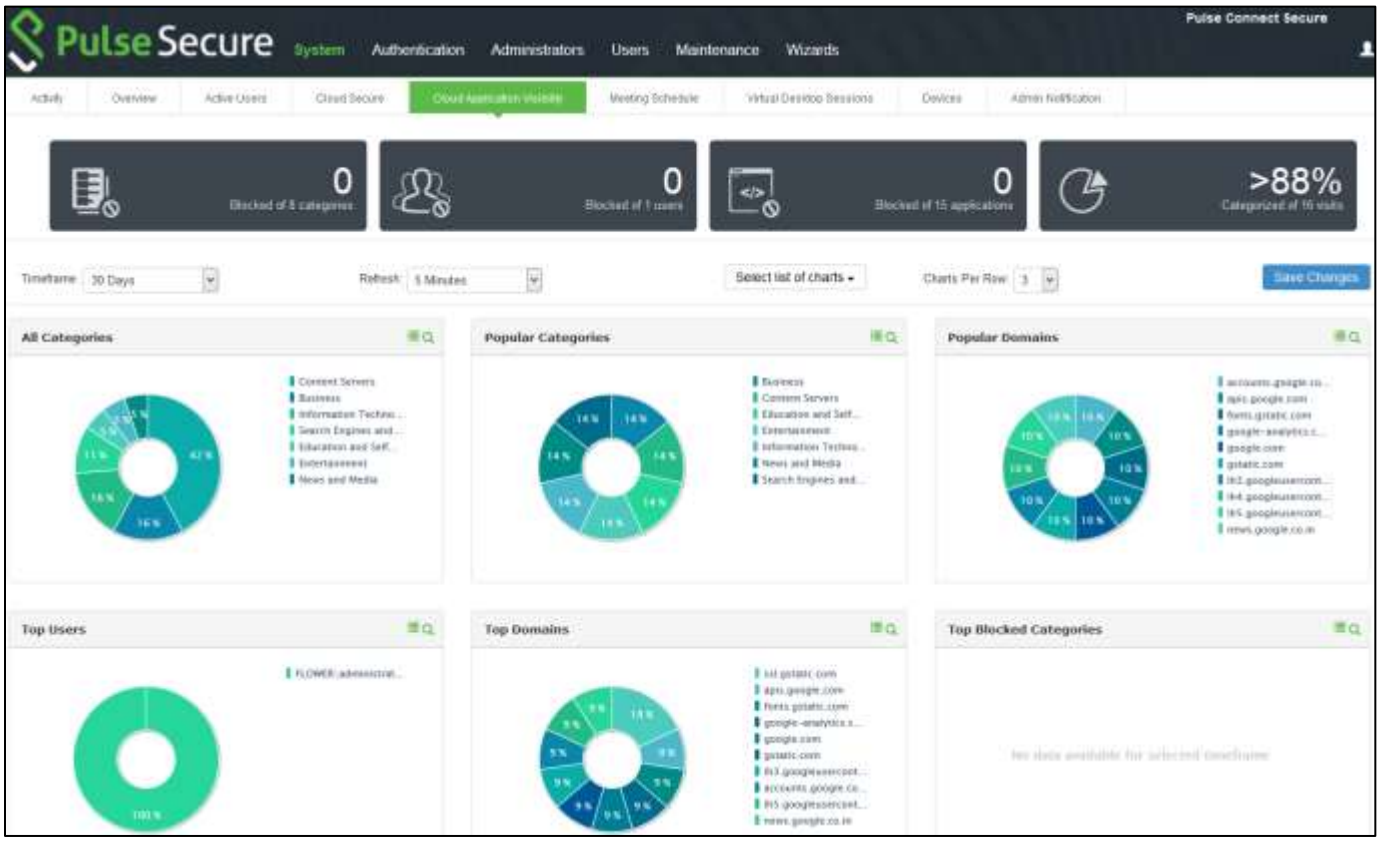
The Cloud Application Visibility dashboard provides visibility of the Cloud Applications used in your enterprise. It provides visibility to all the internet applications used by the user, which includes both the authorized and un-authorized applications so that the Administrator can determine any anomalous behavior.

To view the Dashboard, select System > Status > Cloud Application Visibility.

You can also drill down to other categories such as:

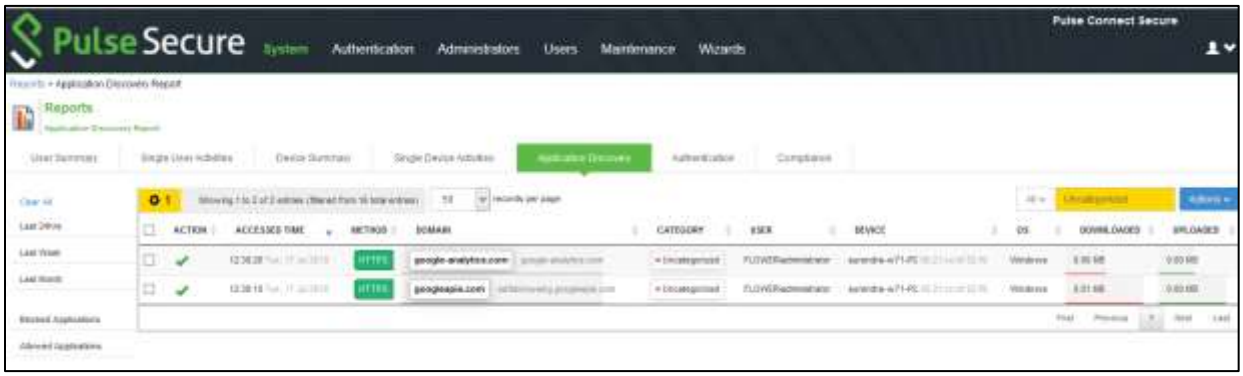
- Popular Categories
- Top Domains
- Top Users
- Top Blocked Categories

Figure: CAV Dashboard Page



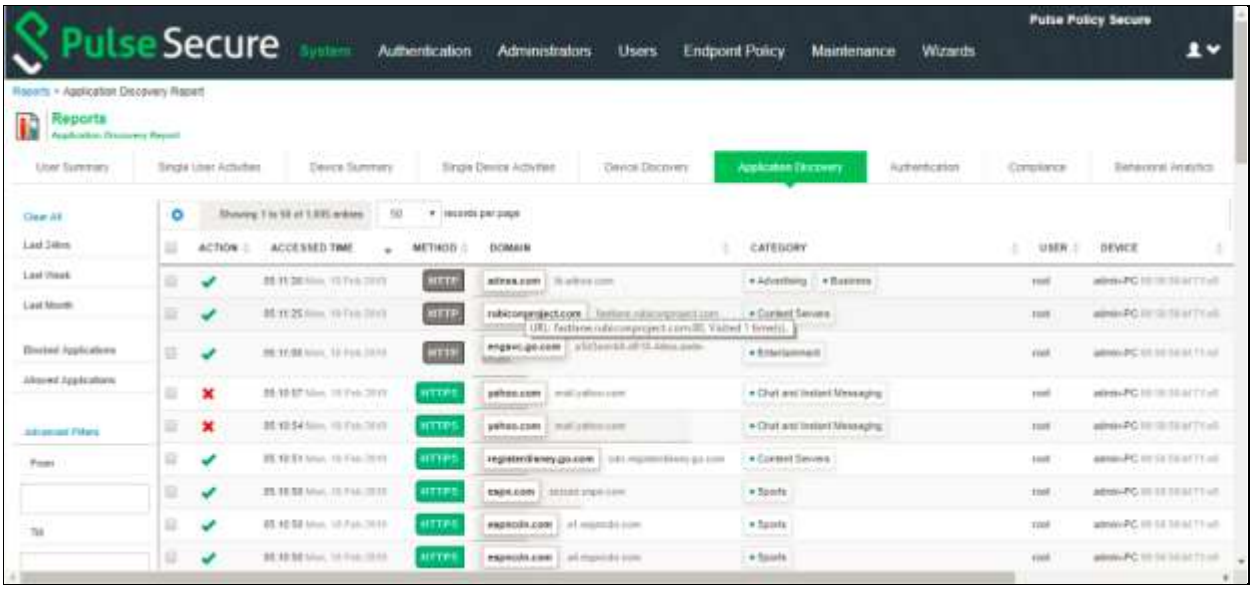
You can also analyze the cloud application usage pattern using the application discovery report from the dashboard. On clicking the statistics on the desired category, Administrator will see the Application discovery report.

Figure: Application Discovery Report Page



You can also see the comprehensive Application Discovery report from System > Reports > Application Discovery Report.

Figure: Comprehensive Application Discovery Report



Note: For http websites complete URI is seen when the cursor hovers the corresponding domain.

The maximum size of visited data stored is 1 GB and once the maximum size is reached, entries are replaced based on First in First out (FIFO) method.

Event Log messages

The event and debug logs can be used for troubleshooting:

The Event logs are generated for the following:

a. CAV Proxy Client Auth token request is logged.

b. When the Administrator exports the CAV data.

You can use the User Access and Admin Logs in case of any issues. The user access logs are generated whenever there is a Role change or when the session is established. The Admin Logs are generated whenever there is a change with CAV options and if there are any changes with respect to application policies.

You can also use Maintenance > Troubleshooting > Monitoring > Debug Log for debugging issues.

Cloud Secure User Experience

Cloud Secure is designed to provide seamless user experience across mobile devices and desktops. Cloud Secure gives better user experience by using features like Certificate authentication and On demand VPN for session establishment.

End-User Flow on Mobile Devices

Once administrator configures Cloud Secure and creates a new user if not present in Pulse Workspace, user must follow below steps to register the mobile device with Pulse Workspace and get seamless secure Single Sign-On access. For PWS registration, see Provisioning Devices.

1. Install Pulse Client on the mobile device. VPN profile will get configured automatically on Pulse Client.
2. 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.
3. Access the application, provide the custom domain or the user name for accessing applications.
4. Sign-On will happen and user will get access to the application.

Screenshots

Login screen

Authorization Failure Screen

End-User Flow on Desktops

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

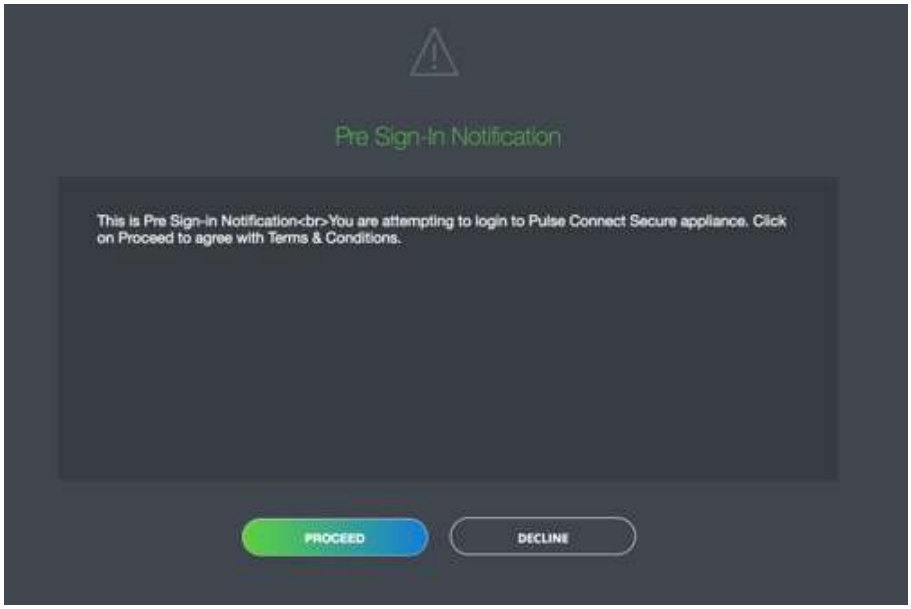
1. Launch Pulse Client and establish a VPN session with PCS.
2. Open any web browser on the desktop and access cloud service.
    a. If the user has an existing VPN session, 'Re-use existing Pulse Session' is used. PCS sends SAML response to cloud service and the user access is granted.
    b. If the user did not establish Pulse VPN session as mentioned in Step 1, user will be redirected to Pulse Connect Secure user login page for authentication depending on the PCS configuration. Once authenticated, PCS will send SAML response to cloud service and the user access is granted.

Note: Automatic VPN connection, based on location through Pulse client in Desktops and through On-demand VPN support in mobile devices eliminates users triggering manual VPN connections.

Screenshots

1. Open the web application (For example, Google), enter the email ID and click **Next**.

Figure: Pre Sign-In Notification

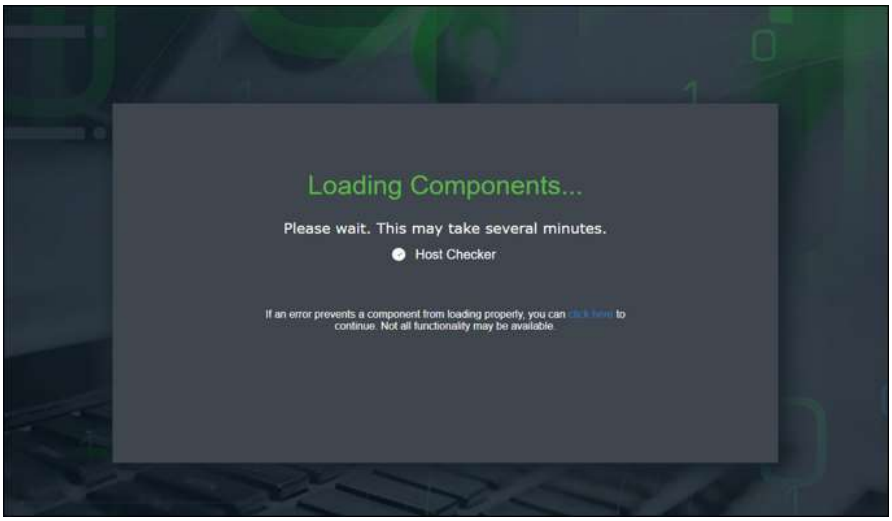


2. Log in to the PCS server using the user name and password and click **Sign-In**.

Figure: User Login Page

3. The host checker process starts and the following page is displayed.

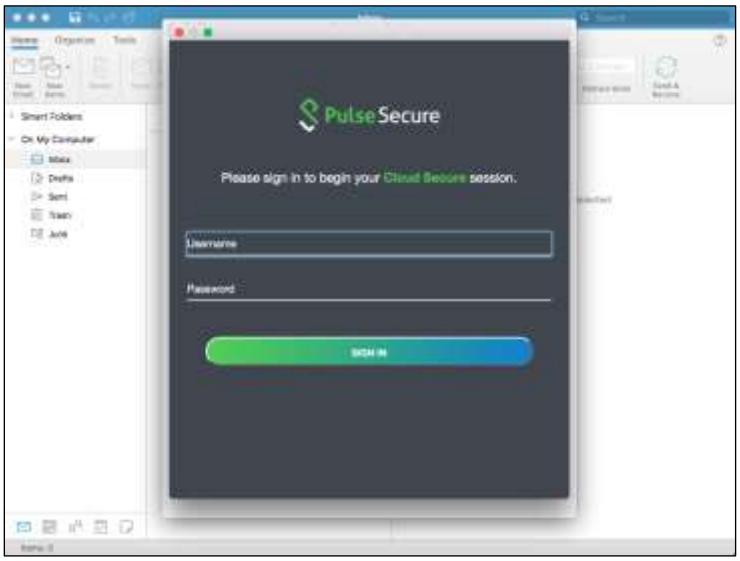
Figure: Host Checker Launching Page



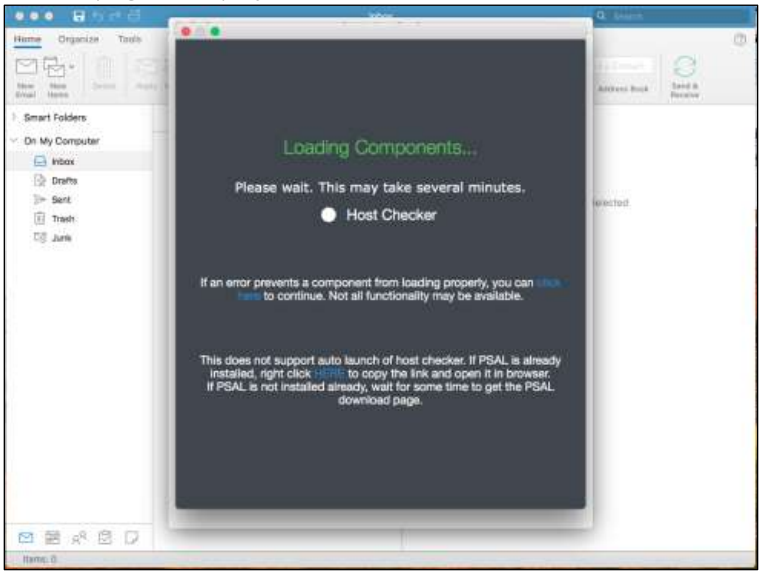
Screenshots for Outlook Application on Mac OS

1. Open the Outlook application, enter the username and password and click **Sign-In.**

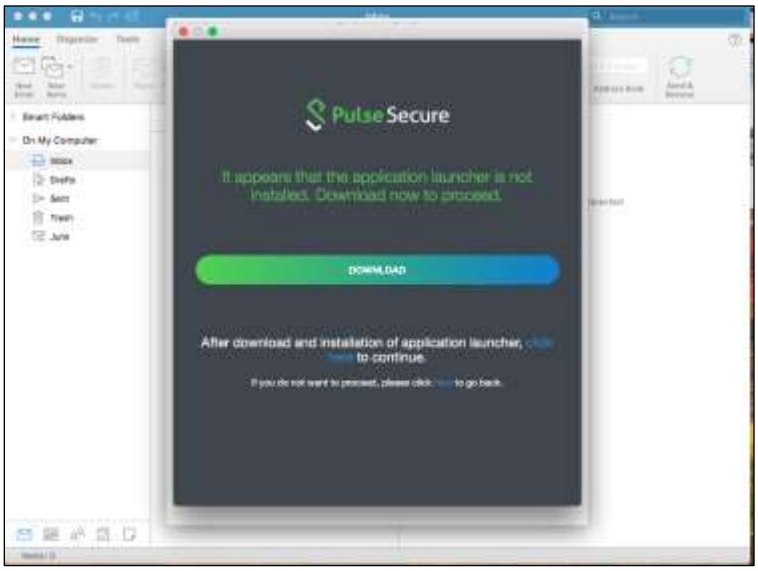
   Figure: Pre Sign-In Notification



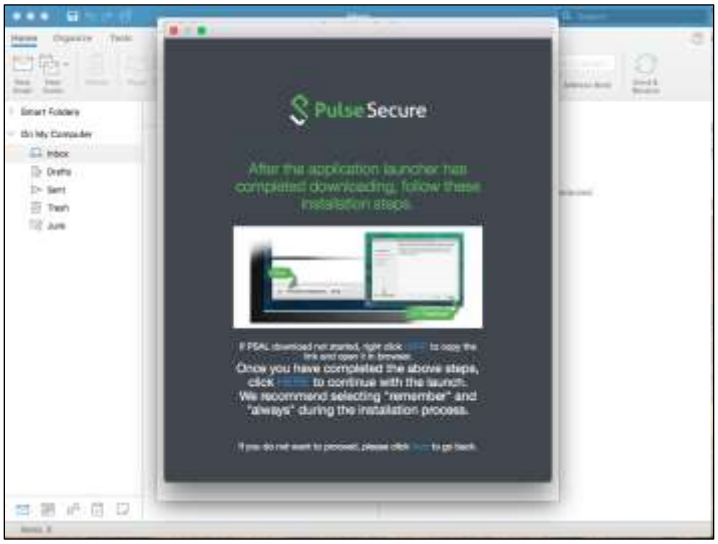
2. The HC page is displayed.



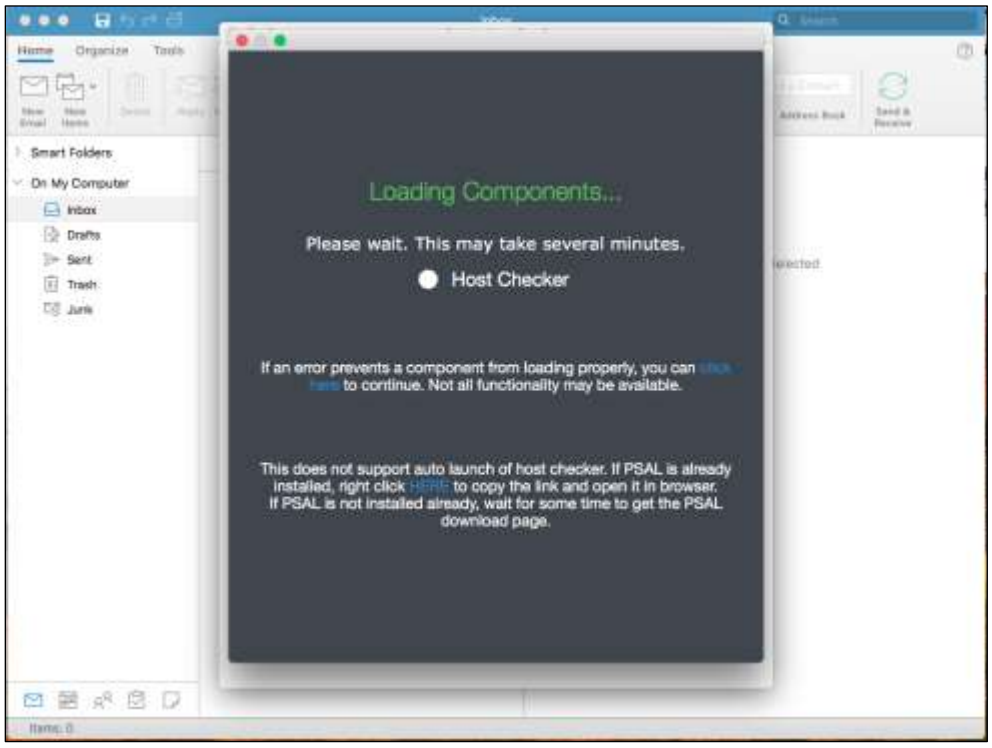
3. If PSAL is not installed wait for the PSAL download page.



4. After clicking on Download, click the Click **Here** link to download and install PSAL.



5. Right click and copy the link and open it in a browser to launch the Host Checker.



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.

This section describes the various troubleshooting tasks:

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 VPN Profile got pushed onto Pulse Client and desired connection is set as default.

  Access Pulse Client mobile application. Check if there is a default VPN connection pushed and managed by Pulse Workspace.
- 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.

Desktops

- Check if Pulse Client is installed and desired VPN connection is available.

Pulse Connect Secure

Follow the below steps to validate the configurations on Pulse Connect Secure.

- Check all the Realm/Role HC restrictions are configured properly.
- Wildcard or SAN (subject Alternative Name) certificates should be used on PCS for signing SAML messages for seamless SSO access to cloud services.
- Alternate Host FQDN for SAML should be resolvable when SSO enabled cloud service is accessed via browser.
- Make sure User Role configurations are configured for either L3 or L4 VPN Tunnel and respective settings should be turned on in Pulse Workspace for Mobile clients. In case of Android mobiles and Macintosh laptops, L3 VPN is the only supported tunnel type.
- Intermediate CAs should also be uploaded to Pulse Connect Secure if your device certificate is issued by an Intermediate CA.
- Make sure that LDAP Server is reachable from Pulse Connect Secure.

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.
- You can perform a packet capture on the client machine.

Pulse Workspace

Follow the below steps to validate the configurations on Pulse Workspace:

- Make sure all the applications are configured with Per-App VPN network access except Divide Productivity application under Android App Rules.
- Make sure that all Applications got installed on the user device. Navigate to Workspaces-> Users-> <Username> -> <Device>. This shows list of all installed applications. If installation is successful, Pulse icon changes to green for the respective app. If installation is not successful, then Pulse icon stays grey.
- Make sure PCS Appliance registration is successful. Navigate to Appliances 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.

Troubleshooting Tips

This section outlines common error messages or problems encountered during the integration of Cloud Secure Solution with multiple Service Providers and provides probable solutions to resolve them.

Scenario: Pulse Connect Secure failed to send SAML Response to Service Provider.

Symptoms:

- Pulse Connect Secure received SAML AuthnRequest from Service Provider but did not send 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.
- **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.
- **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.
- **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.
- **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.
- **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. Check the signing certificate configured on Service Provider.
- **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.
- **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.
- **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.
- **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.
- 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.
- **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**.