

Cloud Secure Administration Guide

Product Release9.1 R8PublishedJuly 2020Document Version3.0.3

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

https://www.pulsesecure.net.

© 2020 by Pulse Secure, LLC. All rights reserved.

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

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Cloud Secure 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 " <u>Conditional</u> <u>Access</u> " section.		9.1R8	
Conditional Access	Updated " <u>Conditional</u> <u>Access</u> " section.		9.1R5	Added location based access.
Conditional Access	Added " <u>Conditional</u> <u>Access</u> " section.		9.1R4	
IdP Initiated Single Logout	Added " <u>Configuring IdP</u> Initiated Single Logout" section.		9.1R2	
URI Filtering	Added URI Filtering functionality in the section "Configuring <u>Cloud Secure</u> <u>Application Policies</u> " and modified the section " <u>Cloud Application</u> <u>Visibility Dashboard</u> ".		9.1R1	
ECP Throttling	Added " <u>ECP Throttling</u> " section.		9.1R1	
Cloud Application Visibility	Added a new chapter for " <u>Cloud Application</u> <u>Visibility</u> ".		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 " <u>Configuring PWS for</u> Location Awareness" section is updated.		9.OR2	

Table of Contents

REVISION HISTORY	3
TABLE OF CONTENTS	4
CLOUD SECURE OVERVIEW	7
Product Briefing	7
Salient Features of Cloud Secure	8
End-User Platform Support Matrix	9
Third-Party Integration Support	9
DEPLOYMENT SCENARIOS	10
Deployment using Web Browser SSO Profile	10
Deployment using Enhanced Client or Proxy (ECP) Profile	11
Deployment using Third-Party IdP	12
Deployment for On-Premise Users	12
ON-PREMISE USER SSO FLOW	13
CONFIGURATIONS	14
Configuring Pulse Connect Secure	15
Basic Configurations	15
Reusing existing PCS configurations	16
Prerequisites	16
LIMITATIONS	16
Basic Configurations (Mandatory)	17
CONFIGURING AUTHENTICATION SERVERS	17
Configuring SAML/IDP Settings	19
Configuring VPN Connection Profiles	21
Advanced Configurations (Optional)	23
Configuring Third-Party IdP Settings	23
Configuring MDM Settings	
Configuring Compliance Policies	
Configuring Applications	
Configuring IdP Initiated Single Logout	
Prerequisites	
Configuring Single Logout	
End User Workflow	
CONFIGURING PULSE POLICY SECURE FOR ON-PREMISE/LOCATION AWARENESS	
Configuring Pulse Policy Secure as IF-MAP Client	
Configuring Pulse Policy Secure as IF-MAP Federation Server	43
Configuring Pulse Connect Secure as IF-MAP Client	
CONFIGURING PULSE WORKSPACE	46
Configuring Pulse Workspace for Mobile Compliance Policies	51
CONFIGURING PULSE WORKSPACE FOR LOCATION AWARENESS	52
Configuring On-Demand VPN for Android devices	54

REDESIGNED END-USER PAGES	
COMPLIANCE FAILURE NOTIFICATION	
ECP THROTTLING	
ENABLING ECP THROTTLING	
Viewing Blocked ECP users	
ROLE BASED ACCESS CONTROL	60
CONDITIONAL ACCESS	61
Conditional Access Policy	61
Conditional Access Settings	
Configuring User Group	
Configuring Device Versions Settings	
Configuring Posture Assessment Settings	
Configuring Additional Authentication Server	
CLUSTERING	
CLOUD SECURE ACTIVE/ACTIVE CLUSTER DEPLOYMENT	70
CLOUD SECURE ACTIVE/PASSIVE CLUSTER DEPLOYMENT	71
DNS Server Configuration	71
DASHBOARD	72
REPORTS	74
Applying Data Filters	75
Sorting Records	
Exporting Cloud Summary Report	76
CLOUD APPLICATION VISIBILITY	77
OVERVIEW	77
Benefits	77
CONFIGURATIONS	
ENABLING CLOUD APPLICATION VISIBILITY AT ROLE LEVEL	
CONFIGURING CLOUD APPLICATION VISIBILITY OPTIONS	
Configuring Cloud Secure Application Policies	
EDITING/DELETING APPLICATION POLICY	
CLOUD APPLICATION VISIBILITY DASHBOARD	
Event Log messages	
CLOUD SECURE USER EXPERIENCE	
End-User Flow on Mobile Devices	
End-User Flow on Desktops	
TROUBLESHOOTING	
Mobile Devices (IOS/Android)	
Desktops	
Pulse Connect Secure	
Pulse Workspace	
TROUBLESHOOTING TIPS	
Service Provider Specific Troubleshooting	

Pulse Connect Secure	
End User Device	
REQUESTING TECHNICAL SUPPORT	

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.





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.





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

vNote: 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 Expor**t: 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
 - Basic Configurations (Mandatory)
 - Advanced Configurations (Optional)
- Configuring Applications
- Configuring Pulse Policy Secure for On-Premise/
- Configuring Pulse Workspace

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.





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

O Date of the			Pulse Connect Secure
S Pulse Secu	re system Authentication Administrators Us	ers Maintenance Wizards	
Cloud Secure > Cloud Secure Configuration >	asic > Authentication Server		
Authentication Server			
Cloud Secure Configuration Clo	Application Visibility		
Basic Applicators Contitional Acces			
Active Director	A Configured aut Authentication Server Settings	athentication Server heithration server for user authentication	Edit Add New Find Server
Server Name	AD204		
User Name	Administrator		Test Authentication server configuration details
Password			Test Server
Domain	Personal		
Kerberos Realm	PULTERANET		
	Continue with these settings?	OK LATER	

🕖 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

Ise Secure	Carbon Authoritication Administration House	Maintenance Manufe	Vinite Builden
itse secure	System Authentication Administrations Users	Marnenance wizards	
Authentication Server Se	ntings		Edit (Add25or (Ebd25orse
Server Type	LOAP	y.	Test Survey
Server Name	LDAP		Buccassfully writed LDAP connection authors
Hostname or IP Address			Test Server
Port	389		
Server Type	Action Constrany	*	
Connection	Userstyped	9	
Admin DN	in a manufacture company company in the		
Password			
Base DN	(B-paintinantanian) (awa)		
Fitter 0	samaccountrame=4J8ER>		

🕖 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

O Date C		Pulse Connect Secure	
Secure System	Authentication Administrators Users Maintenance Wizards		1.4
Cloud Secure > Cloud Secure Configuration > Basic > SAML Settings			
SAME Settings			
Basic Applications Conditional Access			
SAML Metadata Server Settings	Pre-aliced from PCS GAMELAGP Settings Configure antiengs for enabling S3O access	Edu	
	recapulcaceounganet.		
Alternate Host FQDN	100		
Entity Id	https://sco.gutenneeurogu-werkenu-wanvanvermi-endpoint.cg/	1	
Sign-in URL	- Create New-		
New Sign-in URL			
Sign-in Page	Default Sign-In Page		
Subject Name Format (3)	Email Address •		
Subject Name 🧐	-USERNAME-@pulsesecurega.net		
Signature Algorithm 🔋	■ Sha-1		
Use Redesigned pages	● Yes ◎ No		
Certificates for SAML Settings		Upland a New Certificate	
pulse.secure.net@pulse.secure.ne t Jul 16 05:47:17 2018 GMT to Jan 6 05:47:17 2024 GMT	pulsesecurega.net@Go Daddy Certificate File Choose file pulsesecure Certificate Authority - G2 Private Key (Optonal) Choose file Jun 13 08:42:13 2018 GMT to Jun 13 Password (Optional) Uptoad		
	Continue with these 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

O Date C						Pulse Connect Secure	
S Pulse Secure System	Authentication A	Administrators	Users	Maintenance	Wizards		1~
Cloud Secure > Cloud Secure Configuration > Basic > VPN Connect VPN Connection Profiles	on Profiles						
Cloud Secure Conliguration Cloud Application Visibilit							
Besic Applications Conditional Access							
Enabling resource Optimisation	Co	VPN :	Settings rules for VPN	Connection		Edir	
Tunneled Resource List 9	10.96.66.105						
IP Address assignment type ᠑	DHCP			٣			
DHCP Servers 😲	10.209.112.2						
	Continue with these se	ettings?	ОК	LATER			

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



 $rac{1}{2}$ 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

540	ect IdP Provider			×
	Microsoft	okta	Ping Identity	
	_	-		-

- 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

Cloud /	Application Visibility			
Conditional Access				
Metadata File 🚷	Browse Federatio	onMetadata (8).xml		
Relay State 🕕	RPID=um:federation Mic	rosofiOnline		
Signature Algorithm	() () Sha-1 ()) Sha-256		
Select All Roles	Show Roles)			
Allow access to the	resource only if the user belongs to below selec	cted roles.		
Bookmark Settings				
Bookmark Settings Create Bookmark Configure bookmarks bookmarks	a for each SP configured with this 3rd party IDP	2. Use the below table to override Rela	systate, Subject Name format and Subject Name	e for specific
Bookmark Settings Create Bookmark Configure bookmark bookmarks Bookmark Name 0355	s for each SP configured with this 3rd party IDP Relay State RPID=um federation full crosoft Online	2. Use the below table to override Rela Subject Name Format	systate, Subject Name format and Subject Name SubjectName CREECTGUID>	o for spacific
Bookmark Settings Create Bookmark Configure bookmarks bookmark Name 0.355 Peloptees	s for each SP configured with this 3rd party IDP Relay State RPD=um:federation*MicrosoftOnline CERDPartment for MicrosoftOnline	Use the below table to override Rela Subject Name Format persistent	Subject Name format and Subject Name SubjectName CDELIECTGUID>	e for specific Remove
Bookmark Settings Create Bookmark Configure bookmarks Bookmarks Bookmark Name 0365 Salestorce	s for each SP configured with this 3rd party IDP Relay State RPID=um tederation full crosoft Dnline RPID=https://ngsa-test-dev- ed.my.salesforce.com.	2. Use the below table to override Rela Subject Name Format e persistent email	Subject Name format and Subject Name SubjectName COEUECTGUID> Cusemame>@pulsesecureqs.net	e for specific Remove O Remove O
Bookmark Settings Create Bookmark Configure bookmark bookmarks bookmark Name c365 Salestorce	s for each SP configured with this 3rd party IDP Relay State RPID=um federation MicrosoftOnline RPID=tttps://ngsa-test-dev- ed.my.salesforce.com	2. Use the below table to override Rela Subject Name Format e persistent email -Select-	vyotate, Subject Name format and Subject Name SubjectName CBUECTGUID> Cusemame>@pulsesecureqs.net	e for specific Remove O Remove O
Bookmark Settings Create Bookmark Configure bookmark bookmark Name o365 Salesforce Calestonce Cales	s for each SIP configured with this 3rd party IDP Relay State RIPID=um federation: Microsoft Online RIPID=https://ngsa-test-dev- ed.my.salesforce.com	2 Use the below table to override Rela Subject Name Format e persistent email -Select-	ayotate, Subject Name format and Subject Name SubjectName CBUECTGUID> cusemame>@pulsesecureqs.net	e for specific Remove O Remove O
Bookmark Settings Create Bookmark Configure bookmark bookmarks Bookmark Name 0365 Salestorce Creating Re-writer Enabling Re-writer in	s for each SP configured with this 3rd party IDP Relay State RPID=um federation full crosoftDnline RPID=https://ngsa-test-dev- ed.my.salesforce.com.	2. Use the below table to override Rela Subject Name Format e persistent email -select-v edirected through Pulse Connect Sec	ayotate, Subject Name format and Subject Name SubjectName COBUECTGUID> Cusemame>@pulsesecureqa.net Cure.	o for specific Remove O Remove O Add O
Bookmark Settings Create Bookmark Configure bookmark bookmark Name o365 Salestorce Create Re-writer Enable Re-writer in Enable	a for each SP configured with this 3rd party IDP Relay State RPID=um federation full crosoftDnline RPID=https://ngsa-test-dev- ed.my.aslesforce.com Relay all the traffic for the Cloud Service to be in ing additional attributes that needs to b	2. Use the below table to override Rela Subject Name Format e persistent email -Select- edirected through Pulse Connect Sec be sent as part of SAML Attribut	ayotate, Subject Name format and Subject Name SubjectName COEJECTOUID> Cusemame>@pulsesecureqs.net Cure. tte statements.	a for specific Remove O Remove O Add O
Bookmark Settings Create Bookmark Configure bookmark bookmarks Bookmark Name 0365 Salestorce Cabling Re-writer Enabling Re-writer Enabling Re-writer in EDAP server for fetchil Server	s for each SP configured with this 3rd party IDP Relay State RPID=Intrips://ingsa-test-dev- ed.my.salesforce.com Ing.additional attributes that needs to t LDAP Server.	2. Use the below table to override Rela Subject Name Format e persistent email Figure Connect Sec be sent as part of SAML Attribut	ayotate, Subject Name format and Subject Name SubjectName COBJECTGUID> CUSEmame>@pulsesecureqs net cure: tte statements. (Show Details)	y for specific Remove O Remove O
Bookmark Settings Create Bookmark Configure bookmark bookmarks Bookmark Name 0365 Salestorce Cable Re-writer Enable Re-writer Chable Re-writer Server	a for each SP configured with this 3rd party IDP Relay State RPID=un federation MicrosoftDnine RPID=https://ngsa-test-dev- ed.my.salesforce.com.	2. Use the below table to override Rela Subject Name Format e persistent email	ayotate, Subject Name format and Subject Name SubjectName <cbuectguid> <usemame>@pulsesecureqa.net .ure. te statements. (Show Details)</usemame></cbuectguid>	e for specific Remove O Add O

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

The second standard state in the second state of the second state of the second state of the second state of the	
Doud Secure Consiguration > Besic > Third-Party IOP	Isetnigs
e Configuration Visibility	
Icellors Conditional Access	
	Okta Settings Configured actings for IdP
User Identity	Edir Add New Show IdP
Subject Name Format	Email Address Y
Subject Name 🛛 🥹	<username>@<domain></domain></username>
Metadata File 🧕	Browse Choose file
Signature Algorithm	# Sha-1 @ Sha-256
Select All Roles (Show Roles) Allow access to the resource only if I	the user belongs to below selected roles.
Bookmark Settings	
Create Bookmark	
No. of Control of Cont	onnguron with this are party rue. Use the below fathe to dwarride Relaystate, Subject Name format and Subject Name for specific bookmarks.
Configure bookmarks for each SP co	
Configure bookmarks for each SP co	OK
Configure bookmarks for each SP co	OK LATER

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

	PWSSettings Coolegant Mildel server for marked of	NU.10	
Documulally enganeer the contricu	64.		
PWD Settings			Edit (Add New) Jositch MIDM
Server Name	Pets		
Registration Host 0	and in the second second		Test functionality is not supported with Phylice Workspace MOM server
Registration Code 🧕			Test Server
Network Interface	immed Pol	14	
Certificates sppronfig was impressioned Value all hep 13 30:81:05 3037 o shine Adrient	er CAFT Churse netficates or drag tham here Churses		Uphind a New Constitution
	Continue with these settings?	GAINE	

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

	Airvatch Settings	
Alrwatch Settings		Editr (Add New) Second MDM
Server Name	Advauld)	
Server Un	Man Bankle an annihistan	Test NDM server configuration defails
Viewer Uni	Tage Tapate a anna tarta	Tital Dervor
Username	later .	
Password		
Tenant Code	TJ-polojitanjitajit	
ID Template	-sardbh@Me-	
ID Type	une e	
Certificates appeonting, workspace Value of 205740/13	dex.lo Breate Choose setificates or diag them here Lititum	Eghiad a New Constitute
	Continue with these settings?	70 ·

Figure: UX: MobileIron MDM Settings

	MobileTown Settings Configured MDM server for suchic dresses	
Mobileiron Settings		1600 (Add See) Invited MDM
Server Name	Materia tran	
Server Uri	(1986)	Test MOM server certifiquation datails
Viewer Un	(##schmet/immeurspecture)	Hest Berver
Username	All with	
Password	(
ID Template	HeartDN 200-	
Certificates		Upland a New Contificate
appointly,workspand Valid till 265740013	Lesta	
	Cardinue with these 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

levieu Comilance P			
	dicies across devices		Crean 4 new Desiting Compliance Policy Edit Mobile Compliance
ew Desktop Policy Details			
Policy Name	HCt		
05	CHECK	DETAILS	POLICY
Mac .	Process.		Orry V Add. O
Windows	Process	nstopad ave	Required . Remover O
Mac	Process	Terminal	Dany Remove O
Configure the compli	ance policies for Deski	Allo Ovices	
Configure the compil	ance policies for Deski ance policies for Mobil	Atto Street.	
Configure the compil Configure the compil os	ance policies for Deski ance policies for Mobil CHECK	ARD: 24054.	POLICY
Configure the compil Configure the compil os	ance policies for Deski ance policies for Mobil CHECK INCOMMANN	ARD: 24031. tops es DETAILS	POLICY Deny Y Add O
Configure the compil Configure the compil os	ance policies for Deski ance policies for Mobil CHECK INCOMPLIAN	Atto Ovical tops es DETAILS 1	POLICY Deny Add O Request
Configure the compil Configure the compil os (Anares) (M) (OS Anaros)	ance policies for Deski ance policies for Mobil CHECK INCompliant	Atto: Overal. tops es DETAILS 1 1	POLICY POLICY POLICY PO
Configure the compil Configure the compil os (Anares (a) 105 Anaros	ance policies for Deski ance policies for Mobil CHECK INCompliant	Atto OwnerL tops	POLICY POLICY Orry Add O Propund Orry Orry O
Configure the compil configure the compil cos (<u>Anamis</u>) (OS Aested Compliance policies	ance policies for Deski ance policies for Mobil CHECK INCompliant INCompliant INCompliant	Atto: Ownert. tops	POLICY Orry Add O Request Orry Orry
Configure the compil os ///////////////////////////////////	ance policies for Deski ance policies for Mobil CHECK INComplant INComplant INComplant	AED: Overal.	POLICY POLICY Perguned Perguned Pe

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

Pulse Secure System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure
Cloud Secure > Cloud Secure Configuration > Basic	
Basic	
Cloud Secure Configuration Cloud Application Visibility	
Basic Applications Conditional Access	
Basic configuration settings are working fine. (Last modification was on 2019-12-09 03:06:42 PM)	A STREET, STREET, ST
Reuse existing configuration settings for Cloud Secure	Activate / Opdate

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.

Sec Pulse Sec	Ure System Authentication	Administrators Users M	laintenance Wizards		Pulse Connect Secure
Clifuid Secure Configuration	Houd Application Visibility				
Basic co	nfiguration settings are working fine. diffication was on 2019-12-09 03:06 42 PM)				
Add & c applicati is t	onfigure an a that is not be inst.	G <mark>ovigle</mark> Ap	ips	alesforce	box

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

Configuration of 'Office 347 apple	etica for Clean Sectors 10-47 (2010)				Deser
Enable Directory Server Kook	ID Class Dealers Success that results to be	when he part of AM	A. Million classification		
Pair of the later settings are proper	and have in the last				
Application Name	(06	100			
Application loan		Boone de-office-325 ang		Parces (
Subject Name Parenti		inst.			
Subject Harma	-0	ante-			
Melastata Datasta	0	From Local File	From Remote URL	O Manual perigeration	
Madadata URL	1 10	real result (in the monthly large to	armoula m	
Create Boolenaria 0	0	Yee 🗮			
Force Authentication Belanian	(C) April	Repet rReparet	C Reductoritate	C tyrone Re- Authentication	
Signature Algorithm 0	0	bel	🖗 Da-28		
Enhanced Client or Proxy Profile	(ECP) Settings				The Debel 35
B Detect Duplicate ECP requests	stualis and she flam	Turn seriirg 11.8a	meet autoritzatur bei ini		
Users Reseluted	4				
Bisching time (mminutes)	1.996.0				
Single Logout Settings					
Enable Single Logical Cratting the rights of range 27 and Streams		ta puntai in tas 2	7 a alea Mata sun 11 1701	night mit bezeit an	r with SP y down
Single Logant Service URL 🔒	The second	the second second strate of			
Fingle Logout Response URL					
SAM, Customization settings					
Contantos SAML atoliades (Dan Arctinias in the land in CAM, Archi-	dente A finiscentia car be e	-	ratue parts analise to be failing	I from som figurest LEAP since	nry save
User Access settings					

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

Figure: O365 Configuration Completed

Basic configuration setting (Last modification was on 20	s are working fine. 117-08-28 11:03:25 PM)			Open
Add & configure an application that's not in the list.	Office 365	Google Apps	salesforce	box
zendesk		***		

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.



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

Single Logout Settings			
Enable Single Logout Enabling this option will keep SP sessions Single Logout Service URL	slive as long as the session in this IDP is alive. Make su	re to sync assigned role's session option with SP's sess	on timeout.
Single Logout Response URL			
SAML Customization settings			

- 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.

vNote: 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.

arphiNote: 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

On L C					an as desi	Pulse Policy Secure	1
S Pulse Secure	System	Authentication	Administrations	Usera	Materiance		1.*
Configuration + Certificates > Trus	ded Serve	GA > Import T	husted Server C	A			
Import Trusted Server CA							
🛩 Certificate file							
	Im	port tran	owsei CA	Cert.cer			
♥ Import Trasted Server CAT							
Import Certificate							

- 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

DulcoSe	cure						Pulse	Policy Secure
MAP > Overview	cure system	Authentication	Administrators	Users 1	Indpoint Policy	Maintanance	Wands	1
verview								
Overview	This Client							
n IF-MAP federatio Inforcer firewalls, v	n simplifies the w Athout having to I	rork of end use og in again.	ers by letting n	etwork de	rices share	information :	about user si	essions. For exa
Choose whether t	his Pulse Policy :	Secure runs ar	IF-MAP Serve	r, an IF-M	P client, or	no IF-MAP		
 IF-MAP Server IE-MAP Client 					An IF-MAP	Server is auto	natioally an IF	MAP client of itsel
No IF-MAP								
V Server URL								
* Server URL:					1			
 Authentication 								
Basic	Including the second							
* Usemame	testuser							
* Password		1						
O Certificate								
Save Changes	Cancel							

- 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

O P I								Pulse Policy Secure
S Pulse	Secure s	stem Authentication	Administrators	Users	Endpoint Policy	Maintenance	Wizards	
Network Access - RADIUS Cla Anabia	mil = Arube							
V RADIE Client								
* Name Description	Aruba			Liberte	whereas his fitter class			
* IP Address	1.000.00			WARD	ent of this HAZPLEL Clearly			
* IP Address Range.	3			Harober	of #1 Addresses for this MADE	/I Ciert		
 Shared Secret 				RADIES	discut larged			
* Make/Model.	Aruba Networks	•		To yours	un (salariteate), see the PAD	UE Verstor		
IP Address/FQDN				17 Adda	III II TODH II BIN RADUS C	land .		
* Location Geoup	Cert Auth			Torus	or primps, see the Location G	tonage .		
V Dynamic Authorization Se	thoth							
Support Disconnect Massa	agas 🛞	Tracensed Meetings Trace	ut.					
Support CoA Messages	8	Charge of Authoritation Me	anege Support					
*Dynamic Authorization Po	rt 3799	Options: Automation Edu	enning Part					
Save Changes								

- 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

Q Pulse Secure	all all and a			Patre	Policy Secure
Configuration = Pulse One > Setting		Construction of Construction		Martin Martin	1.
Settings					
Licensing Pulse One	Security	Certificates	DMI Agent	Sensors	Client Typ
Sattings					
*Registration Host:	apl.pulseone.net		The Heat to whi	chilter appliance con	necta to sor starte
*Registration Code:			The registration	code provided by Pu	ise One
*Credential Renegotiation Interval:	6 days		t - 7 stays. The	tone wher which cred	letitura are corseg
Preferred network interface:	Internal Port	•	It that an included e	etwork interface is d	trabled, detaults t
Credentials Exchange time:	Tue 2017-01-03 11 0	0:46 IST	The last machine	and credential excha	inge time
> Registration Result Details					
Status Information					
Registration Status Notification Channel Status:	00				
Y Actions					
Save Changes Clear C	Configuration	Renegotiate Cred	ential		

- 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

8	Pulse S	ecure system	Authentication	Administrators	Users	Endpoint Policy	Maintenance.	Wizards	Pulse Policy Secur
Auth De	ne's - New MDM Server								
New 5	IDM Server								
*hares	PWE	Labor is advected from server							
Type	 Puter Wetopeta Ar Vatoh Mobile Iron Wiccest Intere 								
Pulse	Policy Secure is alread	y registered with Pulse One.	lick hers to see the de	toile.					
Save	Changes Reset	llians byrgod is gang Alabaha.	ton Pare Parengano tel 14	Apili minen					

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

Q Pulles Comme	Pulse Connect Sec	ur#
S Pulse Secure system Auto	ventication Administrators Users Maintenance Witards	1.4
User Realms > Users > General		
General		
General Authentication Policy	Role Mapping	
* Name:	Users	
Description:		
	When editing, start on the Role Mapping page	
* Sarvara		
Specify the servers to use for subscribution and a	suborization. To create or manage servers, see the Servers page	
Authentication	Cert Server •	
User Directory/Attribute	None	
Accounting:	None	
Device Attributes:	PWS •	
> Additional Authentication Server		
> Dynamic policy evaluation		
❤ Session Migration		
> Other Settings		
1		
Save Changes		

- 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

er Realms > Users > Role N	apping > Role Mapping	Rule
ble Mapping Rule		
la based on Device Web	Undate	
Device attrib	ute - Chotato	•
lame: Role Mapping 1		
Dute K de de het en of ti	an failteaning attaileata and	
rule: I device has any or th	le tollowing attribute var	ues
Attribute:	(Select an attribute)	Attributes
is •	(Select an attribute) Carrier	If more than one value for this attribute should match, enter one per line. You ca
	complianceReason	
	deviceId deviceName	
then accim these mine	IMEI isCompliant	
men assign meseroles	isCompromised	
Available Roles:	isEnrolled lastSeen	coles.
Android Users	macAddress	
Desktop Users	model	
Guest	osVersion phoneNumber	
iOS Users	platform	
T	UDID	· · · · · · · · · · · · · · · · · · ·
Stop processing rules	userEmail userId	•
o manage roles, see the Roles	configuration page.	
	the second s	

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.
- 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

O Dulas Cogura						Pulse Policy Secure	
N Putse Secure	Syntem	Authentication	Administrators	Users	Maintenance		1*
Configuration > Certificates > Trus	sted Serve	r CA > Import T	rusted Server C.	а,			
Import Trusted Server CA							
🛩 Certificate file							
	Im	port fron	owse CA (Cert.cer			
♥ Import Trusted Server CA?							
Import Certificate							

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

F-MAP > Overview					
Overview					
Overview T	his Server	This Client			
An IF-MAP federation s sehind Infranet Enforce	implifies the w	ork of end users by lett out having to log in aga	ing network devices in	share information about user	sessions. Fo
Warning Please	reduce total log	g file sizes to 500 MB,	under Log/Monitoring	and Troubleshooting, to ensu	ire enough s
Choose whether this f	Pulse Policy Se	ecure runs an IF-MAP \$	Server, an IF-MAP cl	ient, or no IF-MAP	
IF-MAP Server				An #-MAP Server is au	tomatically an I
Enhance IF-M	AP Server stor	age		Note: If PPS is used as	a dedicated IF-
- men client					

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

Q Duto Comme	Pulse Policy Secure
Pulse Secure spines Authoride above Administrations Update Endpoint Policy Maintenance V	1244-05 L ¥
IF-MAP + This Server + Clients - New IF-MAP Clients	
New IE-MAP Clients	
V IF MAP climit	
Name: PPS-IFMAP Client Abel to reference this #-MAP client	
Description:	
IP addresses 1.1.1.1 All possible source IP addresses for inbound con	sneetions from the client
✓ Authentication	
· Basic	
* Usemame: testuser	
Password Password	
Certificate	
Save Changes	

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
- 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

(COD) > CLARK ARRAY					
verview					
Overview The Cle	9.				
IF-MAP federation simplifi forcer firewails, without ha	is the work of end users t ring to log in again	ay letting network dev	rices share information	about user sessions. For	00.00
hoose whether this Pulse	Policy Secure runs an IF-	MAP Server, an IF-NV	4P client, or no IF-MAP		
IF-MAP Server			An ITAMP Datest is and	matcally as 2 MAP starts	titeet
No IF-MAP					
₩ Saruur (III).					
* Server URL	Hittpoic //10	3.204.69.124/diana-ws/	soap/dsiltr		
* Authentication					
· Basic					
* Usemame testucer					
* Password					
- Confidents					

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

S Pulse.	Secure	System Authornication Administrators Users Maintenance Wizards	Pulse Connect Secure
Segrerig in Topical Polices 5 Notema Polices 2000	Tigo et Pagan di Pendisc dT: Coordigacation (Publi	ligh & Hoshutaw	
Protocol Binding to use for 14 = Post = Artilact	AM, Baquess		
* Signing Certificate	1.	Everifiam record for special lists, susception setting the setting	
Decyptor Cethcate	No Encrypticity	* California U un De designing dia keryapisa dan di Della menggin and dia ber Ben Seria Randon (P). Sin andhan a panta dia panta di sure D' a mengi ba mai a da Sela. Menagan	
Offer Configurations # Rease Existing NC (Po Rease Existing #RAW) # Accept ansigned Autor Sign BANL Assertion	ubel Secolar P Secolar PRoquest	Provided, Narowing HC, Principeness (Legend for particle for DF Schwarz HC) provide control of automating Narowing particles in matching in the DF perturbation Provided, Narowing HC, Principeness (Legend for any of Narowing Schwarz HC) provide control of automating Narowing particles in matching in the DF perturbation Provided for any particle schwarz (Legend for Schwarz HC) provide and the DF perturbation Provided SCH, providence with an interpret of the DF perturbation of the DF perturbation of the DF perturbation Provided SCH, providence with an interpret of the DF, provide schwarz (Legend TC) and provide the state of the DF perturbation Provided SCH, providence with an interpret of the DH, respectively which matching TC and provide the state of the DF perturbation Provided SCH, providence with an interpret of the DH, respectively which matching TC and provide the state of the perturbation Provided SCH, providence with an interpret of the DH, respectively which matching TC and provide the state of the perturbation Provided SCH, providence with an interpret of the DH, respectively of the DH, respectively of the state of the state of the perturbation Provided SCH, providence with an interpret of the DH, respectively of the state of the state of the state of the perturbation Provided SCH, providence with an interpret of the DH, respectively of the state of the state of the state of the perturbation Provided SCH, providence with an interpret of the SCH and the state of the state	
"Signature Algorithm	Sha-1 0 tha-356	Approximation and associate to favore and approximation for AMM, associate and managements	
3 Service Provide related	Cartol		

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

ONote: 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	Policv
	, , , , , , ,	

Pulse One Datestant	Applantes ()		- Adaptation.						
DESIGES APP CATALOG	POULIES		Add Policy						
Womapace Policies 🗶 🛄	10000		Polda name*	D	Cloud Secure				
Pelame	Retro		Select the target upers for this	policy by theasing criterie	Fors the options Delo	on The list will show	all users chosen using the entered	rritoria.	
silomet (122)	putering		Hari wine togi	4	mutsec * cs *	Autor selects	laps		
11 augustatukate Citis Inga nasaritikariti	parties a	(M)	LDAP group						
All assessment of the second s	and the second second	-			listen on the second seco				
ET gertreak teet 201 mge geneem teet	instant		Device Owner Made	3	G (BYO and Corporati	e Ownerd: 💙			
If construction (P)	particular.	181	1,7aar	Carner	Manufacturor	Magar	Carriert Pokis		
All appendix (d) toget appendix	albel		eden	Uninavia Carrier	Apple	Padi S	eden		
LT PROPAGETA (19)	autopant		APP	Pruicio Aur obiertagolo	LENOVO	Letters PB2-66	K		
17 Autore Bank III	puttined								
If active time out to an approach in the state of the sta	ettel	. 14						Cancel Save	

- 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

Pulse One	Dashboard A	opliances Vi	And And Admin	istration	*	•	4-
Pour Workspace trial Science explo	erin Frage - Ever	THE ROTAL KEY TO					
DEVIDES APP CATALO	6 POUCES						
Workspace Policies a	ALL ALLEYS -						
11 ÖöhEylö, daskihgdsa., tegedintyiö	estited	=	Cloudsecure (edited)	Fullain Actions +	Activities.	Oriented on 2017-06-10 12:464 Last modified on 2017-04-10 12:464	15 +0530 45 +0530
11 Pår Påköönen (0) tegspär-päelenen	published	=	Android Apps IOS Apps	Properties	Group Members		_
11 Pår (5) tagspär	published	ш	[Assered [JOS [A8]]	Flatform	Name	Value Value	e-
11 final (6) tage:final.test	published	=	Durbenzy		Verificat	https://www.pulleneturescans.het	
IT Ölefikişile (d) tegiszthan,tegisztrual, tent, tegis pi	edited a-piktónerviago;	III A. durhrightning	ülebəl	й.	Vpr Numeric Passworth	Tabe .	DF.
11 Test_sec (Z)	published		Giobal	4	Wpr. Beakin		128
Hann Th			Gistel	16	Vpr/Hole		107
tagaxam	puovaneo		Cloutenure	tina .	Vpn Safari Domaine	to-see publication and	18
II TestPolicy (0) tags/testpolicy	edited	m	(Joba)	ж	Vpridave Passveord	true	08
11 Cloudsecure (0) tags.cloudsecure	edited		Giebel	*	Чро Туре	Pulse SSL	128
testingPasscode+ayu (S)	edited		Gobal	14	wph Usenit Field	opername	18
test/ngPasscode+shub	edited						

- 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

Pulse One	Dashboard A	opliances V	Volkspeces Reports Admir	histration			o 4-
Your Workspeers that Remain expire	en in Roleys - Area	r twee Boarson hay fo	ere Carlos Carlos	-			
DEVICES APP CATALO	G POLICIES						
Workspace Policies o	ALL ACUME						
11 Öåfitfyið_daskjhgdsa	edited	8	Cloudsecure (edited)	Publish Actions +	Articilies	Created sin 2017-04-10 12: Last modified on 2017-04-10 12:	46:45+0530 84:45+0530
11 Pär Påköönen (0) tags pår påkönen	published		Android Apps IDS Apps	Properties.	Group Members		
11 Pår (5) tags pår	published	ш	Policy Name	Platform	Name	Velue	6
II final (6) tegs:final.test	published		Elwin (7)				
11 Öðfikéyið (ð) Tags sthan tags finlal, teid tags p	edited ar påkötnen tags:	III pår tags shilt, a	(Dobal	*	Emerginiae with inner Authentication	MSOWP	œ
IT Yest, sac (2)	published	ш	12tobel	al	Interprise Will Outer Identity		(R
tagstest_sac			Global	41	Wifi Enabled	CO.W	C/C
41 cam (2) tags.cam	published	***	Global		Wift Password		, CP
11 TestPolicy (0) tagistestpolicy	edited	ш	Gootael	et	Well Protocol	WPA2 Criterprise-EAP-TU3	(R
IT Cloudsecure (0)	edited		Global		With Save	douberure	.02
testingPasscode+ayu (5)	edited		Dobal	al.	Will Overname		OF.
testinePasscode+shub	edited i						

- 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

Puise One	Dashboard App	diances W	(oritisp	aces Pulicies Ad	ministration			• •
Workspace Policies o	Add Addons -							
Policies	Status		1	TestPolicy (public)	eit) Amerika Amerika	·	Collated on 2016-07 Last monthed on 2016-08	49.0847:574053 43.11(18)474053
Giobal (13)	published.			Android App Rules	IDS App Rules Proper	tes Group Members		
If scotte-local-testing (0) logs.acorte	edited	#88		Andruid (CS All			Experie	et All Tallacon All
11 TestPolicy (2)	published			Policy Name	Platform	Name	Value	8
tage sampoley				EActiveSync (9)				
				Global	- 41	Activesync Accept All Certs	true	a.
				Giobai	24E	Activelync Domain		
				Giobal	- ai	Activesync Server	outlook.office365.com	100
			э.	Global	45	Activesync Server Proxy	None	00
				Global	85	Activesync Sol	true	i ar
				Ckobuli	16	Activerync Userid Fleid	email	ar i
				Global	at	LIPN Domain Name		01
				Global	(at)	Use Constructed UPN for Workspace Email	false	or
				Global	38	Use Pulse One for authentication (Override Active	Sy., true	12

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

Pulse One	Dashboard	Appitances	Workspaces Polloes	Administration	1			• •-
Workspace Policies o	Ald Artion +							
Policies	Status		Demo-Policy (ed	ifed) Publish Amo		Envired on 201	5-07-11 20:27:41 +0530 6-07-11 20:27:41 +0530	
Global (0)	published		Android App Rules	105 App Rules	Properties	Group Members		
11 Demo-Policy (0)	edited	***	Arstand 105 All					inpund All Collegne All
			olicy Name	Platform	Name		Value	۲
			IOS ActiveSync (4)					
			Giobal	ice	Ios Actives	ync Enabled	true	Dr.
			Giobal	105	ios Actives	ync Name		0
			Global	105	ios Actives	ync Prevent Move	true	(iii
			Global	105	los Actives	ync Prevent Send Dy 3rd Party Apps	true	1 2

🕖 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

Pulse One		<u></u>						a
Carlo provide a line d'anne ante	eniitaun en	Add App from A	pp Catalog			A CONTRACTOR OF		
HACES AND CALME		Departure .						
Workspace Policies #	Table Contrast of	Tatte	Creater	Faibage	Category	town the second		
IT phone 7378 (1)	manad	Compiles		constituents and confi	homerent	Lang Description	ali ani 2111 2104 10 (dita)	0.01405.00
11 TestPolicy 100	antimot	-						_
11 Clausinerure (0)	million						Access	
11 percent 2 181	mattheast					No.	-	
47 tears (00	production of the					and a second	anne.	
It externation (0)	ament					211.4		10.000
southing Personal strate (3)	author					and a	-	-
susting-assesses-shok	entred							
sys-shub after (4)	and the second							
system palloy (1)	particularies and							
Sport State, Sport State, State,	Provinces .				- Eanal An	and a second		and sold party
						addate francisco	The second se	and the second s
Pulse One			Contractor Marcall		9			6 A.
No. Statement Till Income Statem	ante la maria de la filla	Configure App D	etails					
DEWOIS APP CATHLO	G POLIDES	😅 Dropbo	×					
Workspace Policies 21	ALL ALLONS							
11 Cloudsecure (9)	motort	Description	20m-64(1)(111111			Salar months		8 20 + 16 30 8 20 + 16 30
11 phees 2 (0) cogrammed any	edited							
11 emer (0)	published					Bendred	Access	
11 automation (D)	mottett					True	deet	
Cognine field and an and a second state	A REAL PROPERTY AND	Required	Mandatory for t	he user - will be auto-pushed	on enrollment	True	dent	
testingressindershot	entired.	Network access	man soon being	1	7521	Thus	INCOME IN	10
mu+shub afte (#)	auto/mberg	1.1200000000000000000000000000000000000	Per app yes					
anumites notice (1)	materia		n 1	10				
ope-nes parcy in	in the second							
ayu-snuo, eye-rur ruk	processing and							
dyane of Perconten (1)	PROBABILITY OF THE PROPERTY OF							
ananya coancya (2)								
eller manifes concelles (et	and the second				Cancel	3		
			0.00	inse secure		Conversion of Street, or	Owner and D.O. state of the local division o	STATE OF TAXABLE
				and the second		and a second second second	and the second se	and the second sec

- 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 <u>pwsstep2</u>.
 - d. Click Create.

Pulse One	Darkhaard Appliant	ie Washington Danaste	Astronomical and the second sec	5 AU
Your Workspace trial license expl	Create New Use	1		
DEVICES APP CATAL	Username:	testuser	Tags: Cloudsecure × Sendt tag	
Users QSearch	Full Name:	test	Device Match:	ant Users 9 Pending Invites
Users	Workspace Email:	testuser@abc.com	 Create a Space for this user 	
Unregistered	Provision Email:	testuser@abc.com	Send the welcome e-mail to this user	
(El 2)lbor 9() script (1)	Phone Number:		Send the welcome SMS to this user	
Unregistered			-	
(34670wBiC (1)	Create another			Cancel Create
Unregistered				
⊡7mYW00/R(1)	a, iospoliky			
Unregistered				
B7NWyZXIe(I)				
Unregistered				
			S Pulse Secure	Pulse One v2.0.0 (UR1708-93 Server:1708-63) Copyright © 2014-2017 Pulse Secure, LLC. All rights reserved.

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.

Pulse One	Build and		Martin					ı
or installed out and whether	Dashboard	Appliances	worksp	Registrati				
Appliances QSearch	×	AdAppliance	O Create A					17
Name		Mo	del	\bigcirc	Use Registration H following Registrat	lost : api.pulseone.net wi don code <mark>: 6KsbAi1g9JN9</mark>	th the to register	
🖯 😨 profilergrp (2)					your appliance.			
profiler184		MA	G-2600					se select an
profiler182		MA	G-2600				ОК	
aarti-pcs		PSA	-3000	8.2dev (shravan	6d 41min	O Not Connected		
💿 ngsa180		MA	G-2600	8.2R3:B1-44103	95d 1hr 52min	O Not Connected		
Sbrauan-54 223		SAU	1000	R 2deu (shrauan	116d 14br 18min	O Not Connected		

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.

Pulse One	Dashboard Appliances Workspaces Reports	Administration	¢ ه ه
Plate Der Poperten Worksam Propeter LDAP Groups Appel Mille Ger	Ver Norkered Tableame Ingens in 5 days. Inder new Korole key VPN Cert Subject Jasuer Expires		Pulse Doe Properties Workspace Properties LDAP Groups Apple MDM Cent Avidead for Ware Emorphics Usage Agreement
Andread for Wark Princement Unings Agreement Alternation VPIN Cert	Download Click the link to download the cert Renew Renew the certificate Renew		VPN Cert

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 <u>PWS Configuration Guide</u>.

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

DEVICES APP CA	ATALOG POL	UCIES						
Workspace Policies	C AN AN	ore +			-			
Policies	Bisture			cs-qa (published)	Actorn +	Adulan	Last medified on 2018-03-14	14.50:34 +053
Giobei (1)	published			Android Appa 10% Appa	Proefile	Group Members		
11 ankis-policy-sograde (1) tops and policy-sograde	published	88		Android 105 Al			Expend A8	daçan Al
LT ca-ga (R) tegerininge	published			Policy Name	Platform	Name	Value	0
17 un (4) tegente	published	100		Giobal		Enterprise Will inver Authentization	MICHARA	or i
11 agnit_ondemand (3) lege.opti	published	101	4	Globei		Enterprise WIR Outer Identity	Constraints on	Ċ.
						WM Enabled	Pue	9
				Cionel	ai .	Wit Passworth		in the second
				ca-qa		WM Protocol	WHO-Enterprise EAP-TLS	9
				158-Q4	W.	WVF Sekt	alout	a
				Glober	-	Will Livename		a

- 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

Pulse One Date	eard Appliances	-	- (nabiles Administration			
DEVICES APP CATALO	0 POLICES						
Workspace Policies	And Transmot						
Pylicies	Riston		li.	cloudsecure (published)	En Posy Administ		Cividad de 2011/36-00 12:29:38 +9 Lastreadiad en 2018-36-11 13:32:14 +0
Global (127)	pusinned			Australi Appen XXI Appen Properties	Oroug Manders		
11 websconfig.kalo (38) http://paccellgalid	puttioned		Т	AND IN THE AN			Expand M Collapse M
If approvely/Optional (8) http://pocoeffig:publical	patronet.			Patto Name	Patters	liate	Were
IT gyrtman test (ff) Argn galman fest	patiented			01994 (12)			
17 closefeectare (7) Inseries	puttited			(subscreen subscreen subsc		LEADIN LIGHTLY AND THE I	
11 approde (4). Ingelander (4)	with d			Underser		Ver Certificate Auto	we
41 PROS-1272 (19) logo vites: (27)	puttitied		1	Undecay		Van Connection Name	PaterNPN
47 Active Sync (B) light active spin-	published	-		deadlessee		vps.Erwiteet	
IT ACTIVE SYNC OUT SA AS P	withd			Olivitat		vijer Geoug-	
AT setprint (0) logs rates logs when ever with its energy	pulsities			disatissan	*	Yer Hart	trips. Inco. and
AT MONDUL_TANK CAY	publiched			Owner		Van Numeriji Pozoward	No
If prove p (2) High prove p	subturned			Girbst		Vor Realty	
II oden (11)	putrated			Clobal	.e.	Vps Rite	

Figure: VPN Properties for Android

Pulse One	Cashboard	Appliances	-	Analytics	Administratio	1 .			•
Your Workspoor Bial Ramon o	igens in 43 days	Enter new lice	nia key hi			diame.			
DEVICES APP C	ataLOG	PODDIES							
Workspace Policies	2	Parent al		Cloudsec	ure (public	shed)	Eat Folly	Cleated or Last modified or	201217 1.921 - 22
11 (ext12 (0) high-heat12	published	m		Androide Appen	K05 Apps	Properties	Group Mambers		
11 manth (2) togs as with	published	***		Antroid IOS	14			Ex	codagee All
18 ankit tout (8) tage and lesi	published	IH		Policy Name		mattern	Nare	Value	٥
IT Islag-test (0)	published			Citudoscura			Enable Location Awareness	true	a
#1 DEP (0) lighting	published	**	II.	Clobal		android.	On Demand VTW Timeout Immuter)	5	3
II centra (0) tage mintre	published	100		Clouideante		antrad	Shafty Medie	the	
II bb (0) lege to	published			Global		88	toe L3 VPN	Tables	a.
If antifold-location-aware higt android-location-assessment	published	100	11	Giotturi			Vgir Certificate Auth	true	C/
11 Cloudwetare (#) Ingt.an	published	=		Cloudsecure			Van Connection Name	CSVPN	9
			1.10	Camadacora		0000948	ATL POPULATION (1994	Garriseinen.	1.

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

n-demand-vpn (s	difact) Puttern Actors	Actuities	Crusteet In Last modifies of	37.62.1333.3
Andread 101 Augus	Properties Organise	ribera		panit Ali Collagna Ali
Status Name	Platform	hame .	Value	0
IV9N (171				
Global	108	Enable Location Awareness	false	æ
Global	android	Circ Demand VPN Timeout (romules)	(B);	æ 🏢
en-demand-vph	android	Ethealth Mode	114	
Olabai	ium (UNELS VPN	tarse	Cit .
an-demand-upit	(at	Vpn Certificate Auth	trim	CX III
an-bemand-spri	and the second sec	Vpr Convector Name	VPN	
un-demand-upn	android	Vpn Connection Type	prOemand	
un-demand-upt		Vpr Enabled	154	CH I
Grobal	47	Von Group		

For more information, see <u>PWS Configuration Guide</u>.

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

SAME Motortatis Science Software	SAMLAR Settings		ja.
Host FGDN	No. gaberni ama comp. Anti		
Atturnate Host FGDN	Starty up: Separation reg		
Entity ki	Nan Ster prime constants and these records are expected age	Propulation / Upstanee	
Sign-in URL	*****		
Subject Name Format	Ernel Address		
Subject Name	distinues - Conservation of		
Signature Algorithm	= Sha-1 - Sha-256		
Una Flachesigned pages 🧕	· Via		

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

Year Main Main Main Main Main Main Main Main	0		30		=			Pulse Connect Secu	(e):
Sign-is page Sign-is page DataIt Sign-in Page * Transform Transform Transform Transform Transform Solution sign-is page Transform Transform Solution sign-is page Transform Transform Solution sign-is page Transform Solution sign-is page Transform Solution sign-is page Solution sign-is page Transform Solution sign-is page S	S Puls	eSecure	System Au	uthentication Admin	istrators Users	Maintenance	Wizards		1~
Signish gap: Default Signish Pagi * Meeting UR: ************************************									
Meeting URL * meeting* Attention mean Seech how to saled an authentication reade oder algoing its. Our types the mean reade The sea wort type the intex of the excitation argoing autos. Our types the means Our types types the means Our types types the means Our types types types the means Our types types types the means Our types types types types types the means Our types types	Sign-in page	Default Sign-In Pa	gal * 1911 - 110 Samin payon						
	Meeting URL	*imeeting/	3						
Specify how it saided an authentication reader when algoing is User Typics the reader same The ase multiple the reader of dubentication reader. 4 User joints from all of authentication reader. 4 User joints from all of authentication reader. 4 User joints from all of authentication reader. 5 User those were the falses states authenticates causes when they sign if all or one reader is selected. It is autoraticately used the regular page will stat during the list). To reade or manage mores, see the loss <i>luthentication</i> page or the <i>lubenticate</i> 4 Users 5 User those causes 5 User those the falses 6 Users 7 Concerts Eigen Relations 9 Po-Auth Sign-Is holfscation: 9 Po-Auth Sign-Is 	- Authentication reak	6							
 User typics the reatin name The sets multiple the rises (if each of the switched sources) User picks from a list of authentication restms Arstation reating Selected reading Selected reading Users Selected reading Multiple Work Duration Selected reading Selected rea	Specify how to select	an authentication realm v	duerr aligning to						
The same watch by the farms of the or all label sufficients on maximal.	- User types the m	raim name	and a grant grant t						
* User picks from a list of authentication realmanage meanses, see the User Authentication page on the Authentication page on	The uses must type to	he name of one of the available	6 authentitation resime.						
The same wait should use of the following sets that is the information page of the same is even match is sets chell, it is automatically used the same is page will set standard, the taip. To predie of maxage manes, see the User Automaticality page of the Automatic	· User picks from	a list of authentication r	naime						
Available readins: Selected readins: Desktop Addis Modellap Modellap <td>The ster studi shoot Automotion page</td> <td>e are if the following selecte</td> <td>l istlierlication essens iste</td> <td>en they sign in 11 anis one realm is</td> <td>selected, it is automatically</td> <td>uted the sign-in page via</td> <td>i ast display the laty. To used</td> <td>or manage reasons, see the User Authoritation page or the Au</td> <td>minimator</td>	The ster studi shoot Automotion page	e are if the following selecte	l istlierlication essens iste	en they sign in 11 anis one realm is	selected, it is automatically	uted the sign-in page via	i ast display the laty. To used	or manage reasons, see the User Authoritation page or the Au	minimator
Desktop Middlas Remove Remove Move Down Pre-Auth Sig-Is Notification Pre-Auth Sig-Is Notification Pre-Auth Sig-Is Notification Additional Settings Additional Settings Enable index index pages for this Sign-in Policy The Theorem is the sign of the Sign-in Policy	Available realmo.	Se	elected realms						
Michies Remove Move Down Configure Reprin Roblewines Configure Reprin Roblewines Pro-Auth Sign-Is Notification Advanced Software Advanced Software Employment population was why for Clear Toware Laters Save Chargets	Desktop	- Add-> U	sers	Move Lip					
Configure Signa Bolification Pro-Auth Sign-Is Notification Advanced Settings Advanced Settings Configure Indesigned pages for this Sign-in Policy Bave Chargets Save Chargets	Mobiles.	Remove		Move Down					
Configure Sign Addition Configure Sign Addition Pro-Auth Sign-In Notification Post-Auth Sign-In Notification Advanced Softings Advanced Softings Enable indesigned pages for this Sign-In Paloy Barke Champer									
Configure Equity Robinstone Pro-Auth Sign-In Notification Advanced Settings Advanced Settings Configure redesigned pages for this Sign-in Policy Robin Robinstoner Josef and the Configure Setting Robinstoner Settings Setting Robinstoner Settings									
Pro-Auth Sign-In Notification Advanced Settings Advanced Settings Carter Indesigned pages for this Sign-In Policy Read Industry of Clear Tences Settings Save Chargets	V Configure Signific Ro	data allocations							
Post-Auth Sgr-In Notification Advanced Settings Conditional system Policy Total Theorem And and My for Clear Sectors Save Chargets	III Pre-Auth Sign-Is	NotEcation							
Advanced Settings Enable redesigned pages for this Sign-in Policy Toole Theorem and wy for Clear Sectors Save Chargets	E Post-Auth Sign-H	n Notification							
Emable redesigned pages for this Sign-in Publicy Emitting Theorem 2018 and any the Clear Decision Interest Interest Environment Environment	🗸 Advanceri Settinga								
Their Housepart poper are used any far Chart tensor allows Save Chartyri	Enable redesigne	ed pages for this Sign-in P	falicy						
Save Changes	Rain History of Logic	pression and the Charl lines	AN INCOME.						
	Save Change	r6.							

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.
- 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

S Pu	Ise Secure System Authent	calion Administrators Users Mai	ntenance Wizards		Puise Connect secu	
User Role	es > Remediation > General > UI Options					
UI Opti	ons					
Gen	trei Web Files	SAM Teinet/SSH	Terminal Services	Virtual Desktops	HTML5 Access	Mee
Overvie	w Restrictions VLAN/Source IP 1	Seealon Options UI Options				
Save	Changes Restore Factory Def	autts				
> Head	ler					
> Sub I	neaders					
> Start	page					
> Book	marks Panel Arrangement					
> Help	Page					
> User	Toolbar					
> Brow	reing toolbar					
> Post	Auth Sign In Notification					
> Pers	onalized greeting					
Y Com	pliance Failure Notification					
	Show Compliance Failure notificatio	n message on user's page				
	Display the following message as a compli if endpoint's compliance check fails, this m	ance failure notification on the user's p assage is displayed on user's page y	age. hile accessing SAML IOP ene	bled resource.		
	You have limited connectivity becau device does not meet compliance pe	se your blicies				
> Other						
Save	Changes Restore Factory Def	aults				

- 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

Cloud Secure > Cloud Secure Configuration > Applica Applications	tions			
Cloud Secure Configuration Cloud Applic	ation Visibility			
Basic Applications Conditional Access				
Basic configuration setting	s are working fine.			
(Last modification was on 2	019-12-09 03:06:42 PM)			
			0	
÷				
Add & configure as	Coffice 365	Google Apps	salesforce	box
in the list.				

- 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.

		20	the Barbard State and
Enhanced Glient or Proxy Pro	Re (ECP) Settings		and a second second
The party of the p	1		
Connect advantage Con regime	Spanning and party from their second of the heatman in the re-	and a second	
Users tiresheld			
Disching line 0	l'ant		
second and M	1 (1998-1		

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

Course	iters.						
Farmed .	monthline	ereta (
Usenane		Appy Filer					
Refimal	Unblock						Veet to
a the	oname 🔻	Disched Since	Maint Macanet Gargesont Group	Beause Court	Unsched 100	Recent ECP Request from	Reator
		Tue Apr 23 10 16 29 2019	Tue Apr 23 10 55 30 2019	1	Tae Apr 23 22 56 29 2519	Android-Mail/8 11.25 224448071 release	Antoid_CloutSecure_Realm
		Tim Apr 21 10 50 25 2019	Yue Apr 23 10 58 29 20 19	1	Tee Apr 22 11 01 25 2010	Andraid Mail 11:25 22440071 release	Animat_CloudSecure_Ilcum
		Tuo Apr 23 10 58 31 2018	Tue Apr 23 10.58:33 2019	+	Tex Apr 23 22 56 31 2919	Anthone Allabilit. 11 25:224448571 release	Andholf_CloodSecure_Realm
	-	Tun Apr 22 10.56.25 2019	Tost Age 23 10 58:28 2019	1	Tax Apr 23:22:56:25:3919	Anthroid-Mail/R.11.25.2244/8571 release	Annue_CloodSecure_Report

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

Metadata Detaile	From Local File	 From Harodic Urb. 	 Numual contiguration
Select Metadata File	firmer Dusse fie		
Create Bookmark	= Na * No		
Force Authentication Behavior	# Reject AuttorRequest	Re-Autoenticate	G Ignore Re-Authentication
New York Street and Street and Street	(C-9)	0.042	
Sporture Agorithm SAME, Customization settings Contomize SAME, attribute Attribute to the over in SAME, attribute had	terrents sen la corfigant de hiere value pais antre t	te letted for ordered the dee	they server
Signature Algorithm	herents par la configurat de hérre volte pais émbre f	in table (her only of Chin Au	liniy servet
Signature Algorithm	terrent an le carifant la terre obs pérs entre t	le india (ten ovigen) die des	they serve
Signature Agentition SAME, Constormizations settings Constormize SAME, attributee Attributes in the vert in SAME, Attribute Seer Access settings Select All Roles (Bale Soler) After access to the subschere exit of the UI ACS_Chardinaree Role	terrents am te configurad do terre value paiss andre n per beograp to believ somstad rotes. © Chardbeurer, Flerned Rote	in Antel Coursen	they server

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:

- 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**.

Define Policy	Policy Name:	alesforce_group
🐥 User Groups	Description : Sa	ilestorce group
Devices		
Posture Assessment		
S Location		
Applications		
Q Action	4	
	Save Changes	Cancel

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.

Define Policy	Select User Groups for which the action can be applied. Click here for defining a new user group.	*
🐥 User Groups	Marketing_Team_Group	
Devices	i Ma Sales_Users_Group	
Posture Assessment		
& Location		
# Applications		
Q Action		
	Save Changes Cancel	

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.

Define Policy	Select device types for which the action can be applied. Click here for defining a new device type.	^
🖧 User Groups	Linux	
	los	
	Android	
Desture Assessment	Mac Mac	
Solution	Vindows	
# Applications		-
Action	4	•
	Save Changes Cancel	

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.

Define Policy	Click here for defining a new possure assessment rule.	*			
A User Groups	Host Checker				
Devices	Host_Check_Mac_with_AV_Process				
Posture Assessment	MDM				
& Location	Android_9_Mobiles				
# Applications	iPhone_Compliant_Devices				
Q Action	4				
	Save Changes Cancel				

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

Define Policy	Select countries for which the action can be applied.	^
A User Groups	Search country	
🖸 Devices	Afghanistan	
Posture Assessment	Albania	
Solution	Algeria	
# Applications	Andorra	
Q Action	Angola	+ T
L	Save Changes Cancel	

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	Масао
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	El Salvador	Iceland	Mauritius
Bonaire	Equatorial Guinea	India	Mayotte
Bosnia and Herzegovina	Fritroa	Indonesia	Mexico
Botswana	Estonia	Iran	Micropesia
Bouvet Island	Ethionia	Iraq	Moldova
Brazil	Europa	Iroland	Monaco
Didzii Pritich Indian Ocean		Isla of Man	Mongolia
Tarriton	(Mahipas)		Montonagro
Prupei Darussalam	(Ividivilias)	Isidei	Montcorrat
Biuliel Dalussalalli Bulgaria		lamaica	Moração
Bulgaria Durdina Fasa	Fiji	Jamaica	
Burkina Faso	Finiand	Japan	Musambique
Burundi	France	Jersey	Myanmar
Cambodia	French Gulana	Jordan	Namibia
Nauru	Qatar	Slovenia	Tunisia
Nepal	Reunion	Solomon Islands	Turkey
Netherlands	Romania	Somalia	Turkmenistan
New Caledonia	Russian Federation	South Africa	Turks and Caicos Islands
New Zealand	Rwanda	South Georgia and the	Tuvalu
Nicaragua	Saint Barthelemey	South Sandwich Islands	Uganda
Niger	Saint Helena	South Sudan	Ukraine
Nigeria	Saint Kitts and Nevis	Spain	United Arab Emirates
Niue	Saint Lucia	Sri Lanka	United Kingdom
Norfolk Island	Saint Martin	Sudan	United States
Northern Mariana Islands	Saint Pierre and	Suriname	United States Minor
Norway	Miquelon	Svalbard and Jan Mayen	Outlying Islands
Oman	Saint Vincent and the	Swaziland	Uruguay
Pakistan	Grenadines	Sweden	Uzbekistan
Palau	Samoa	Switzerland	Vanuatu
Palestinian Territory	San Marino	Syrian Arab Republic	Venezuela
Panama	Sao Tome and Principe	Taiwan	Vietnam
Papua New Guinea	Saudi Arabia	Tajikistan	Virgin Islands
Paraguay	Senegal	Tanzania	Wallis and Futuna
Peru	Serbia	Thailand	Western Sahara
Philippines	Seychelles	Timor-Leste	Yemen
Pitcairn	Sierra Leone	Тодо	Zambia
Poland	Singapore	Tokelau	Zimbabwe
Portugal	Sint Maarten	Tonga	
Puerto Rico	Slovakia	Trinidad and Tobago	

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.

Define Policy	Select applications(s) for which the action can be applied. Click here for defining a new application.
A User Groups	Office 365
Devices	
Bosture Assessment	
S Location	
H Applications	
Action	A b
	Save Changes Cancel

- 10. Select **Action** and choose one of the following actions for the policy:
- Allow (\oslash) This action ensures that the application access is granted.
- Deny (^(N)) This action denies application access to the end user. An error page "Authorization Failed" is presented to the user.
- MFA (L) This action ensures that the application access is granted only after two levels of authentication.

Define Policy	 O is Allow O is Deny 	*
User Groups	C L Additional Authentication	
Posture Assessment		
& Location		
Applications		_
Action	٠	
	Save Changes Cancel	

- 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.

Pulse Seco	URE system Authentication Admir	nistrators Users Maint	ienance Wi	izardis			ulse Conneot Secure
Secure + Ooud Secure Configuration + diffional Access Calad Secure Configuration Calad Secure Configuration Calad Secure Configuration Calados - Secure Configuration Calados - Secure Configuration Calados - Secure Configuration Calados - Secure Configuration + Configuration Configuration - Configuration + Configuration Configuration - Configuration + Configuration + Configuration Configuration - Configuration + Configuration Configuration - Configuration - Configuration + Configuration Configuration - Configuration - Configuration - Configuration - Configuration - Configuration - Configuration Configuration - Configuration - Confi	Conditional Access of Application Walterly						
Pointe Eske Of	anges	Devices	MOM	HC	8 colligations	Lostin	Add N
geo_po(_dubal	domgrp1	Windows		.055	Office 365	United Arab Emirates	La
geo_pol_gemany1			1		Office 365	Germany	l.a
Geo_ppi_tance					Office 365	Frence	Q
geo_Poi_SriLanka	Marketing_Team_Group	Windows			Office 365, Salesforce	Bri Lanka	Q
Geo_pol_nepsi					Office 365	Nepel	6
geo_pol_Australia	domgrp1	Windows			Office 365,Selesforce	Australia, Brazil, Canada	1.
Geo_pol_india1					Office 365	India	6
Geo_poi_china1					Office 365	China	6
Geo_pol_2_maxmindo	e e e e e e e e e e e e e e e e e e e				Office 365	China,India	6
Geo_Pot_1	n				Office 365	India,Nepal	L.
Polt		Windows,Mac			Office 365	India,United Kingdom,United States,Dubal	Q
policy1	domgrp1	Windows			Office 365		(
Detault Policy							Q

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.

V Us	✓ User Group Settings					
	Delete	Add Group				
	8	Users Group name	Details			
		Marketing_Team_Group	CN=marketing_Team,CN=Users,DC=pulsesecurescoress,DC=net			
		Sales_Users_Group	CN=salesteam,CN=Users,DC=guilbenaetumeactereira,DC=net			
> De	vice Versions S	əttings				
> Posture Assessment Settings						
> Ad	iditional Authen	tication Settings				

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**.

٩dic	Selected	
10	records per page Search:	
0	Matching DNs	Тура
D.	CN=WinRMRemoteWMIUsersCN=Users,DC=pumerercurse.coms,DC=net	static
۵	CN-Administrators,CN-Builtin,DC-	static
D)	CN=Users,CN=Builtin,DC=c+meser+max+max,DC=net	static
0	CN=Guests, CN=Builtin, DC=;+Jnenec.umax.cens, DC=net	static
D	CN=Print Operators, CN=Builtin, DC=pumerer uman cens, DC=net	static
0	CN=Backup Operators,CN=Builtin,DC=;metermaxmax,DC=net	static
D.	CN=Replicator,CN=Builtin,DC=putsesecureaccess,DC=net	static
n)	CN=Remote Desktop Users,CN=Builtin,DC=putteres one ceres,DC=net	static
0)(CN=Network Configuration Operators.CN=Builtin,DC=puinemecureaccens,DC=net	static

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.

Y De	✓ Device Versions Settings						
	Delete Save Changes						
	8	Pattern	Display Name	Display Icon			
				Browse	Add		
		Linux	Linux	Δ.			
		ios	IOS	٩			
		Android	Android	0			
		Mac	Mac	`			
		Windows	Windows	(
> Po	> Posture Assessment Settings						
> Ad	ditional	Authentication Settings					

Configuring Posture Assessment Settings

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

> User Gro	> User Group Settings							
> Device V	> Device Versions Settings							
Y Posture /	assessment Settings							
Click Dele	Click Here to configure Windows and Mac desktop policies Delete Save Changes							
~	Posture assessment Name	Check	Details					
		- Select -		Add				
	Android_9_Mobiles	osVersion	9.1					
	iPhone_Compliant_Devices isCompliant 1							
> Addition	Additional Authentication Settings							

Configuring Additional Authentication Server

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

> User Group Settings		
> Device Versions Settings		
> Posture Assessment Settings		
✓ Additional Authentication Settings		
You can specify an additional authentication server for Cloud applications. Please note that user trying to access a cloud application will have to provide additional credentials in case if the realm does not have any additional authentication configured.		
Additional Authentication server AD_Auth_Server		

1 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.





🕖 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.

- 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.

Whote: 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

	Pulse Connect Secure	
S Pulse Secure Nymme Authentication Administrations Divers Wardenwerke Willards	1*	
dans - Court Innun - Settage		
Satury .		
Adapt Owner MontCorr Ownersphere Units Warry Literas Intel Dering Second Ad	the Notice in the Notice	
teres teres		
w James Settings		
ie Ende Daat Secur Dational		
Terestiane to churte 24 Hours .		
Radiose Internet for strates 4 Members		
Sant Changes		
3 Insien Aptrone integer		
3 (hove former former		
> Investa Balana Setterga		
3 Opini a Aggin alman homogu		

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.

· •						Pul	se Connect Secure
e Se Report art	cure	System Authentic	ation Admini	strators Users Maintenance 1	Wizards		11
Grigte U	ter Activities	Detce Summary	Single Device Activiti	er Application Discovery Authent	Cample Cample	enter Dehavioral	Analytica Cloud Second
ort Dov	naued Report CB	V) tab Detroited					
•	Com	Compliant pliance Non-Compliant Non-Compliant Non-Compliant Non-Assessed	* Usernam	e. Paysed Applications	Fale	ed Applications.	Apply Piller
							View 10 *
Device ID	OS Detail(s)	Login Session Time 🔻	Compliance Status	Initial Compliance Check Details	Passed applications	Failed applications	Assigned Roles
9	Mac 10.13	Wed Oct 17 11.47 37 2518	Complant	Host Check time: Wed Oct 17 11:47:25 2018 Host check result: Pass	Salesforce		Mac_CloudSecure_Role
	Mac	Wed Oct 17 11:13:31 2018	Complant.	Host Check time Wed Oct 17 11:13/03 2018 Host check result: Pass	Salesforte		Mar_CloudSecure_Role
	Mac 10.13	Wed Oct 17 11 12:50 2018	Nitl-Assessed			Microsoft	CloudSeture_Remed_Role
99	Mac 10 13	Wed Oct 17 11:10:14 2018	Compliant	Hast Chack time: Wed Oct 17 11 15:05 2018 Hoat chack tenuit: Pass	Microautt		Mar_CloudSames_Rele
	Anstroid 8	Wed Gct 17 10 41 26 2010	Complant	Host Check time: Wed Oct 17 10 41 20 2016	Salesforce		Android_CloudSecure_Role
	Export and simple U wort Dow	Export and Somple Unior Activities Comple Unior Activities Comm Comm Research Device Dipole OS Detail(a) Some OS Detail(a) Some Comm Research Resea	Device Operation Authoritic Image: Device Activities Device Burrney Simple User Activities Device Burrney Simple User Activities Device Burrney Image: Device Burrney Compliance Compliance Compliance Image: Device Burrney Macci Compliance Image: Device Burrney Compliance Image: Device Burrney Macci Dimagee Image: Device Burrney Macci Dimageee	Compliance Compliant Compliant Image: Compliance Compliant Utername Compliance Compliant Utername Compliance Compliant Utername Compliance Compliant Utername Mac: 10: 13 Wed Oct 17 11: 12: 37 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 31 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 33 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Nutr-Assessed Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant Mac: 10: 13 Wed Oct 17 11: 12: 32 Compliant	Secure System Authentification Administrators Users Mandematication Name integration attentification Authentification Authentification Authentification Authentification integration Single Device Activities Authentification Authentification Authentification Authentification integration Device Activities Device Berger COV (160 Device) Compliance Parced Applications integration Compliance Compliance Integration Parced Applications integration Compliance Compliance Integration Parced Applications integration Compliance Compliance Integration Parced Applications integration Macci Oct 17 11.47.37 Compliance Integration Wed Oct 17 11.47.25 2118 Mac Macci Oct 17 11.47.37 Compliance Heat Check tense Wed Oct 17 11.47.25 2118 Mac Wed Oct 17 11.47.37 Compliance Heat Check tense Wed Oct 17 11.13.03 2018 Mac Wed Oct 17 11.12.50 Nint-Assessed Heat Check tense Wed Oct 17 11.13.03 2018 Mac 10.13 Wed Oct 17 11.	OPENCIPE System Authentitication Administrators Users Maniferiance Witards Read If If	Secure System Authonblication Administratore Users Maniferinance Witzards stand st st strate strate <tdt< td=""></tdt<>

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

A									Pulse Conner	tt Secure
S Pulse S	ecure	ysteri Auto	intication	Administrators	Users	Maintenance	Wizards			1~
Reports > Claud Secure Report		_								
Cloud Secure Report										
Reports										
Uner Summary Single	User Activities	Device Summary	Seigle ()	wice Activities	Application Di	covery A	destation	Complance	Behavoral Anslytics	Cour Secan
Cloud Secure Report o	writed Report CW11	on Deireded								
Filter by: Oote Range	Comeilan	Compliant	dant	Usemana	Pass	d Applications		Failed Apple	oations.	Acety Film
Last 24 Hours •	Results	Hernedian Not-Asses	id wed :							Contraction of the local division of the loc

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

A						Pulse 0	onnect Secure
S Pulse S	ecure system Authenti	cation Admin	istrators Us	ers Maintenance) Wizards		1~
Cloud Secure Report	Download Report: CBV Tab Delivitied						
Filter by: Data Ranga Last 20 Days	Compliance Non-Complian Results Remetianed Not Assess		ame	Passed Applications	Faled A	pplications	Apply Filter
		-				W	ew 10
Username Device	OS Detail(s)	Login Semion Time	Compliance Status	Initial Compliance Check Details	Passed applications	Failed applications	Assigned Roles
Calent	android 8.1.0	Tue Oct 15 10:51:04 2018	Compliant	Host Check time: Tue Oct 15 10 51 04 2018 Host check result Pass	Salestone, Microsoft		Android_CloudSecure_Role

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

0	-					a an an		Pulse C	connect Secure
S Puls	se S	ecure syste	m Authenticatio	n Admin	istrators Us	ers Maintenance	Wizards		1~
Cloud Secure Re	port 0	ownload Report CSV [Tab D	61778002						
Filter by: Date Range Last 30 Days		Compliance Results	Compliant Non-Compliant Romediated Not-Accessed	Usem	8718	Passet Applications	Faled /	Applications	Accely Filter
								v	ew 10
Username 🔺	Device ID	OS Detail(b)		Logio Semiloo Iloo	Compliance Status	Initial Compliance Check Details	Passed applications	Failed applications	Assigned Roles
cateat		android 8 1.0		Tue Oct 16 10:51:94 2018	Compliant	Host Check time Tue Oct 16 10:51 04 2018 Host check result Pass	Salestore Microsoft		Android_CloudSecum_Role

Cloud Application Visibility

- Overview
- Configurations
- Cloud Application Visibility Dashboard
- Event Log messages

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.

WNote: 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

PulseSecure ****	n Authentication Advantations Unors England Policy Mainlangeum Weards
en "Bras A Lives + Tonand + Overview	
Average fragment of the second s	
ment April Aprilan	
And Annual Property and and	
Tarte	Tans
lisent/200	Overset control Lawy Inte
	and the second se
	Gene Charges
P Statement	
These settings are not pacified by the train sergical to the use, the party	A PROJECT (MALE AND ALL AND AL
Smaller Dydness	Real and a second s
a 11 Dates	Population (Channel
Gridee Guest Lee: Roosurt Management Hights	
C Studie Sponsonel Guart Line Account Management N	lans
THE R. LOW CO.	
and the state of the	

Figure: PCS User Roles Page

General Web	Fifter SAM	TeineitSSH	Terminal Services	Virtual Desidopa
Ourses Restrictors V.	Allflearni P Seeann I	lytune al Oytune		
Name			Users	
Description				Contraction in the second
			Saw Changes	
A Objinite		27.53		
	the such cover beindlungs to sure a	own our words spectres in	Content of Content And Se cand	
Ethen widings are not quarker	artica			
Fitaee entings are not cavaflast	(Ear)			
Fitnes entings are not quarties U.A.N.Source: IP Session Options tra 15 Octions	(Edd) (Edd)			

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 <u>Pulse Secure support portal</u>.

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

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

Figure: CAV Visibility Options Page

oud Secure > Cloud Applicatio	n Visibility > Options
ptions	
Cloud Secure Configuration	Clased Application Wathility
Options Application Policies	
Poll Interval	5 Becauds: Specify the interval locus frequently the user data shall be sent
Block Message	NotAllowed
	Orly applies to MTTP competition (not MTTPS connections)
Threatprint database.	No file chosen Browse Last uploaded version: 1.0.0 Last imported on: Tuesday July 24, 08:39:38 2018
Thready in state up to	The manufacture and the approximate resident rules (the industries on: Tokanay any 47, 36,35,36 as in
Save Options	

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.



- 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:

Q nul -	Carry					Pulse Policy Secure	
S Puis	Secul	e typtem Authent	ication Administrators	Users Endpoint	Policy Maintenance	Wizerds	1 *
wed Status + Cloud Au	en and Yoldery > App	tration Policies					
pplication Policies							
Cloud Application M	***						
Options Australian	alizet						
+ New Application P	vercy.						
Application Policy	Reiter	Rented Categories	Stocked Applications	Exchangen	Master URL	Exclusive UPPS	
bed.	Steen	 0 Elocated Categories 	C 1 Biblied Apploidung	O - 9 Exclusions	G 1 Booked URIS	3 Excluded URIS and approximate combination	

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

a dese	becone	And the state of t	anniosanois Users Enope	are rowy mana	enance vitzaids	فليقبط والمصب		
lectre + Cloud Applica	don Viribility - Application If	Poticave						
ation Postats	_							
our Application Writight	¥2							
ree Application Parks								
ew Application Polic	sy							
cation Policy	Roles	Bischool Categories	Blocked Applications	Exclusions	Bioched URUS	Exclusive URIS		
Edit Applicatio	on Policy							
* Darme								
tiest								
© Block have	d on categories	© a	ten, loksek these closel applications	. L C	hoose the Roles for which this cl	and application rates result to be		
III Drugs +		 . http://www.sec.com/page/2006/2006/2006/2006/2006/2006/2006/200	p myspeciaes ante	dv263	alable Rules Selected Roles			
II forwary as	d Finance +				(2)/00/21	DISS.		
E Rescalari at	nd Self-Help +			Que	t Sponen	Overs		
C frietares				Ques	4			
E Parad and Re			clusions: Allow these applications even if it	wy fail Goan	t Wang Rastrichat			
U Garding -		Linder	töccked appn					
III Gamer +		100	ini allorin pan da ordinezt per linit. Hegylar estro julei bir uneil		Ant			
To Hanting and	Cracking +				Contraction of the second			
U reath .					- Contraction			
E Hand +		- 1	Ri Marrie					
Till Hegel Covin	et a l	@ a	lock these URIs					
internation (Territorializzy .	-	w expressionts com/c/content					
ill ann ant Ca	uteria a							
Waterman 4		1.00						
		√ E Mark	schusions: Allow these URIs even if they fail ad URIs.	onder				
		too tab	o especialmento consultato ambandeplações provytoperante inforção banqui					
		-1a0	p-myspecies or folloolog					
				-				
			1.0	D Help				

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	None
under blocked applications	
Block these URIs	www.espncricinfo.com/ci/content
Exclusion: Allow these URIs even if they fall under	www.espncricinfo.com/ci/content/player
blocked URIs	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

sé .			
C. Music based on uniquenes C. Annotes + C. A	C Ana, taxa free that again alors	A Course for blass to encoded without the sectors. And the form th	
The second and the second seco			

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

Q Dulce	Secu	ro							Pulse Connect Sec	cure
S ruise	Jecu	C System A	othernticatio	n Administrators Users Mairiù	enance Wizer	de .				1.
Travents + Application Direct	who Report									
Reports										
AN Institution Dynamic	Republic									
Gent Surrows	Single Lines Hold	Decis Summ		ngie Device Actualization (Francisco Document	Advertision	Constant				
		and the Work of the American		The second second				1100	Charles and	Concession in the local division in the loca
CBB* HE	01	and a part of the second state and		and the second second						Chinese and
(aar 200)	ACTOR	ACCESSES DIME	88(7808)	beatau.	CATEGORY	155.8	BEYROD	05	OOVINE.DADED	BPLOADED
Last Water		123628-54 17-0119	Heres	prophe analytica come and an an and an and	+ Dealeymont	FUTWERMENT	sends of the local law	Vienteren	1010	0.00.000
LAM BURD		122818/16/01/2011	arran .	peopleapia.com	+ Disangement	full Williamstate	444444-47145-001-001-001	7 million	8.0146	0.00.000
Stated Applications			-						that Person 12	() - New (1.644)
Address in the street ways										

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

0					Pulse Policy Secure		
Y Puls	Secu	re system Automic	ation Administrators Users En	spornt Policy Maintenance Wizards		1.	
eents + Application Dec	overy Report						
Reports	The Personal						
User Summary	Single Lines Activit	tes Devce Summery	Single Device Activities Onivice Discovery	Application Decovery Ratheretication	Compliance	Behavioral Vinastica	
Deer All	O these	eg 1 to 18 of 1,825 ardines 50 +	ierzidztev zalie				
and Selens	action	ACCESSED TIME . METH	OD 0 DOMEN	CATEBORY	UNR I	DEVICE	
and threads		88 H 2010 10 To 10 TO 10	TO afressee Sufference	+ Adventurg + Rammun	real	alter-PC Internation	
art Month		M 17 25 Alema 19 File 20 1	TP Indecorpreject.com Testion site opport i	en e Carliert Seven	108	ainin PO Internet a	
Insteel Applications	a 🖌	. 86. 97. 80. No. 10. Page 3 (11)	12 stand ge cam all for the design of the	+ Environment	real.	atron #5 0100 1000 114	
Internal Applications		26-19-17 Mar. 10 744-2017	patron and and address of	- Churt and Indian's Messaging	part .	when-PC 1010 104/11/	
in present Privace	= *	Maldelan minateri	yahas.com mail principer	+ Churt and Testant Mesonaphy.	140	almin-PG 1010 10171	
Fromi		HE REAL PROPERTY OF THE OWNER OF T	P2 repeterdancy galors (set representation pa	- Carmel Seven	100	anni-PC III II II III I	
		B. H. M. More, 12 Percent 1	22 ENDA 2009 SECOND STORE STOR	* Tports	100	A810-PC 10.00000000	
14	a 🥐	45.46.52 Mar. 10.746-2010	with the second states	+ facete	rand	atton PC 10.18.10.0171	
	0.0	MARCHINE, ST. PARTIES.	11 aspendences al manifelition	+ fairle	1000	4000-PC 10 10 10 10 10 10	

Figure: Comprehensive Application Discovery Report

1 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.

all Arthri 😤

Screenshots



Cancel sso.pulsesecureaccess.net

Authorization Failure Screen

11:19 AM

1



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 Ondemand 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

Pre Sign-In Notification
This is Pre Sign-In Notification-cbr>You are attempting to login to Pulse Connect Secure appliance. Click on Proceed to agree with Terms & Conditions.

2. Log in to the PCS server using the user name and password and click **Sign-In**. Figure: User Login Page

S Pulse Secure	
Please sign in to begin your Cloud Secure session.	
Username	
Password	
SIGN IN	

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

••• Grand 2	ALC: NOT THE REAL PROPERTY OF	4
		°
Smert Folders On Vy Computer Distance	S Pulse Secure	
(≥ Derts I> Seni ≅ Trani	Please sign in to begin your Clicked Sectors session.	Termine T
10 AV	Person	-
	ROL N	

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)
- Desktops
- Pulse Connect Secure
- Pulse Workspace
- Troubleshooting Tips

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.