Pulse Secure®

Pulse Workspace Appliance Administration Guide

Supporting Pulse Workspace 2.0.1903.1

Product Release	2.0.1903.1
Published	11 December 2019
Document Version	1.0

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

https://www.pulsesecure.net

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.

Pulse Workspace Appliance Administration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Preface

Document Conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure technical documentation.

Text Formatting Conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command output
	Identifies command syntax examples

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

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

- Product warranties—For product warranty information, visit **https://support.pulsesecure.net/product-service-policies/**

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: **https://support.pulsesecure.net**
- Search for known bugs: **https://support.pulsesecure.net**
- Find product documentation: **https://www.pulsesecure.net/techpubs**
- Download the latest versions of software and review release notes: **https://support.pulsesecure.net**

- Open a case online in the CSC Case Management tool: **https://support.pulsesecure.net**
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: **https://support.pulsesecure.net**

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: **https://kb.pulsesecure.net**
- Ask questions and find solutions at the Pulse Community online forum: **https://community.pulsesecure.net**

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at **https://support.pulsesecure.net**.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see **https://support.pulsesecure.net/support/support-contacts/**

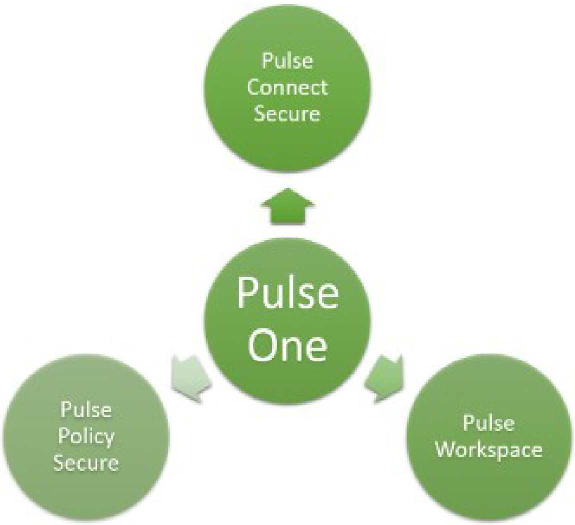
Getting Started

Overview of Pulse One

Pulse One provides unified management of Pulse Connect Secure and Pulse Policy Secure appliances in a single easy-to-use console.

Pulse One, a single, comprehensive management console, offers the administrative end-to-end control and the visibility needed to manage remote, local and mobile access to corporate applications. Administrators use its intuitive, role-based console to monitor system health, manage security policies, troubleshoot issues, monitor appliance and device health, and publish appliance/device configurations.

FIGURE 1 Pulse One Unified Management



It controls enterprise access to datacenter and cloud from a single console.

- **Role-based access** – Grants console access and privileges based on IT role and credentials.
- **Group-based management** – Publish software updates, policy changes and configuration provisioning using custom-defined groups.
- **Centralized administration** – Collectively administers multiple appliances without logging into them on a box-by-box basis.
- **Built-in Mobility Management** – Provides basic EMM functionality for iOS and Android devices and management of BYOD Workspaces.

- **System Dashboard** – Assesses the collective health of all appliances and provides security alerts and appliance alarms.
- **Appliance Dashboard** – Provides appliance status with analytics for connectivity, capacity, utilization, and uptime.
- **Administrator Audit Logging** – Tracks administrator changes to appliance configuration.
- **Monitor and Reporting** – Monitors system activity and provides historical reporting.
- **SaaS Deployment** – Introduces new features and scales without datacenter logistics and planning.

Logging Into Pulse One

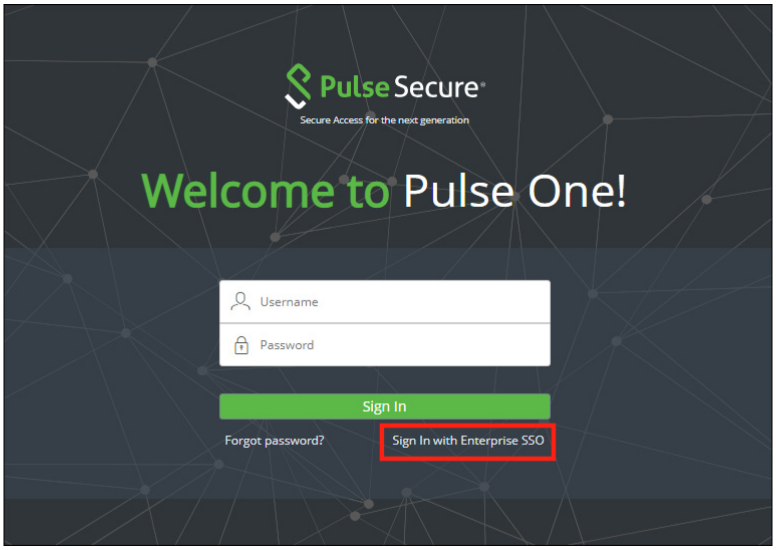
This section details the steps to log in to Pulse One administration.

Use the Pulse One admin URL to launch the Pulse Secure Pulse One console.

If you are an existing user, enter the user name and password. Click **Sign In** to log in to Pulse One.

If Enterprise SSO is configured for your user ID, then click **Sign In with Enterprise SSO**. For details about the Enterprise SSO configuration, see **"Enterprise Connections" on page 181**.

FIGURE 2 Pulse One Login Page



If you are a new user, you would have received a Welcome Mail from Pulse One to your registered mail address. Click the **Set your password** link in the Welcome Mail. In the Pulse One login page that appears, provide a strong password and confirm the password. On successful login, the End User License Agreement (EULA) page appears.

If you have forgotten your Pulse One password, click the **Forgot password** link. In the page that appears, enter your user id and click **Request reset**.

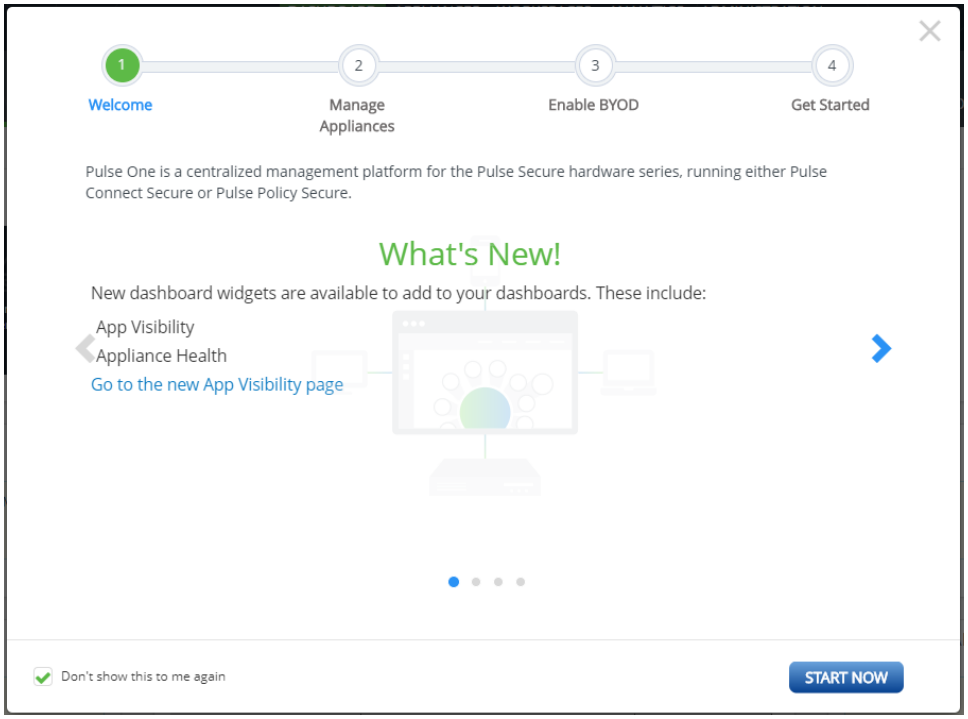
An email that contains **Reset your password** link will be sent to your registered mail id. Use this link to launch Pulse One and provide your new password and confirm the new password.

Note: The **Reset your password** link that you received in the email has an expiration time of 1 hour. Beyond this time, you should make a new request for reset.

If you are a new user logging into Pulse One for the first time, then in the EULA page use the scroll bar to read through the terms of the agreement and then click **Agree**.

The Welcome wizard page appears.

FIGURE 3 Welcome Wizard



Pulse One is a centralized management platform for the Pulse Secure hardware series, running either Pulse Connect Secure or Pulse Policy Secure.

What's New!

New dashboard widgets are available to add to your dashboards. These include:

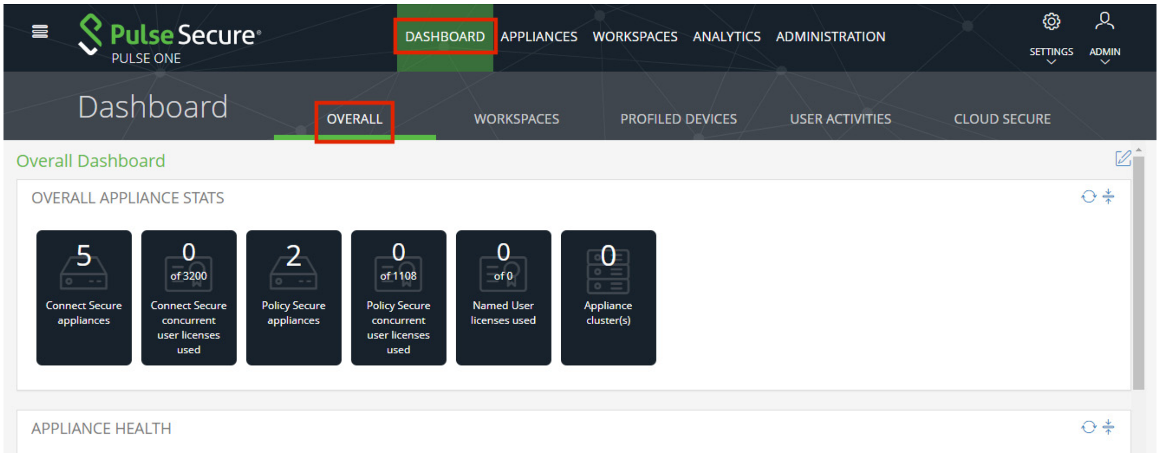
App Visibility
Appliance Health
Go to the new App Visibility page

☑ Don't show this to me again

The Welcome wizard provides you a brief overview of Pulse One. Click the right-arrow button until the **Get Started** option appears. Optionally, select the **Don't show this to me again** check box and then click **Start Now**.

Note: You can view the Welcome wizard any time by clicking the settings icon on the top right corner of the page and selecting **Show Welcome Wizard**.

FIGURE 4 Pulse One Home Page



Select the appropriate tab, settings icon or user icon, and get started with the administration.

Adding a Pulse Workspace License

To activate the **Workspace** menu and Pulse Workspace functionality, you must install a Pulse Workspace license. This license enables the **Workspace** menu and workspace functionality.

Pulse Workspace licenses for OnPrem/Appliance (either hardware or software) have the following format:

```
PWS-nnnnU-xxxxxxxx-xxxxxxxx
```

For example, *PWS-10U-a1b2c3d4-e5f6g7h8.*

Pulse Workspace licenses for SaaS/Cloud have the following format:

```
PWS-nnnnU-nnY
```

To view and install licenses, access the Command-Line Interface (CLI) and use the following commands:

```
licenses show
licenses add <license key>
```

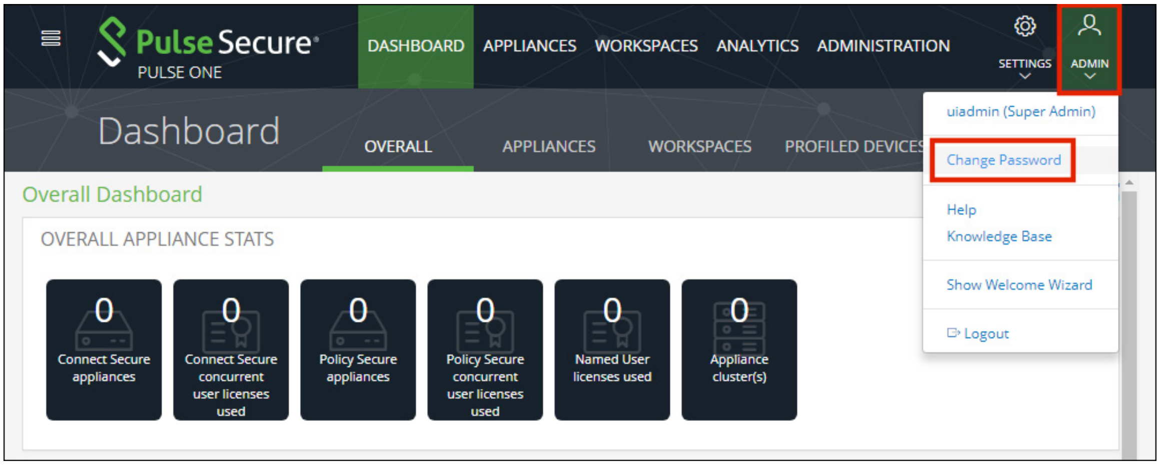
Refer to the *Pulse One Command Reference* for full details of CLI commands.

Changing the Password

To change the password:

1. Click the **user** icon on the top-right corner of the page.
2. From the pull-down menu, click **Change Password** to change your login password.

FIGURE 5 Change Password



An email that contains **Set new password** link will be sent to your registered mail id. Use this link to launch Pulse One and provide your new password.

Note: The **Set new password** link that you received in the email has an expiration time of 1 hour. Beyond this time, you will have to make a new request for setting the new password.

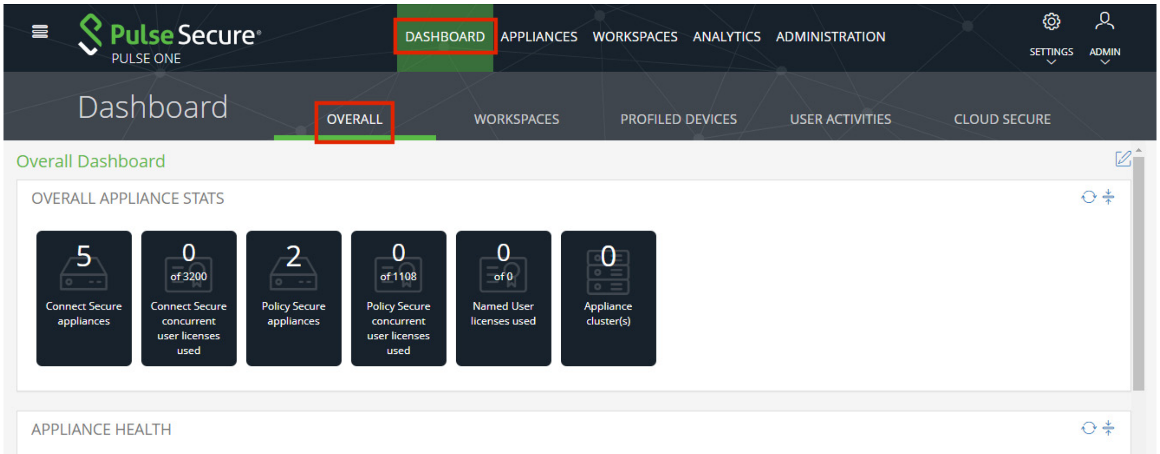
3. To log out of the admin console, click **Logout**.

Viewing Pulse One Dashboards

Viewing Overall System Health

To view metrics for system health, select the **Dashboard** tab, and then select the **Overall** tab. For example:

FIGURE 6 Overall Dashboard



This dashboard includes the following widgets by default:

- Overall appliance statistics.
- Appliance health for individual appliances.
- VPN realm usage.
- Role usage.
- Frequent user logins.
- Logins in the past 24 hours.
- Critical appliance events with timestamps.
- Resource dial.
- Pulse Connect Secure versions.
- Pulse Policy Secure versions.

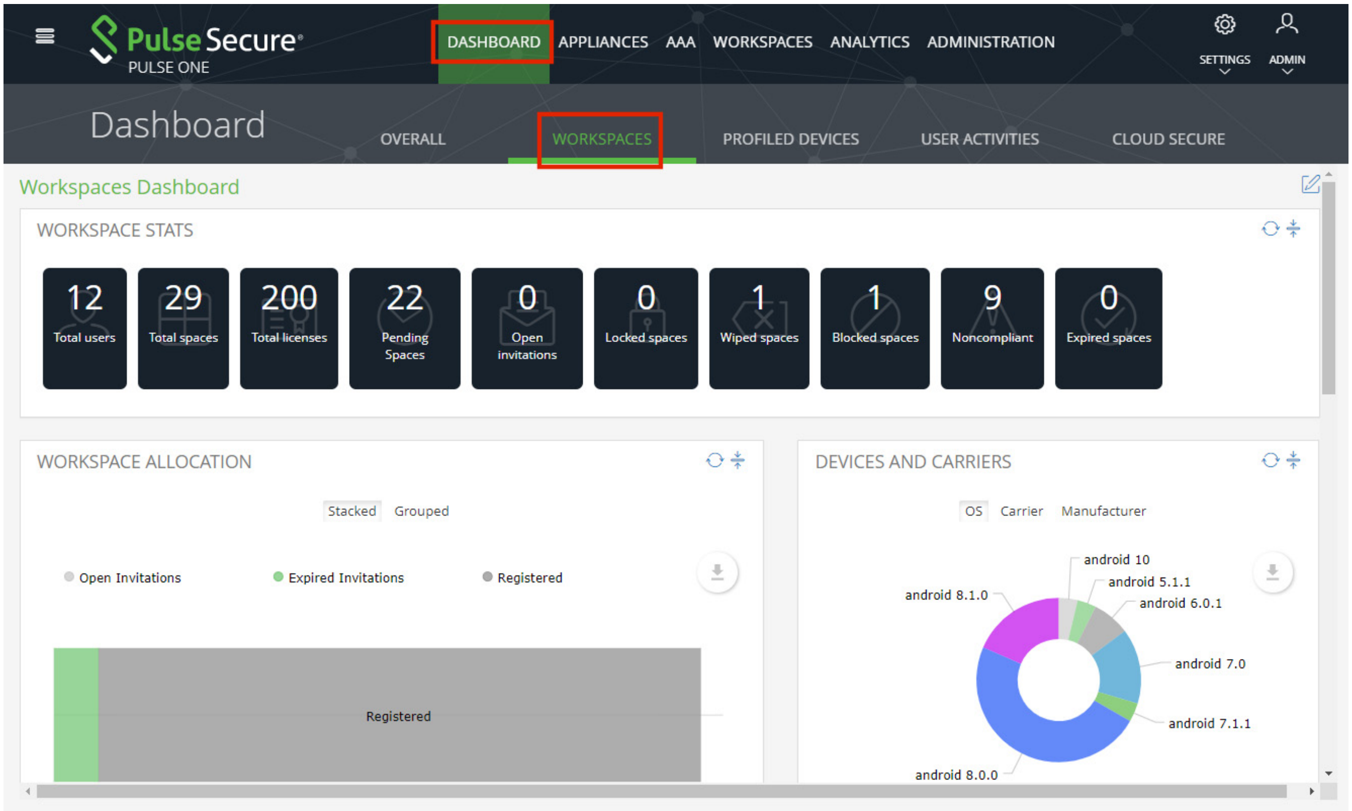
Each widget that can be refreshed by clicking **Reload Widget Content** (⟳) and collapsed by clicking **Collapse/ Expand Widget** (⇅).

Viewing Workspace Metrics

To view metrics for workspaces, select the **Dashboard** tab, and then select the **Workspaces** tab.

Note: The **Workspace** tab is only enabled when a Pulse Workspace license has been installed.

FIGURE 7 Workspaces Dashboard



Each widget that can be refreshed using the **Reload Widget Content** (⟳) and collapsed using the **Collapse/ Expand Widget** (⇕).

The administrator can view the following information:

- Workspace statistics, including:
  - The total number of users.
  - The total number of (work)spaces.
  - The total number of licenses.
  - The number of open device invitations.
  - The total number of locked/wiped/blocked (work)spaces.
  - The total number of non-compliant devices.
  - The total number of expired (work)spaces.

- Workspace allocation, in terms of:
    - Open invitations.
    - Expired invitations.
    - Registered workspaces.

  These can be displayed as **Grouped** or **Stacked** bar chart data.
- Devices and carriers, in terms of:
    - Operating system on the device. For example: Android 7.1.1, iOS 11.2.5, iOS 12.0, and so on.
    - Carrier for the device. For example: Sprint, AT&T, T-Mobile, and so on.
    - Manufacturer of the device. For example: Apple, Samsung, Huawei, and so on.
- Device owner, in terms of:
    - Android corporate.
    - Android corporate owned single use (COSU).
    - Android BYO.
    - Apple corporate.
    - Apple BYO.

  Note: These can be displayed as **Grouped** or **Stacked** bar chart data.
- Coverage by policy, in terms of individual current/pending policies.
- Workspace Connectivity.

System Management

Working with LDAP Groups

Enterprises typically assign policies based on the LDAP group. For example, staff in Sales need access to a specific set of Enterprise apps, while staff in Finance need a different set of Enterprise apps.

You can configure LDAP groups and assign these groups to policies. These policies are then sent to Workspaces when users configure Workspaces on their mobile devices.

If users are in multiple LDAP groups, then they get multiple policies. The order of policies applied to Workspaces depends on the order of polices configured on Workspace Server.

- "Adding an LDAP Group" on page 15.
- "Removing an LDAP Group" on page 17.
- "Configuring an LDAP Group" on page 17.

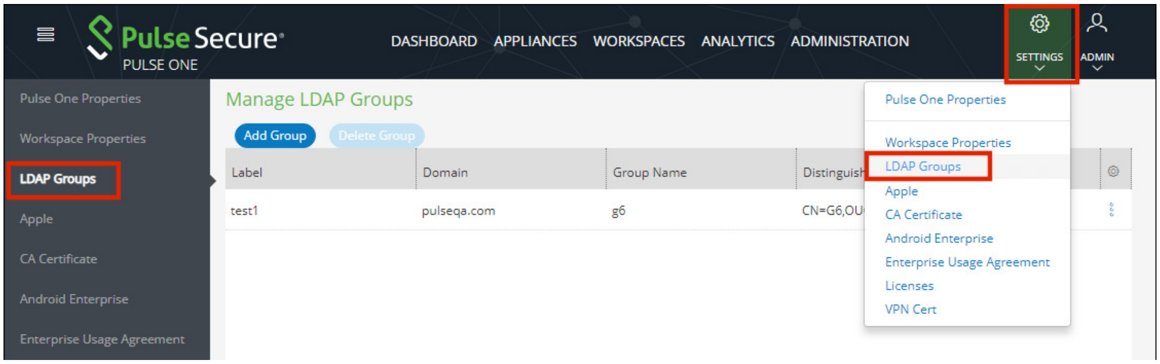
Adding an LDAP Group

To add an LDAP group:

1. On the Pulse One console, select **Settings > Workspace Settings > LDAP Groups**.

   The **Manage LDAP Groups** page appears.

FIGURE 8 Adding an LDAP Group



Label	Domain	Group Name	Distinguish
test1	pulseqa.com	g6	CN=G6,OU

2. Click **Add Group**.

   The **Add LDAP Group** dialog appears.

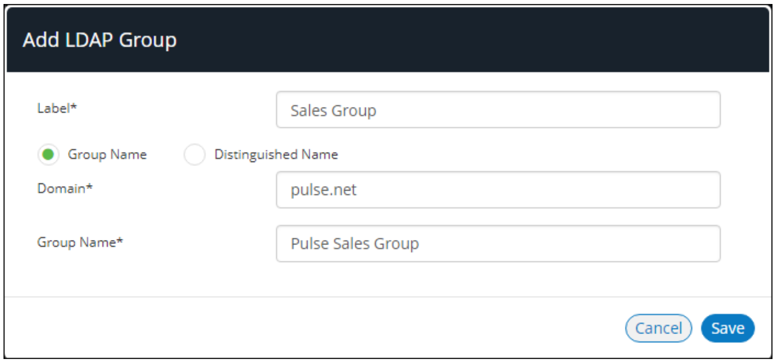
3. Enter a **Label** for the group.

4. Select either **Group Name** or **Distinguished Name** format. The dialog updates.

5. (Optional) If you selected **Group Name**:

   - Enter the **Domain** name to which the group belongs.
   - Specify a **Group Name**.
   - Click **Save** to add the group.

FIGURE 9 Add an LDAP Group using a Group Name



Add LDAP Group

Label* Sales Group

● Group Name ○ Distinguished Name

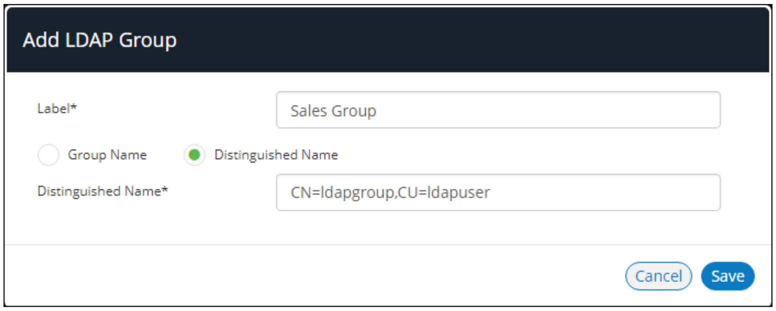
Domain* pulse.net

Group Name* Pulse Sales Group

6. (Optional) If you selected **Distinguished Name**:

   - Enter a **Distinguished Name** in the *CN=Name,OU=organizationname,DC=domain,DC=com* format.
   - Click **Save** to add the group.

FIGURE 10 Provide LDAP Group details – using Distinguished Name



Add LDAP Group

Label* Sales Group

○ Group Name ● Distinguished Name

Distinguished Name* CN=ldapgroup,CU=ldapuser

When an LDAP Group is added, it is unverified.

A notification is then sent to PCS, which will validate the group name against the LDAP server and will send one of the following validation status:

- *Verified* - Group name is available and validated.

  Note: Admin can only assign verified LDAP groups to policies.

- *Invalid* - Group name is not available.
- *Pending* - LDAP provider is not configured.
- *Expired* – Group name is deleted from the back-end LDAP server.

Removing an LDAP Group

To remove an LDAP group:

1. To remove an LDAP Group, click the **More** icon next to the state of the group that you want to remove, and select **Delete Group** from the options.
2. In the dialog displayed, click **Yes** to remove the group.

Note: When the LDAP Group is deleted, it is removed from all the policies to which it is attached.

Configuring an LDAP Group

To configure an LDAP group:

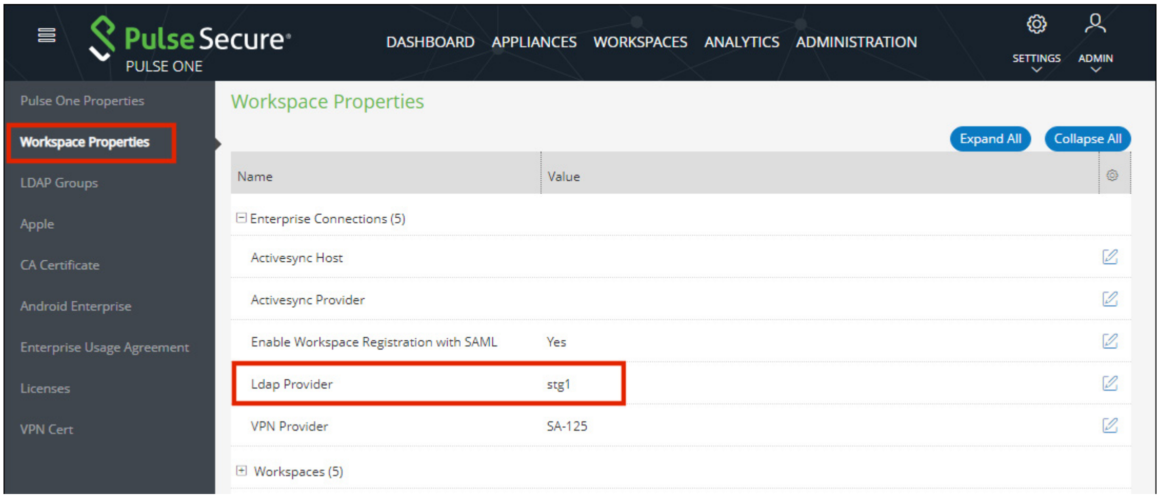
1. Click the **Settings** icon on top-right-corner of the page.
2. Select **Workspace Properties**.

   The **Workspace Properties** page appears.

3. Expand **Enterprise Connections.**

4. Click the **Edit** icon corresponding to **LDAP Provider**.

FIGURE 11 Edit the LDAP Provider



Workspace Properties

Name	Value
⊟ Enterprise Connections (5)	
Activesync Host	
Activesync Provider	
Enable Workspace Registration with SAML	Yes
Ldap Provider	stg1
VPN Provider	SA-125
⊞ Workspaces (5)	

The **Edit Property** dialog appears.

5. Select the required **LDAP Provider** from the drop-down list and click **Save**.

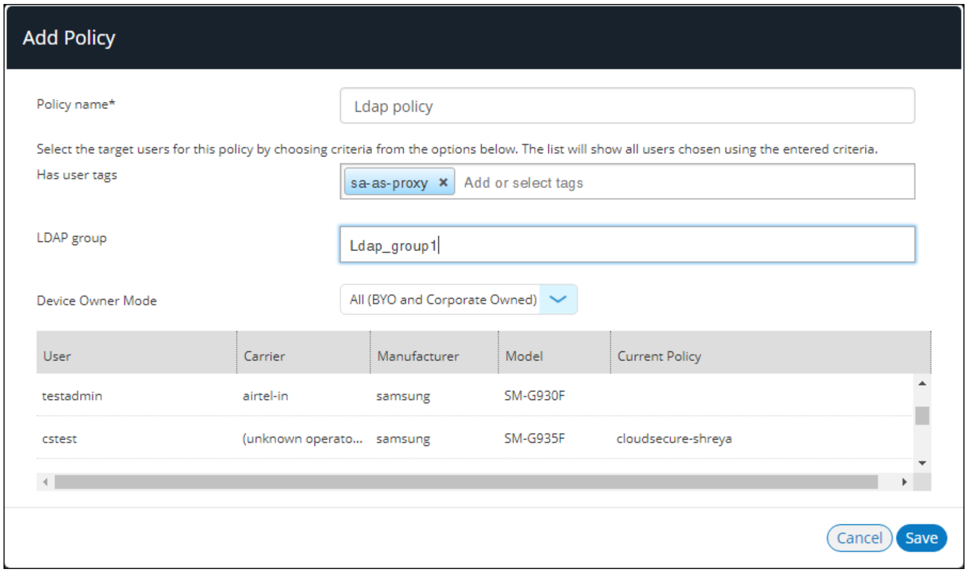
6. Select the **Workspaces** menu, and then the **Policies** tab.

7. Under **Workspace Policies**, click **Add**.

   The **Add Policy** dialog appears.

8. Specify a **Policy Name**, one or more user tags, and choose a verified **LDAP group**.

FIGURE 12 Map Policy



Add Policy

Policy name* Ldap policy

Select the target users for this policy by choosing criteria from the options below. The list will show all users chosen using the entered criteria.

Has user tags sa-as-proxy × Add or select tags

LDAP group Ldap_group1

Device Owner Mode All (BYO and Corporate Owned)

User	Carrier	Manufacturer	Model	Current Policy
testadmin	airtel-in	samsung	SM-G930F	
cstest	(unknown operato...	samsung	SM-G935F	cloudsecure-shreya

9. Click **Save**.

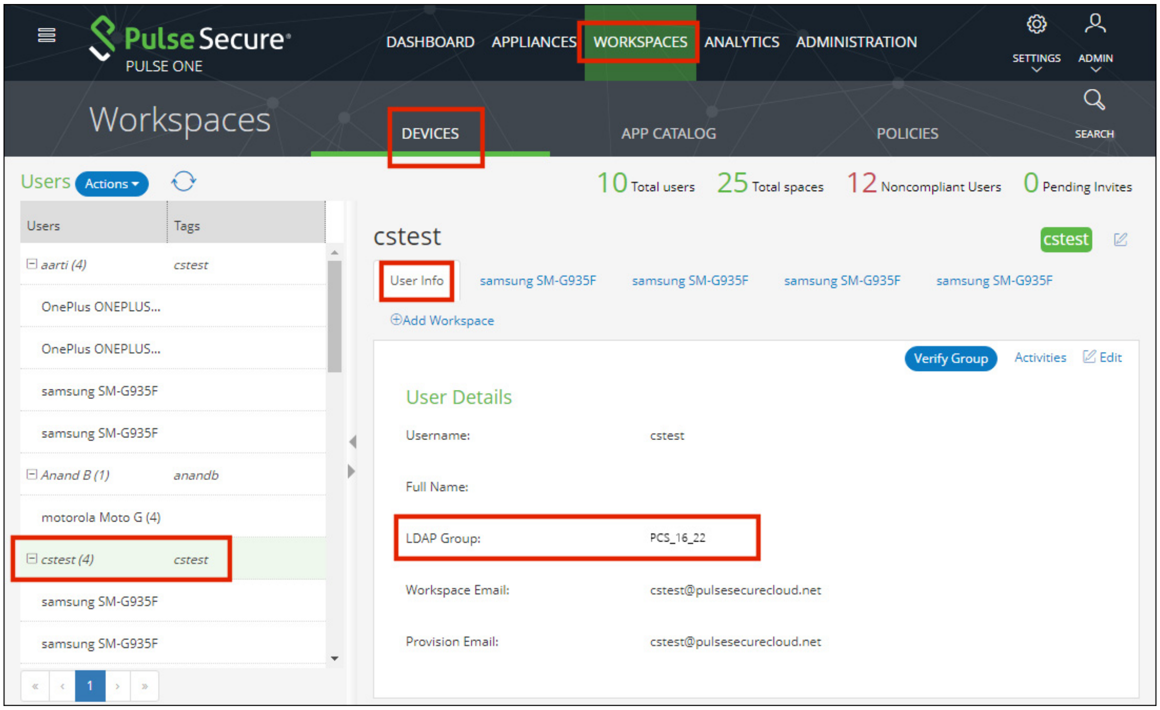
10. Select the **Workspaces** menu, and then the **Devices** tab.

    A list of workspace **Users** is displayed.

11. Select a user.

    The **User Info** tab shows the LDAP Group to which the user is attached.

FIGURE 13 LDAP Group in User Details



Users	Tags
⊟ aarti (4)	cstest
OnePlus ONEPLUS...	
OnePlus ONEPLUS...	
samsung SM-G935F	
samsung SM-G935F	
⊟ Anand B (1)	anandb
motorola Moto G (4)	
⊟ cstest (4)	cstest
samsung SM-G935F	
samsung SM-G935F	

cstest

User Details

Username: cstest

Full Name:

LDAP Group: PCS_16_22

Workspace Email: cstest@pulsesecurecloud.net

Provision Email: cstest@pulsesecurecloud.net

Adding an Apple MDM Certificate

This section details the steps to add an Apple MDM push certificate to your Workspace management console. An Apple MDM push certificate allows your Workspace management console to push policies, updates and actions to your managed iOS devices.

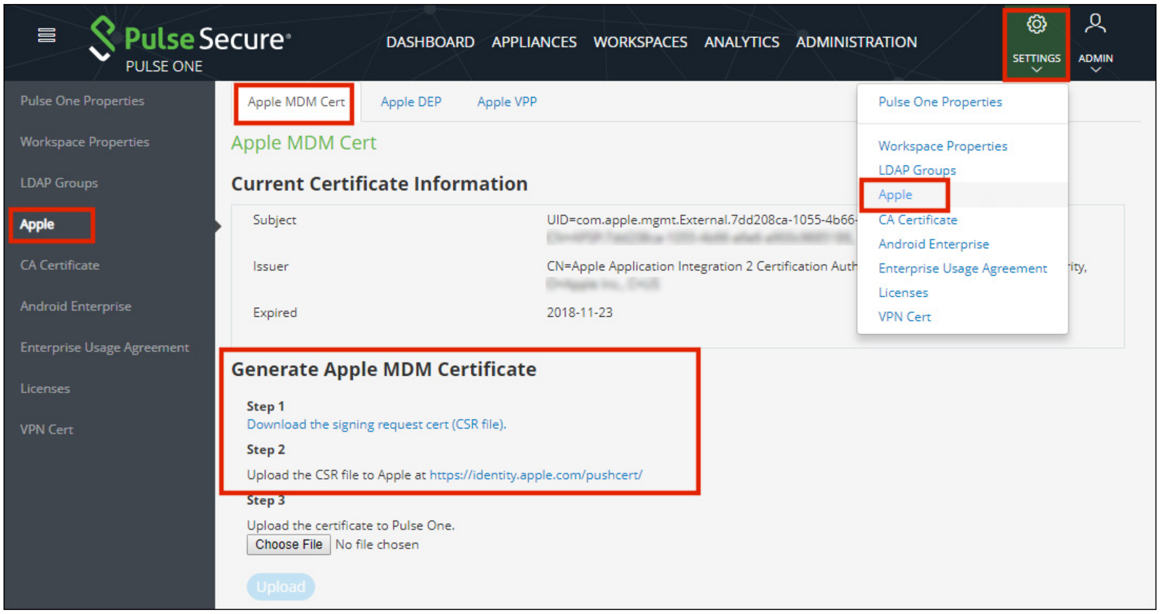
Note: An Apple MDM certificate is required to provision and manage iOS devices. This certificate, downloaded from Apple, is valid for one year and requires renewal. If the certificate expires, the enrolled iOS devices will appear offline and must be re-provisioned.

To add an iOS MDM certificate:

1. Click the **Settings** icon on top-right-corner of the page and select **Apple**.
2. Select the **Apple MDM Cert** tab.

The **Apple MDM Cert** management page appears.

FIGURE 14 Apple MDM Cert page



Apple MDM Cert

Current Certificate Information

Subject	UID=com.apple.mgmt.External.7dd208ca-1055-4b66- [redacted]
Issuer	CN=Apple Application Integration 2 Certification Auth ity, [redacted]
Expired	2018-11-23

Generate Apple MDM Certificate

Step 1
Download the signing request cert (CSR file).

Step 2
Upload the CSR file to Apple at https://identity.apple.com/pushcert/

Step 3
Upload the certificate to Pulse One.
Choose File No file chosen

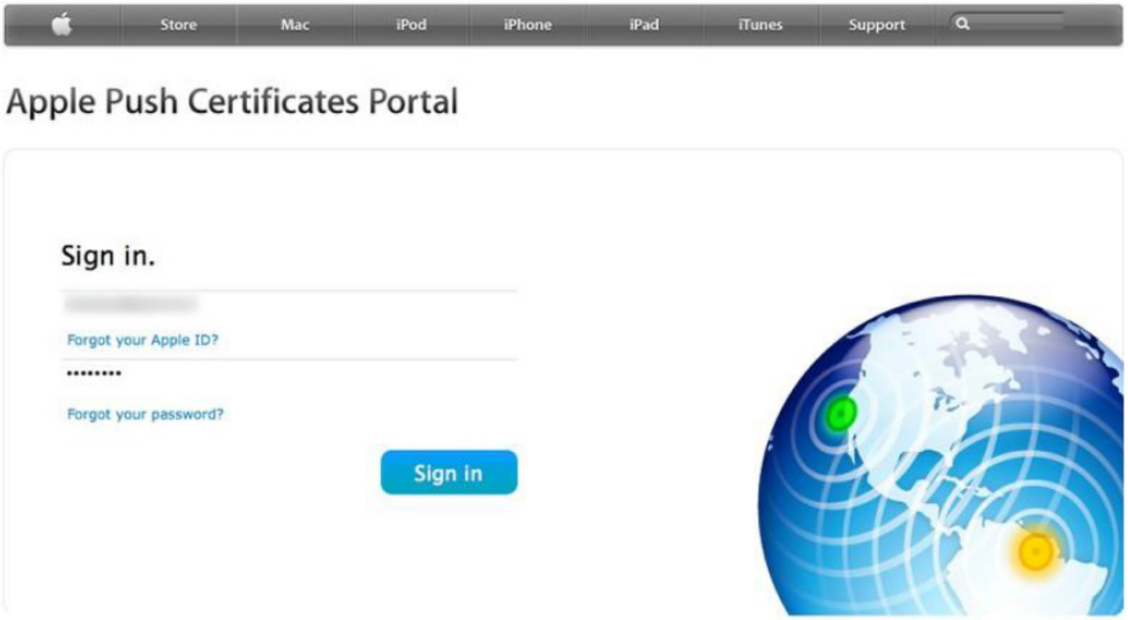
Upload

3. Click the **Download the signing request cert (CSR file)** link to download the MDM push certificate's CSR (Certificate Signing Request) file to your computer.

4. Click the **Upload the CSR file to Apple** link to go to the *Apple Push Certificates Portal* web site.

5. Sign in to the Apple Push Certificates Portal using your organization’s Apple ID.

FIGURE 15 Log in to the Apple Push Certificates Portal



Apple Push Certificates Portal

Sign in.

[redacted]

Forgot your Apple ID?

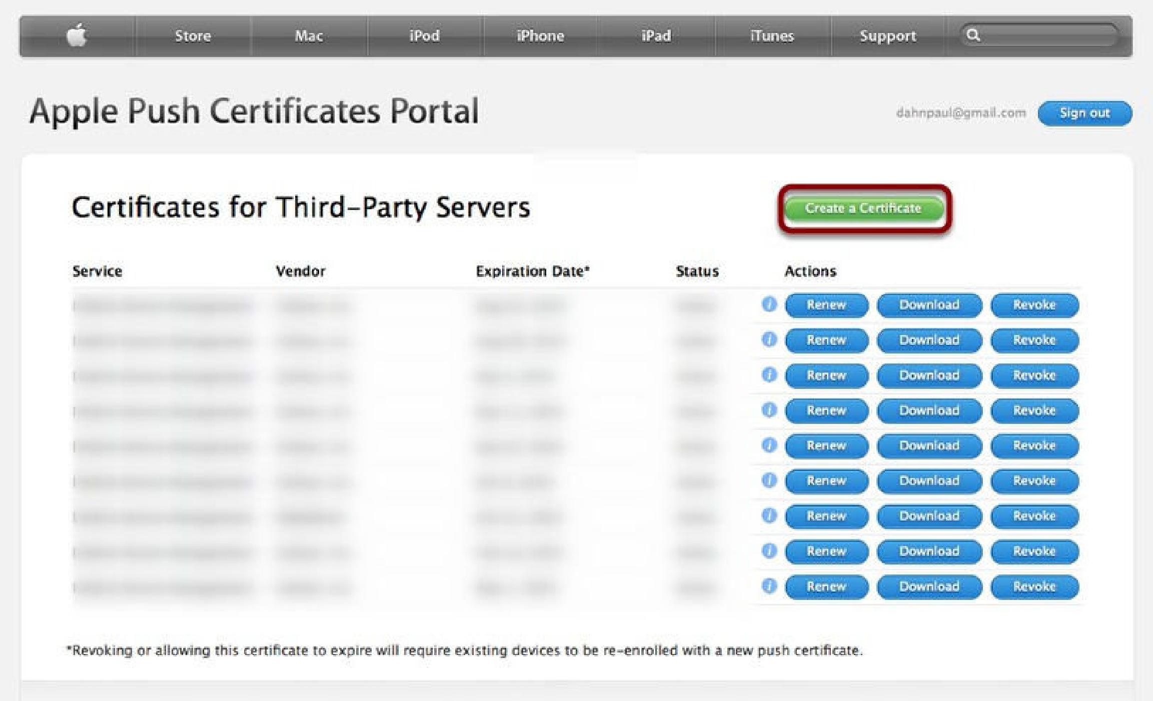
••••••••

Forgot your password?

Sign in

6. Click **Create a Certificate** to create a new MDM push certificate.

FIGURE 16 Create a New Certificate



Apple Push Certificates Portal

dahnpaul@gmail.com Sign out

Certificates for Third-Party Servers

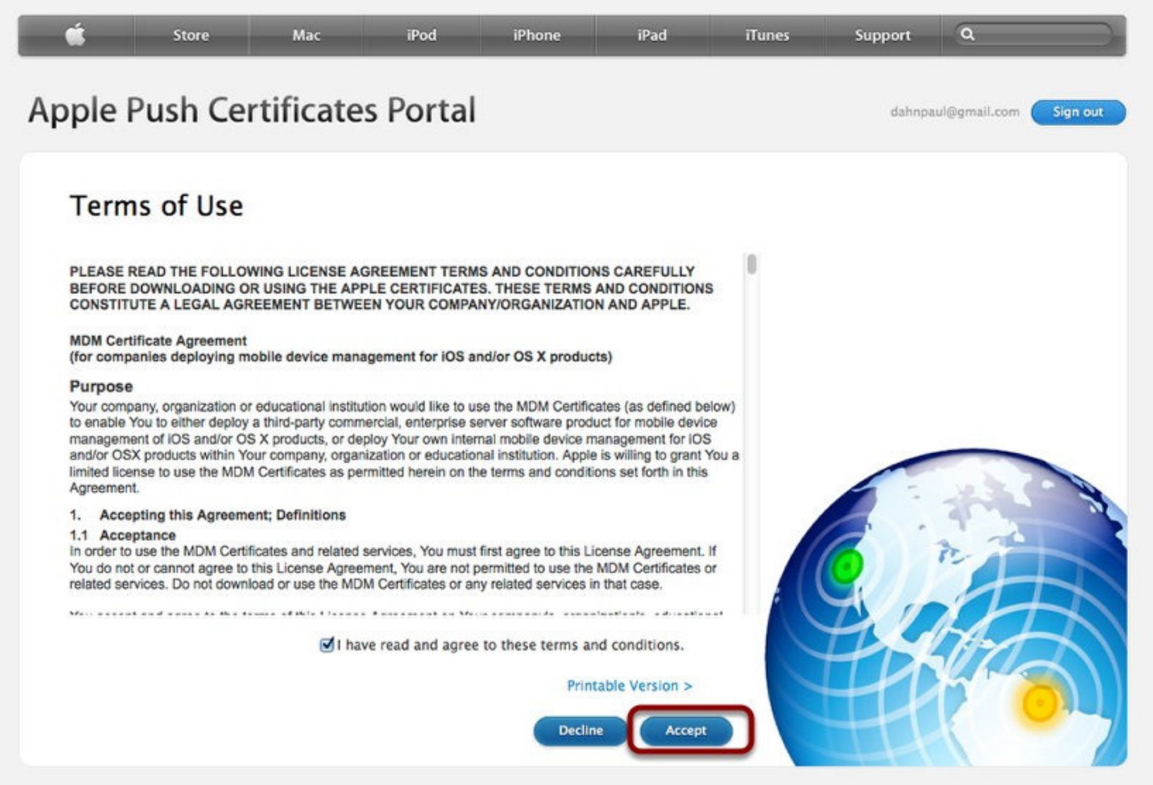
Create a Certificate

Service	Vendor	Expiration Date*	Status	Actions
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke
[redacted]	[redacted]	[redacted]	[redacted]	ⓘ Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

7. Review and accept the terms of use.

FIGURE 17 Accept Terms of Use



Apple Push Certificates Portal

dahnpaul@gmail.com Sign out

Terms of Use

PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.

MDM Certificate Agreement
(for companies deploying mobile device management for iOS and/or OS X products)

Purpose

Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile device management for iOS and/or OSX products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.

1. Accepting this Agreement; Definitions

1.1 Acceptance

In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational

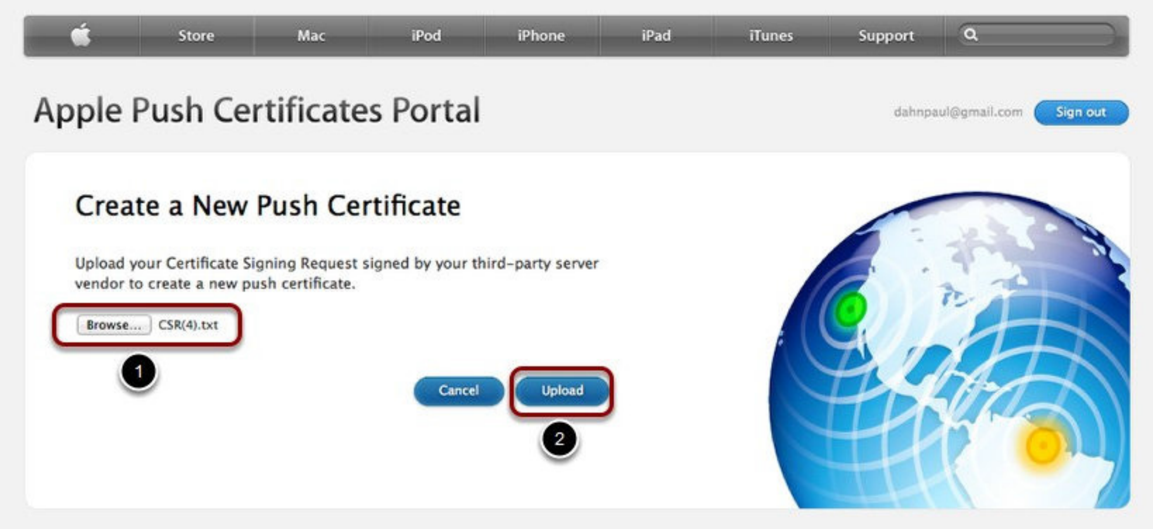
☑ I have read and agree to these terms and conditions.

Printable Version >

Decline Accept

8. Click **Browse** and then select the CSR file downloaded from your Pulse One console, and click **Upload**.

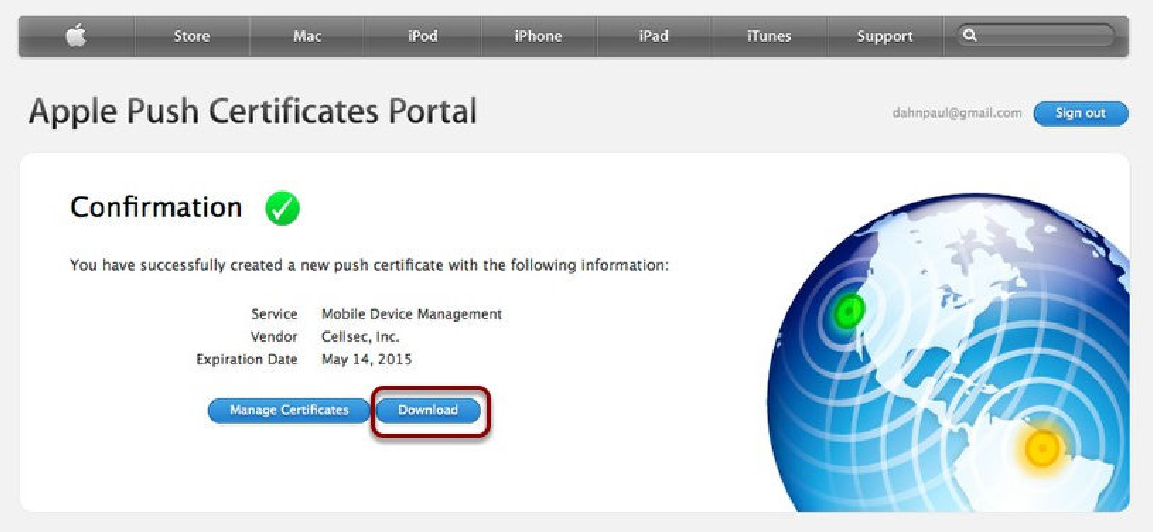
FIGURE 18 Upload Certificate Signing Request



Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

9. Click **Download** to download the MDM push certificate's PEM file. Save the file to your computer.

FIGURE 19 Download Signed Certificate

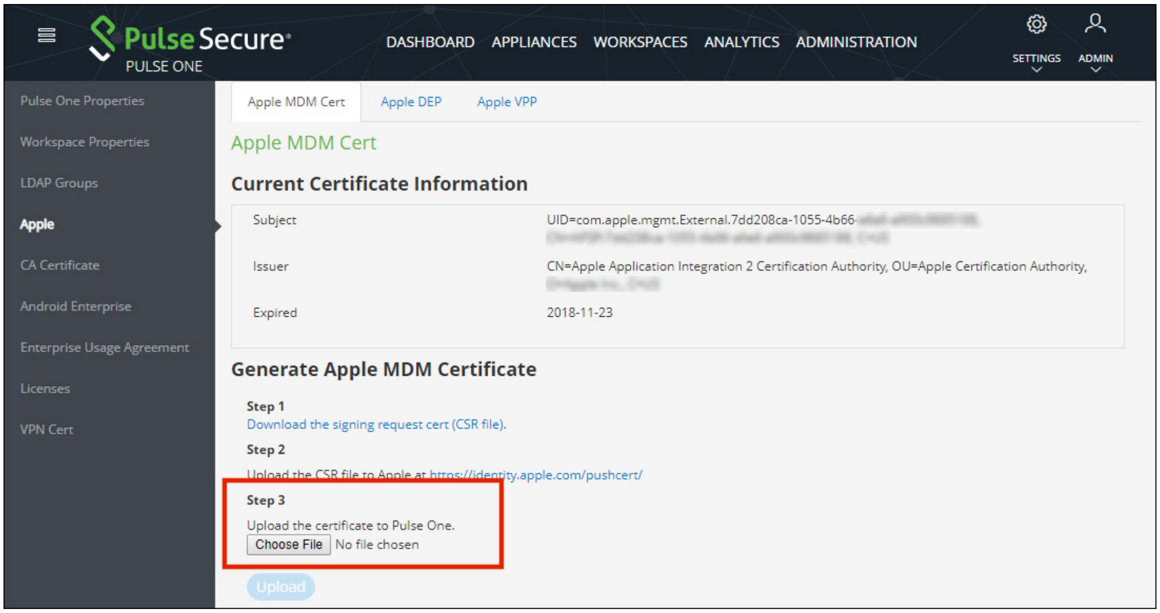


You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Cellsec, Inc.
Expiration Date	May 14, 2015

10. Return to the **Apple MDM Cert** page in your Pulse One console.

FIGURE 20 Upload Signed Certificate



Apple MDM Cert

Current Certificate Information

Subject	UID=com.apple.mgmt.External.7dd208ca-1055-4b66-[redacted]
Issuer	CN=Apple Application Integration 2 Certification Authority, OU=Apple Certification Authority, [redacted]
Expired	2018-11-23

Generate Apple MDM Certificate

Step 1
Download the signing request cert (CSR file).

Step 2
Upload the CSR file to Apple at https://identity.apple.com/pushcert/

Step 3
Upload the certificate to Pulse One.
Choose File No file chosen

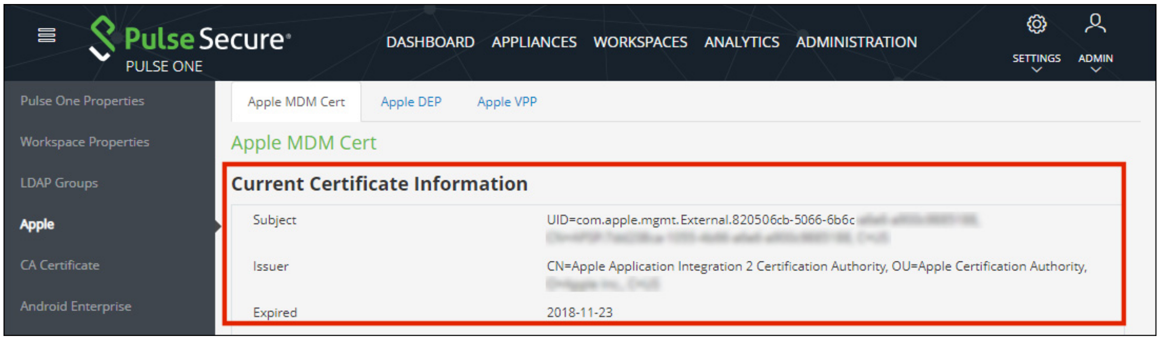
Upload

11. Click **Browse** and select the PEM file you downloaded from the Apple Push Certificates Portal.

12. Click **Upload**.

13. You can now review the MDM push certificate information in your Pulse One console.

FIGURE 21 Review Certificate



Apple MDM Cert

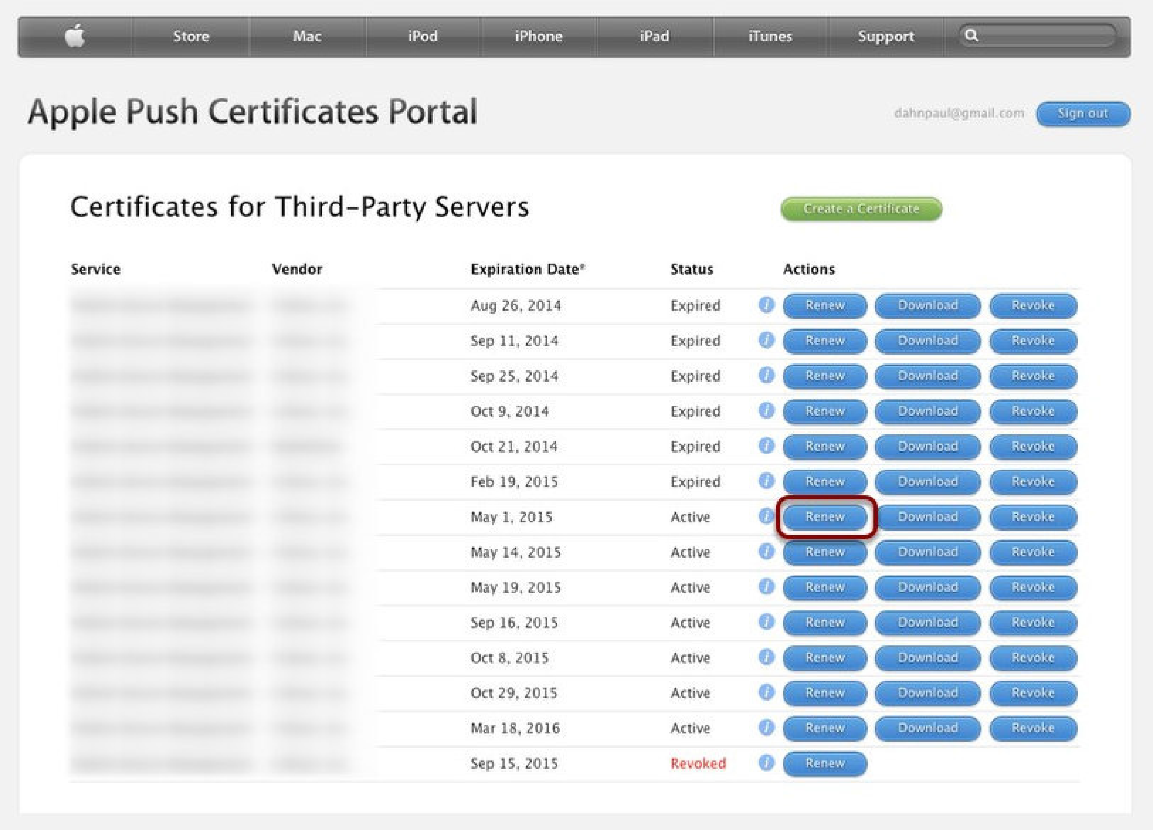
Current Certificate Information

Subject	UID=com.apple.mgmt.External.820506cb-5066-6b6c[redacted]
Issuer	CN=Apple Application Integration 2 Certification Authority, OU=Apple Certification Authority, [redacted]
Expired	2018-11-23

To renew a certificate:

1. Log into the Apple Push Certificates Portal.
2. Click **Renew**. For example:

FIGURE 22 Renew Certificate



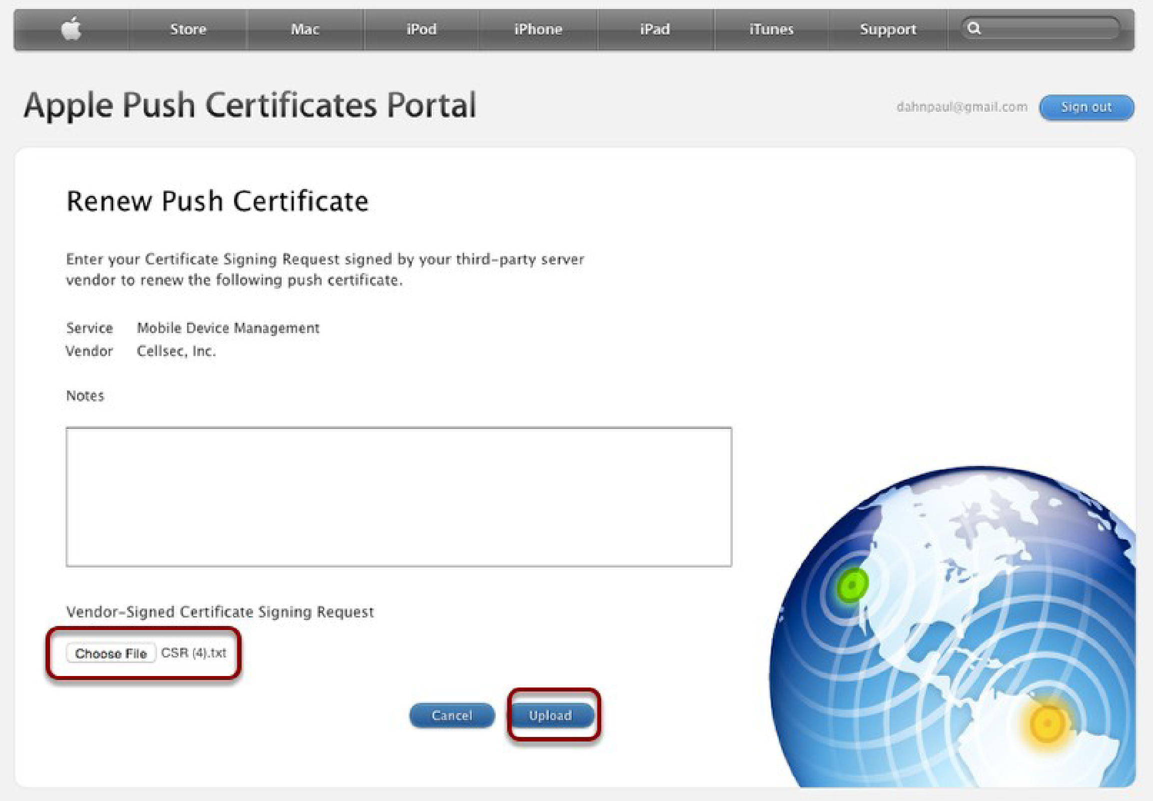
Apple Push Certificates Portal

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
[redacted]	[redacted]	Aug 26, 2014	Expired	Renew Download Revoke
[redacted]	[redacted]	Sep 11, 2014	Expired	Renew Download Revoke
[redacted]	[redacted]	Sep 25, 2014	Expired	Renew Download Revoke
[redacted]	[redacted]	Oct 9, 2014	Expired	Renew Download Revoke
[redacted]	[redacted]	Oct 21, 2014	Expired	Renew Download Revoke
[redacted]	[redacted]	Feb 19, 2015	Expired	Renew Download Revoke
[redacted]	[redacted]	May 1, 2015	Active	Renew Download Revoke
[redacted]	[redacted]	May 14, 2015	Active	Renew Download Revoke
[redacted]	[redacted]	May 19, 2015	Active	Renew Download Revoke
[redacted]	[redacted]	Sep 16, 2015	Active	Renew Download Revoke
[redacted]	[redacted]	Oct 8, 2015	Active	Renew Download Revoke
[redacted]	[redacted]	Oct 29, 2015	Active	Renew Download Revoke
[redacted]	[redacted]	Mar 18, 2016	Active	Renew Download Revoke
[redacted]	[redacted]	Sep 15, 2015	Revoked	Renew

The **Renew Push Certificate** page appears. For example:

FIGURE 23 Renew Push Certificate



Apple Push Certificates Portal

Renew Push Certificate

Enter your Certificate Signing Request signed by your third-party server vendor to renew the following push certificate.

Service Mobile Device Management
Vendor Cellsec, Inc.

Notes

Vendor-Signed Certificate Signing Request

CSR (4).txt

3. (Optional) Add **Notes**.
4. Click **Choose File** to select the CSR file.
5. Click **Upload** to renew the push certificate.

Adding a CA Certificate

For IOS 10.x devices and later, the custom certificates are not trusted by IOS device by default. When the iOS device tries to connect to the Pulse Connect Secure appliance whose device certificate was signed by the root CA certificate that is not in iOS device Trust Store, the device refuses the SSL handshake with the Pulse Connect Secure appliance.

The solution is to push the CA certificate with the MDM payload.

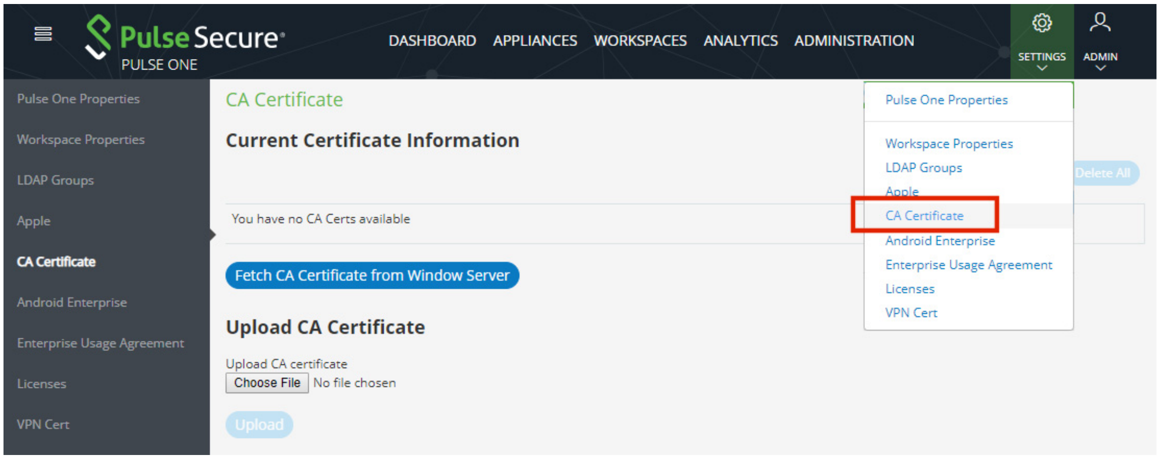
The **CA Certificate** page provides the following options to the Pulse One administrator:

- Upload a certificate or certificate chain.
- Update a certificate or certificate chain.
- Update a certificate or certificate chain after expiry.
- Fetch a CA certificate from a Windows server.
- Delete a certificate or certificate chain.
- Delete all certificates.

To upload a CA certificate from Pulse Workspace Console, do the following:

1. Click the **Settings** icon on top-right-corner of the page.
2. Select **CA Certificate** to go to the **CA Certificate** page.

FIGURE 24 CA Certificate Page



CA Certificate

Current Certificate Information

You have no CA Certs available

Upload CA Certificate

Upload CA certificate

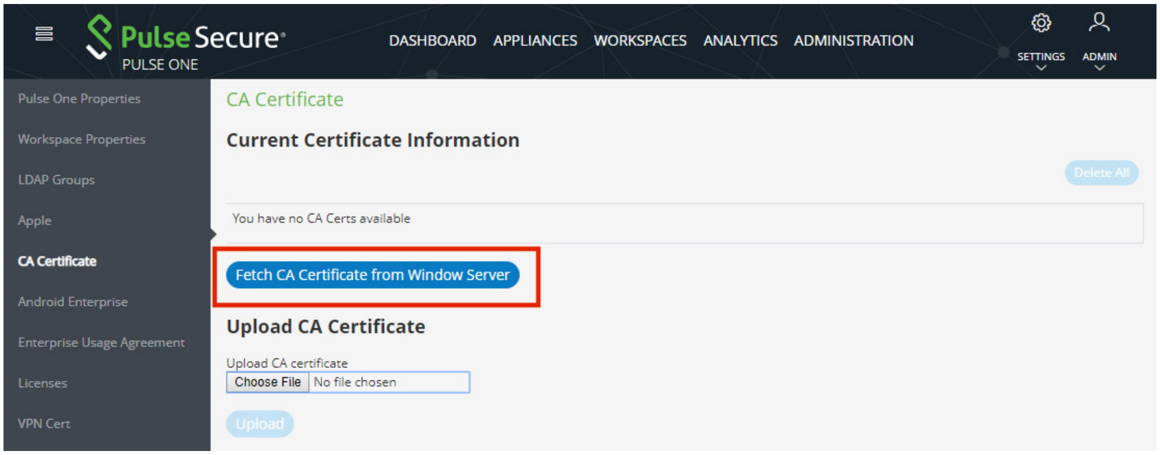
No file chosen

Note: The **Fetch CA Certificate from Windows Server** button is only displayed when you have an external PKI server configured, see **"Configuring an External PKI Server" on page 29**.

3. Click **Browse**.
4. Select the certificate file(s), which must be in PEM format.

5. (Optional) If an external PKI server is configured, you can click **Fetch CA Certificate from Windows Server**. See **"Configuring an External PKI Server" on page 29** for details of the required configuration.

FIGURE 25 Fetch CA Certificate



CA Certificate

Current Certificate Information

You have no CA Certs available

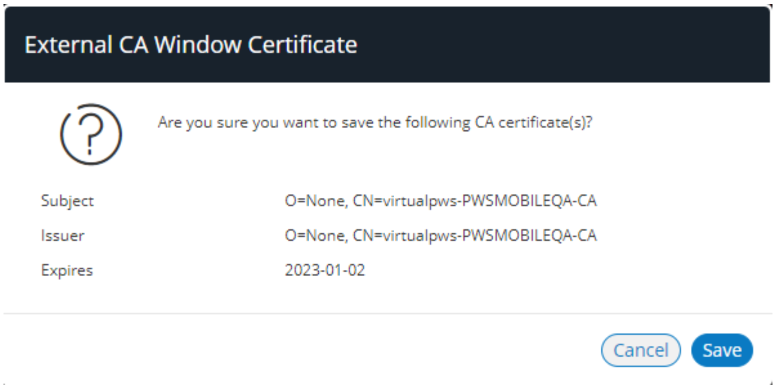
Upload CA Certificate

Upload CA certificate

No file chosen

A confirmation dialog for the retrieved CA certificate appears. For example:

FIGURE 26 Confirm CA Certificate



External CA Window Certificate

Are you sure you want to save the following CA certificate(s)?

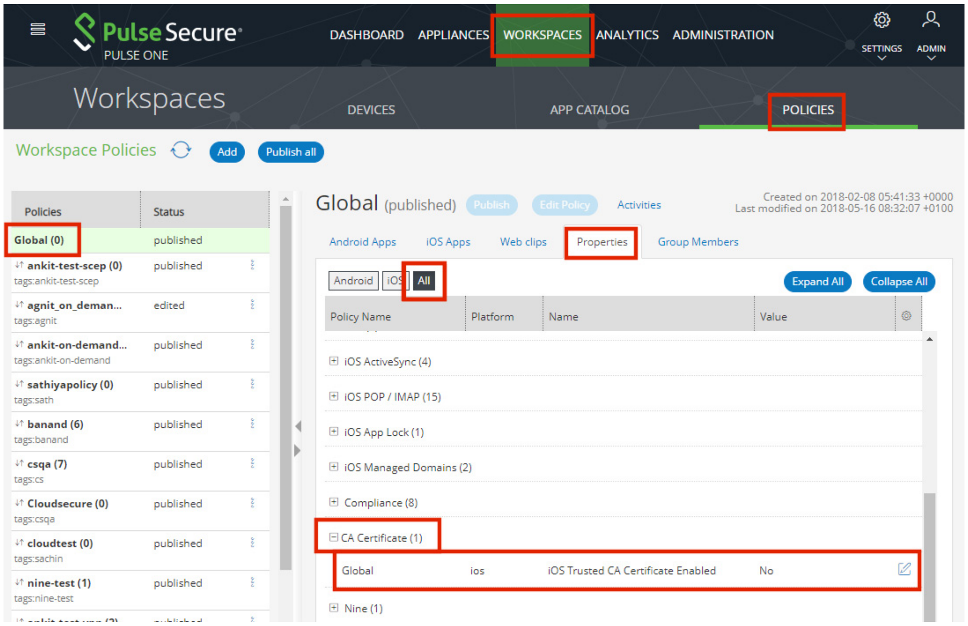
Subject	O=None, CN=virtualpws-PWSMOBILEQA-CA
Issuer	O=None, CN=virtualpws-PWSMOBILEQA-CA
Expires	2023-01-02

Click **Save** to add the CA certificate.

6. (Optional) Click **Upload** to upload one CA Certificate. You can upload one or more certificates.

7. Select **Workspaces > Policies > Global > Properties > All > CA Certificate**.

FIGURE 27 CA Certificate Settings



Global (published)

Created on 2018-02-08 05:41:33 +0000
Last modified on 2018-05-16 08:32:07 +0100

Policies	Status
Global (0)	published
ankit-test-scep (0) tags:ankit-test-scep	published
agnit_on_deman... tags:agnit	edited
ankit-on-demand... tags:ankit-on-demand	published
sathiyapolicy (0) tags:sath	published
banand (6) tags:banand	published
csqa (7) tags:cs	published
Cloudsecure (0) tags:csqa	published
cloudtest (0) tags:sachin	published
nine-test (1) tags:nine-test	published

Policy Name	Platform	Name	Value
⊞ iOS ActiveSync (4)			
⊞ iOS POP / IMAP (15)			
⊞ iOS App Lock (1)			
⊞ iOS Managed Domains (2)			
⊞ Compliance (8)			
⊟ CA Certificate (1)			
Global	ios	iOS Trusted CA Certificate Enabled	No
⊞ Nine (1)			

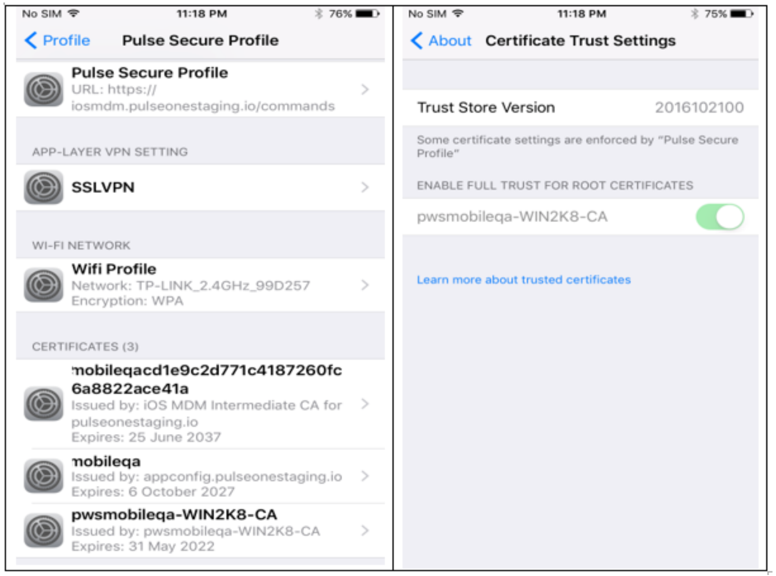
8. Set **iOS Trusted CA Certificate Enabled** to Yes.

9. Click **Publish**.

10. You must then provision an iOS device. To do this, from the device, navigate to **Settings > General > Profile and Device Management > Pulse Secure Profile > More Details** and verify that the CA Certificate is pushed as part of MDM payload.

11. Navigate to **Settings** > **General** > **About** > **Certificate Trust Settings** and verify that the CA Certificate is trusted.

FIGURE 28 CA Certificate



No SIM 11:18 PM 76%

Profile **Pulse Secure Profile**

Pulse Secure Profile
URL: https://
iosmdm.pulseonestaging.io/commands

APP-LAYER VPN SETTING

SSLVPN

WI-FI NETWORK

Wifi Profile
Network: TP-LINK_2.4GHz_99D257
Encryption: WPA

CERTIFICATES (3)

mobileqacd1e9c2d771c4187260fc6a8822ace41a
Issued by: iOS MDM Intermediate CA for pulseonestaging.io
Expires: 25 June 2037

mobileqa
Issued by: appconfig.pulseonestaging.io
Expires: 6 October 2027

pwsmobileqa-WIN2K8-CA
Issued by: pwsmobileqa-WIN2K8-CA
Expires: 31 May 2022

No SIM 11:18 PM 75%

About **Certificate Trust Settings**

Trust Store Version 2016102100

Some certificate settings are enforced by "Pulse Secure Profile"

ENABLE FULL TRUST FOR ROOT CERTIFICATES

pwsmobileqa-WIN2K8-CA

Learn more about trusted certificates

12. (Optional) To update a certificate, click **Browse**, select the certificate file and click **Update**.

13. (Optional) To delete a certificate, click the corresponding **Delete** button and confirm with **Yes** in the confirmation box.

14. Optional) To update a certificate chain, click **Browse**, select the certificate file and click **Update**.

15. (Optional) To delete a certificate chain, click the corresponding Delete button and confirm with Yes in the confirmation box.

16. (Optional) The Delete All option deletes all the certificates.

Configuring an External PKI Server

If you want to fetch CA certificates from a Windows server from the **CA Certificates** page, you must configure an external PKI server for use. To do this:

1. Click the **Settings** icon on top-right-corner of the home page.
2. Select **Workspace Properties** to go to the **Workspace Properties** page.
3. Expand **Enterprise PKI Integration**.
4. Set **Use external PKI server** to *Yes*.
5. Set **Windows CA Server 'certsrv' URL** to the required URL. For example: *https://www.example.com/certsrv/*

6. Set **Windows CA Server certsrv page user name** to the required CA server user name. For example: *Administrator*.

7. Set **Windows CA Server certsrv page user password** as the password for the specified user.

The configuration is complete.

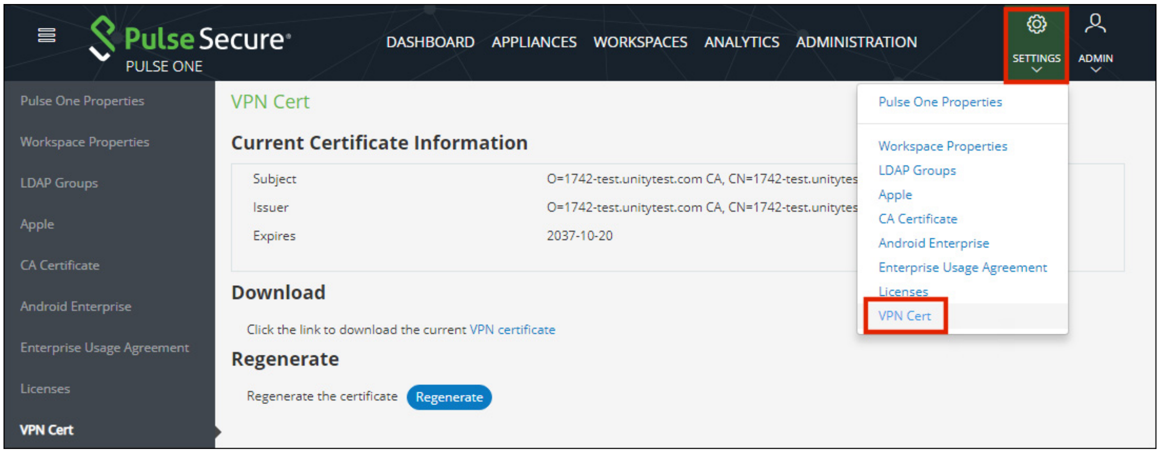
Configuring a VPN Certificate

The Workspace Management Server includes an integrated Certificate Authority (CA) and Online Certificate Status Protocol (OCSP) server. These can be used to issue certificates to workspaces for client certificate-based VPN authentication. You can use the VPN Cert window to download your Workspace Root CA certificate. This will be used when configuring your VPN.

1. Click the **Settings** icon on top-right-corner of the page and select **VPN Cert** to go to the **VPN Certificate** download page.

2. Click the **VPN certificate** link to download the CA Certificate for this Management console.

FIGURE 29 Download VPN Root Certificate



VPN Cert

Current Certificate Information

Subject	O=1742-test.unitytest.com CA, CN=1742-test.unitytes
Issuer	O=1742-test.unitytest.com CA, CN=1742-test.unitytes
Expires	2037-10-20

Download

Click the link to download the current VPN certificate

Regenerate

Regenerate the certificate Regenerate

3. To renew the certificate, click **Regenerate**.

4. In the confirmation dialog that is displayed, click **Yes**.

5. Click on the **VPN Certificate** link to download the regenerated cert.

6. Log in to PCS appliance and navigate to **System > Configuration > Certificates > Trusted Client CAs**.

7. Delete the old CA certificate.

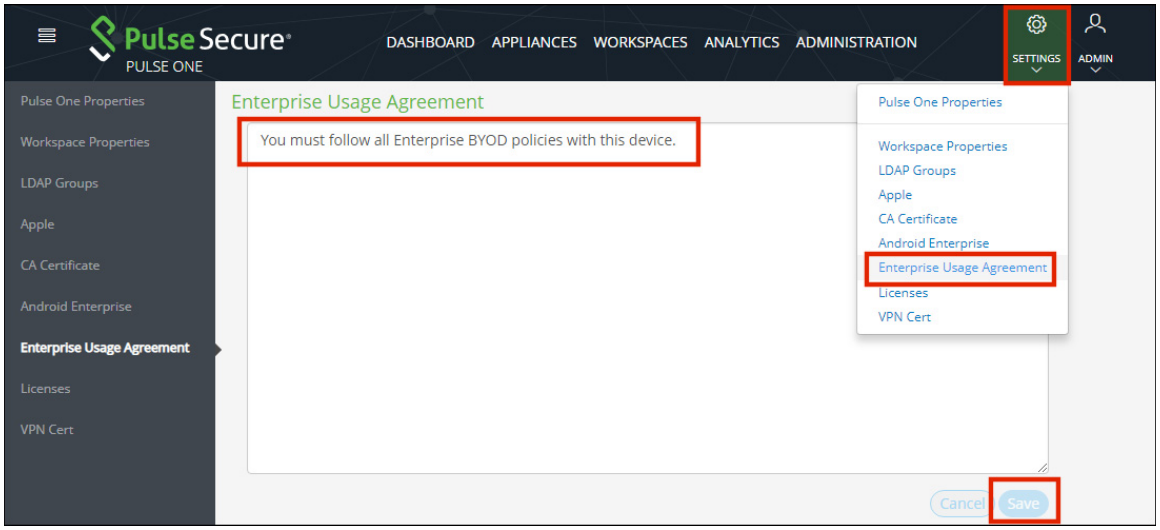
8. Click on the **Import CA Certificate** link to upload this certificate.

Changing the Enterprise Usage Agreement

The Enterprise Usage Agreement must be agreed when you provision the Workspace. This should be modified with your required Enterprise Usage Agreement. This section details the steps to edit the Enterprise Usage Agreement.

1. Click the **Settings** icon on top-right-corner of the page.
2. Select **Enterprise Usage Agreement** to go to the **Enterprise Usage Agreement** management page.

FIGURE 30 Navigate to Enterprise Usage Agreement



You must follow all Enterprise BYOD policies with this device.

3. Edit the text in the **Enterprise Usage Agreement**.
4. Click **Save**.

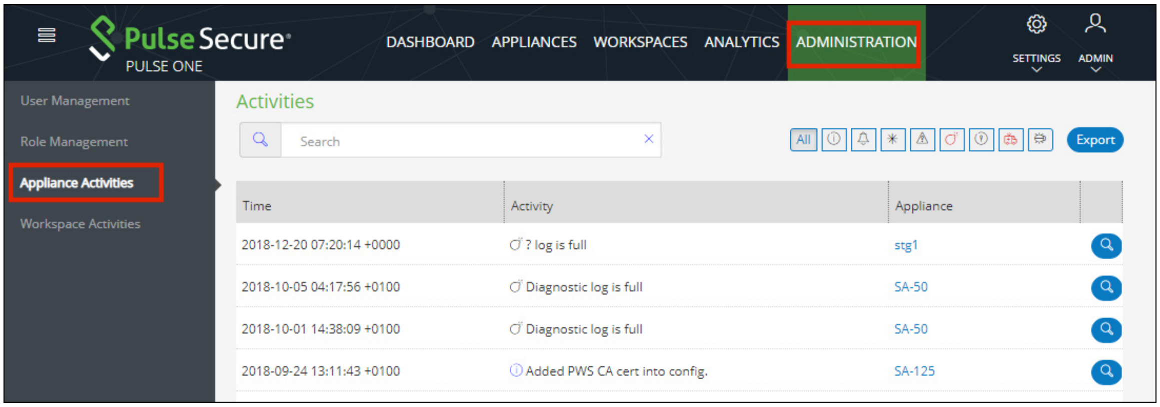
Viewing Activity Logs

The Activity Logs display information about the events registered in the Management Server. These include Appliance and Workspace activities. You can view filtered Activities for Users, Workspaces or Policies.

To view Appliance activities:

1. Select the **Administration** menu.
2. Click **Appliance Activities**. For example:

FIGURE 31 Appliance Activities

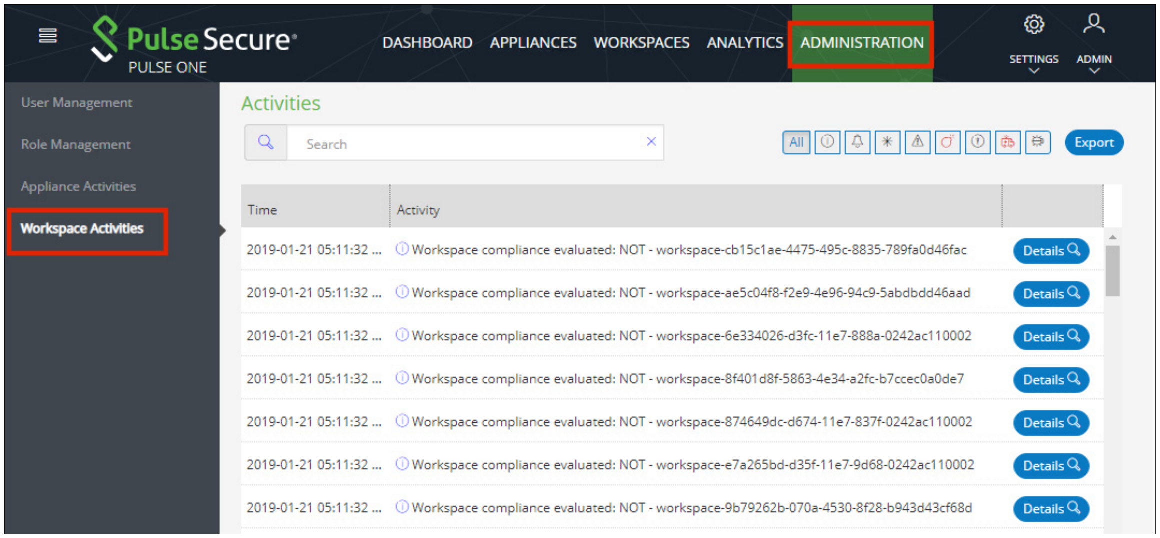


Time	Activity	Appliance
2018-12-20 07:20:14 +0000	? log is full	stg1
2018-10-05 04:17:56 +0100	Diagnostic log is full	SA-50
2018-10-01 14:38:09 +0100	Diagnostic log is full	SA-50
2018-09-24 13:11:43 +0100	Added PWS CA cert into config.	SA-125

To view Workspace activities:

3. Select the **Administration** menu.
4. Click **Workspace Activities**. For example:

FIGURE 32 Workspace Activities



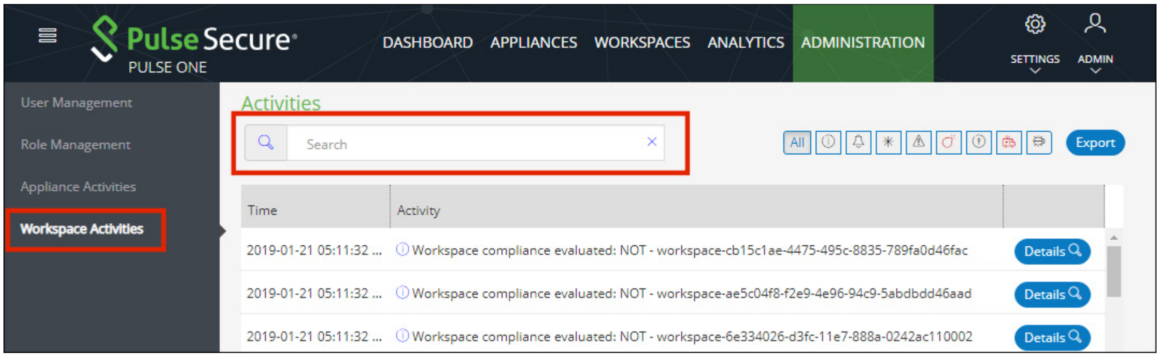
Time	Activity	
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-cb15c1ae-4475-495c-8835-789fa0d46fac	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-ae5c04f8-f2e9-4e96-94c9-5abdbdd46aad	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-6e334026-d3fc-11e7-888a-0242ac110002	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-8f401d8f-5863-4e34-a2fc-b7ccec0a0de7	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-874649dc-d674-11e7-837f-0242ac110002	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-e7a265bd-d35f-11e7-9d68-0242ac110002	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-9b79262b-070a-4530-8f28-b943d43cf68d	Details

Searching for an Activity

To search for individual events:

1. Access workspace activities.
2. Type a search term into the search box and press **Enter**. Examples of search terms for Workspace activities are usernames, event types and workspace IDs. For example:

FIGURE 33 Search Activity

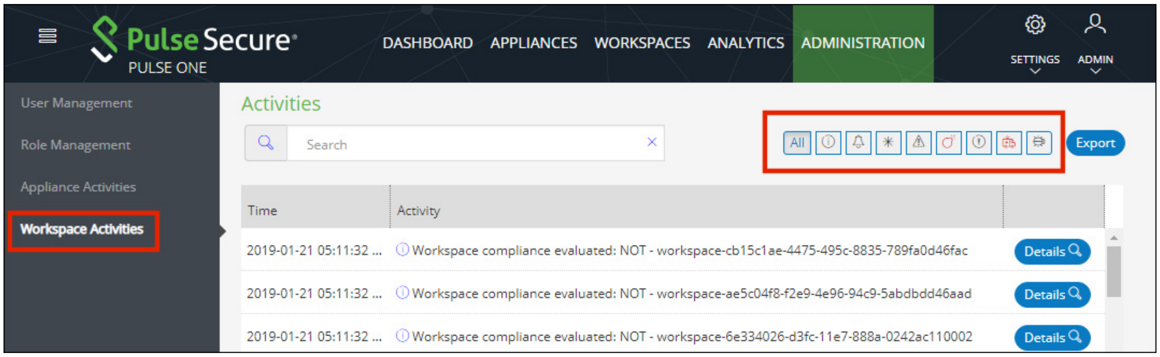


Time	Activity	
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-cb15c1ae-4475-495c-8835-789fa0d46fac	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-ae5c04f8-f2e9-4e96-94c9-5abdbdd46aad	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-6e334026-d3fc-11e7-888a-0242ac110002	Details

Filtering Activities

1. Access workspace activities.
2. Click an event type button to filter for a specific event type. For example:

FIGURE 34 Filter Activities

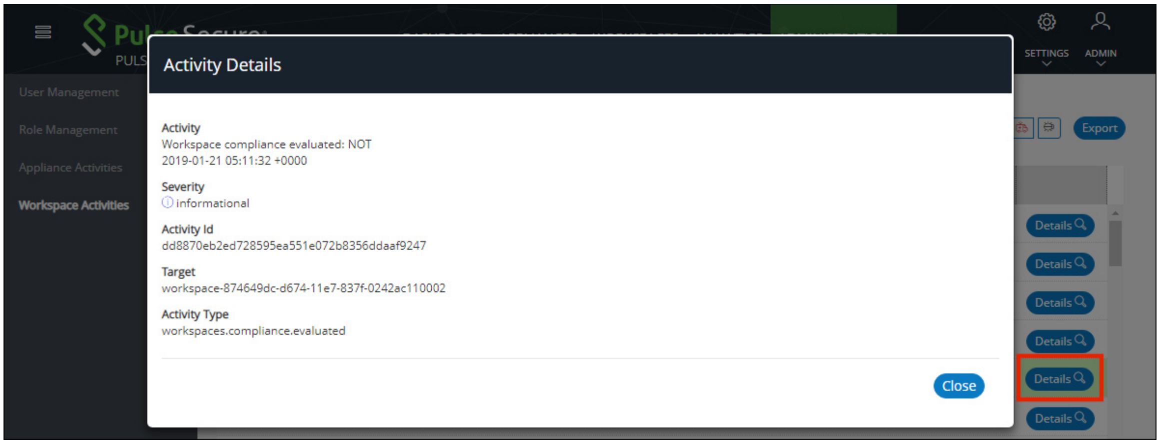


Time	Activity	
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-cb15c1ae-4475-495c-8835-789fa0d46fac	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-ae5c04f8-f2e9-4e96-94c9-5abdbdd46aad	Details
2019-01-21 05:11:32 ...	Workspace compliance evaluated: NOT - workspace-6e334026-d3fc-11e7-888a-0242ac110002	Details

Viewing Activity Details

1. Access workspace activities.
2. Click the **Details** button associated with the activity you want view the details. The Activity Details dialog displays the additional details.

FIGURE 35 Activity Details



Activity Details

Activity
Workspace compliance evaluated: NOT
2019-01-21 05:11:32 +0000

Severity
informational

Activity Id
dd8870eb2ed728595ea551e072b8356ddaaf9247

Target
workspace-874649dc-d674-11e7-837f-0242ac110002

Activity Type
workspaces.compliance.evaluated

Licensing Pulse One and Pulse Workspace

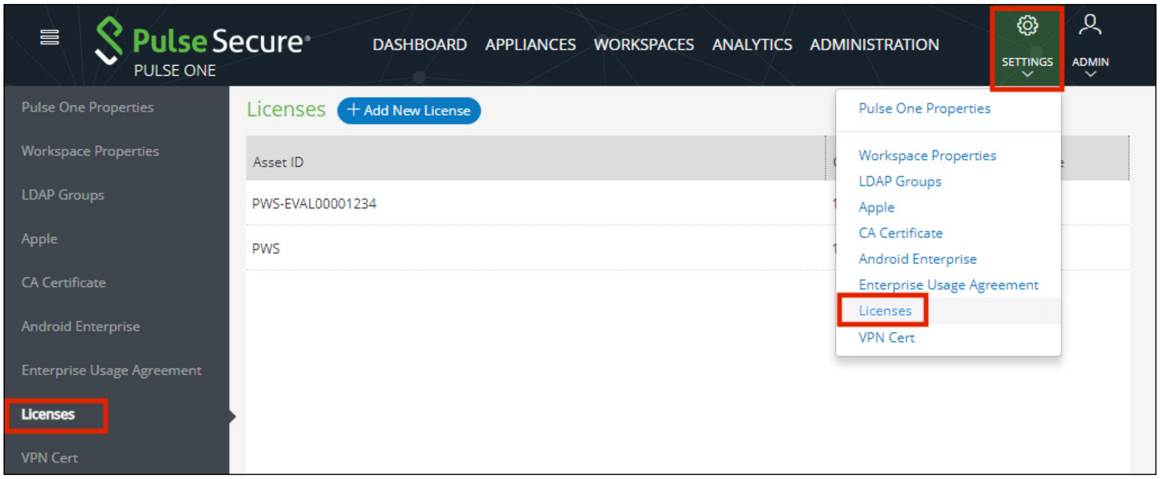
The **Licenses** screen lists:

- Licenses, identified by their **Asset ID**.
- The **Quantity** of each license available.
- The license **Expiration Date**.

To view licenses:

1. Click the **Settings** icon on top-right-corner of the page.
2. Select **Licenses**.

FIGURE 36 License Details



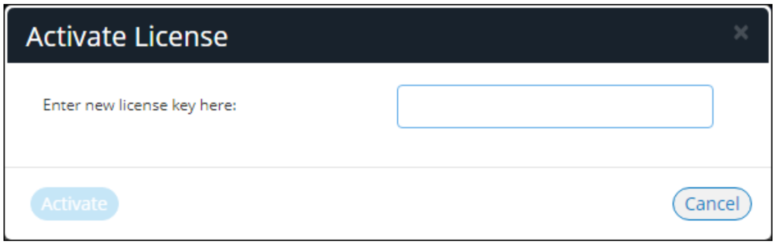
You can add one or more Pulse One and Pulse Workspace licenses on the **Licenses** page.

To add a new license:

1. Click **Add New License**.

   The **Activate License** dialog appears.

   FIGURE 37 Activate License



2. Enter the new license key.
3. Click **Activate**.

   If the license key validation is successful, a confirmation is displayed, and the license is added to the **Licenses** page.

Provisioning Devices

Features Supported on iOS and Android Devices

This section provides information about the features supported by Pulse Secure Client on iOS and Android devices.

Note: For iOS devices, the Pulse Secure Client requires iOS v10 or later.

Features supported on iOS v10.0+ Devices

- **VPN + Workspace**: The client supports any of the following connectivity modes:
  - *VPN only* – connects to Pulse Connect Secure (PCS).
  - *Workspace only* – connects to Pulse Workspace (PWS).
  - *VPN+Workspace* – connects to PCS for VPN and PWS for Mobile management.
- **Seamless onboarding to PCS and PWS**: The Pulse Secure client:
  - Enables the end user to enter a connection URL on the **Welcome** page.
  - Can automatically detect the type of server (PCS or PWS) by validating the user-entered connection URL.
  - Provides a seamless onboarding to the corresponding server.
- **PWS onboarding using SAML based authentication**: Pulse Secure client supports SAML based authentication for onboarding a user to PWS. For this feature, PWS acts as the SAML Service Provider (SP) and PCS acts as SAML Identity Provider (IdP). For this release, IdP support is restricted only to PCS. The third party IdPs are not supported.
- **Compliance reporting**: Pulse Secure client can detect the compliance status of a device. If the device is non- compliant, additional actions are provided to the end-user.

- **Apple Volume Purchase Program**: The Volume Purchase Program (VPP) allows businesses to purchase apps in volume and distribute them within their organizations.
- **Blacklisting of iOS Package Names**: This policy controls the user's ability to install and use apps that are flagged as blacklisted.
- **Device Location –** Registered iOS devices can now be located from Pulse Workspace via the Apple Push Notification (APN) service, see **"Working with Device Location" on page 235**.
- **Application Visibility**: These policies enable the collection of app usage and version metrics from devices. These metrics are used for the App Visibility Report.
- **Modifying Bluetooth Settings policy**: This policy controls the user's ability to change Bluetooth settings.

Features supported on iOS v7.0+ Devices

- **Kerberos authentication** - Registered iOS devices can use Kerberos-based authentication over HTTP, see **"Configuring Kerberos-Based Authentication" on page 232**.

Features supported on Android v8.0+ devices

- **Device Location –** Registered Android devices can be located from Pulse Workspace, see **"Working with Device Location" on page 235**.

Configuring Domain Discovery and Email-based Authentication

This section describes:

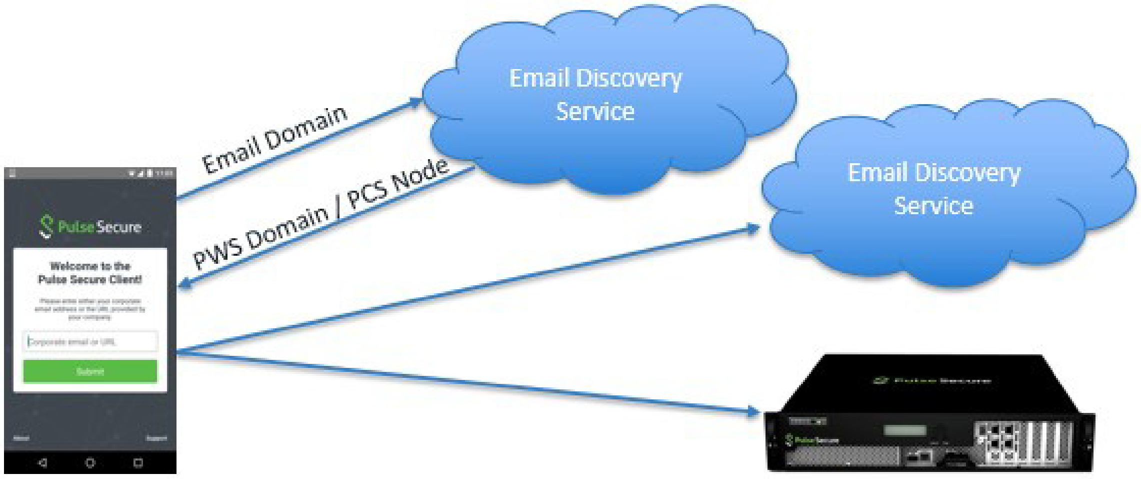
- "Overview" on page 39.
- "Adding a Customer" on page 40.
- "Adding a Domain" on page 40.

Overview

The email discovery service uses the domain in user's email to discover the right PWS / PCS to connect, and requires the user just to enter the email address to enroll or authenticate and access the resources.

The email discovery service runs in the cloud environment. It works with iOS and Android mobiles and requires PWS / PCS servers.

FIGURE 38 Email Discovery Service Overview



Note: To set up the Auto-Discovery experience, you will need to contact Pulse Secure Technical support through DevOps ticket. After the required information is provided (and validated), Technical Support will enable the Auto-Discovery experience for your Email Domain.

The process is as follows:

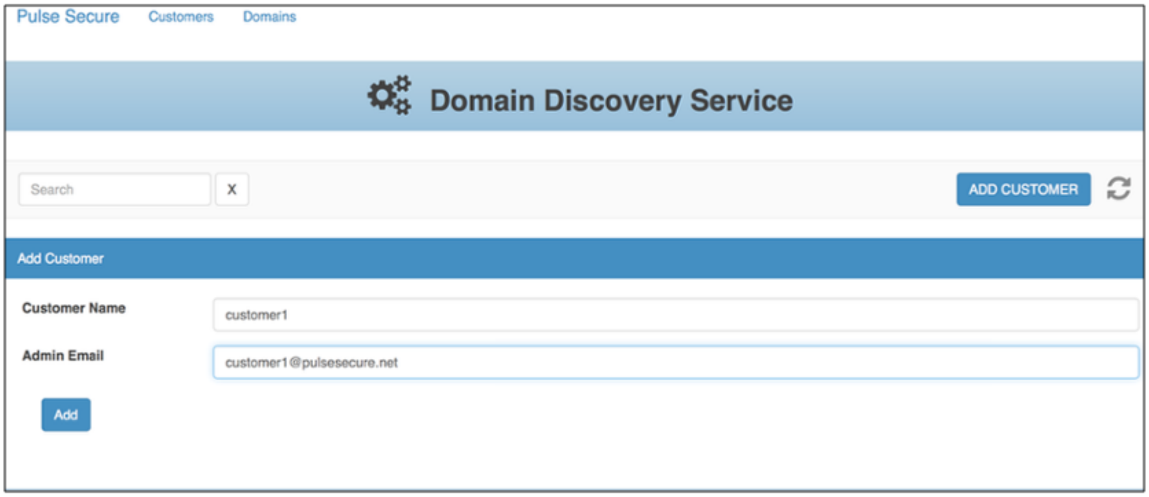
1. The customer calls Support to request an email discovery service.
2. The customer must provide the following details: PWS domain, PCS URL and email domain.
3. Support raises a DevOps ticket.
4. DevOps sets up an email account.
5. The customer then uses the email to authenticate and access the resources.

Adding a Customer

When you receive a request for setting up domain discovery service, use the **Domain Discovery Service** page to add the customer details.

1. Log in to Pulse One using super admin credentials.
2. In the **Domain Discover Service** page, select the **Customers** tab.
3. Click **Add Customer**.
4. Enter **Customer Name** and **Admin Email**.
5. Click **Add**.

FIGURE 39 Domain Discovery Service Page



Customer Name: customer1

Admin Email: customer1@pulsesecure.net

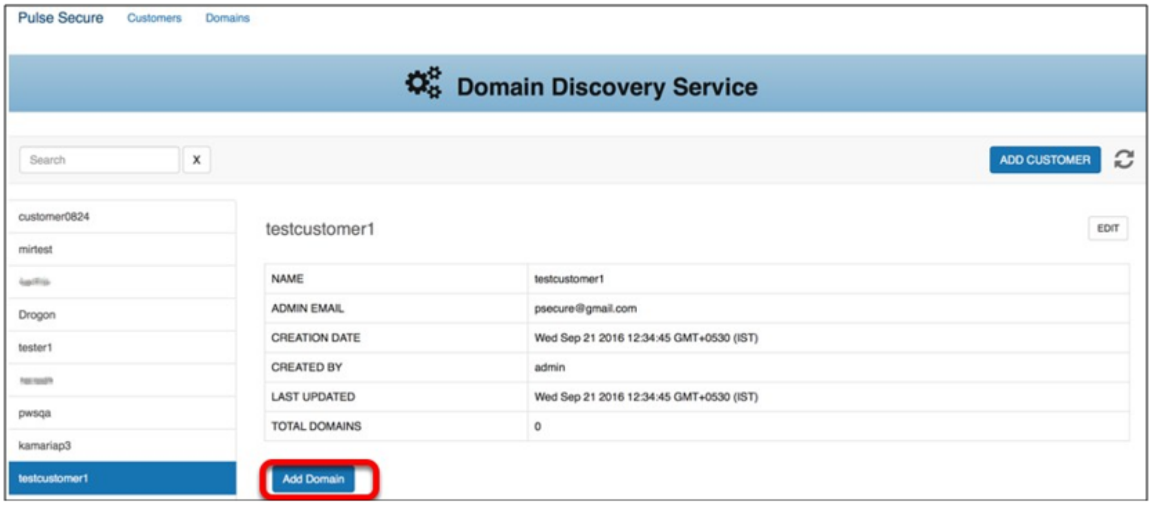
Adding a Domain

After you create the customer for domain discovery service, you must add a domain to the customer.

1. Log in to Pulse One using super admin credentials.
2. In the **Customers** tab, select the customer to whom you want to provide the domain discovery service.

3. Click **Add Domain**.

FIGURE 40 Add Domain



testcustomer1

NAME	testcustomer1
ADMIN EMAIL	psecure@gmail.com
CREATION DATE	Wed Sep 21 2016 12:34:45 GMT+0530 (IST)
CREATED BY	admin
LAST UPDATED	Wed Sep 21 2016 12:34:45 GMT+0530 (IST)
TOTAL DOMAINS	0

4. In the **Add Domain to <customer>** page, enter the domain details.

   - **Domain Name**
   - **Domain Short Name**
   - **Console URL**

5. In the Android Configuration:

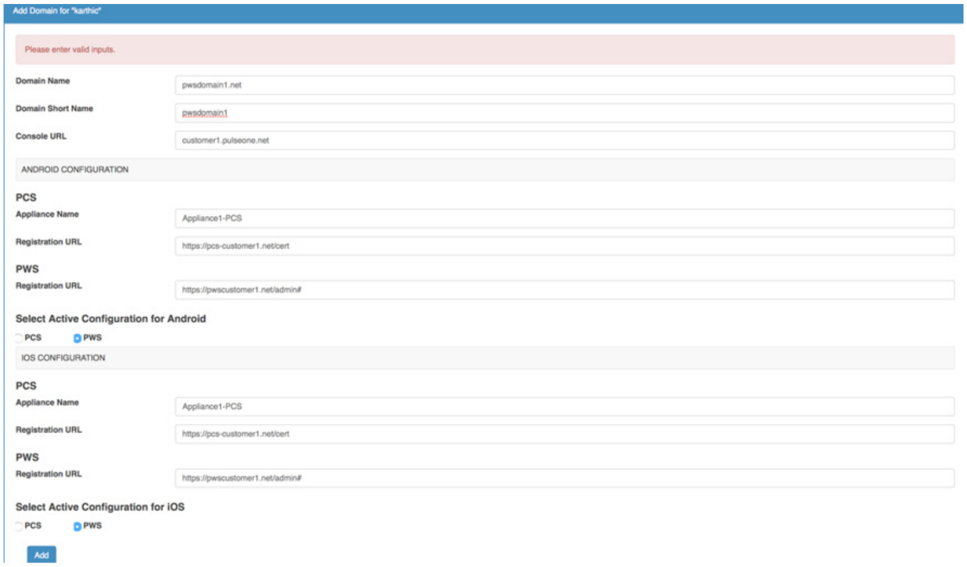
   - Enter **PCS Appliance Name** and **Registration URL**.
   - Enter **PWS Registration URL**.
   - To select Active Configuration for Android, click the *PCS* or *PWS* option.

6. In the iOS Configuration:

   - Enter the PCS and PWS details.
   - To select Active Configuration for iOS, click the *PCS* or *PWS* option.

7. Click **Add**.

FIGURE 41 Add Domain Details



Add Domain for "karthic"

Please enter valid inputs.

Domain Name: pwsdomain1.net

Domain Short Name: pwsdomain1

Console URL: customer1.pulseone.net

ANDROID CONFIGURATION

PCS

Appliance Name: Appliance1-PCS

Registration URL: https://pcs-customer1.net/cert

PWS

Registration URL: https://pwscustomer1.net/admin#

Select Active Configuration for Android

○ PCS ● PWS

IOS CONFIGURATION

PCS

Appliance Name: Appliance1-PCS

Registration URL: https://pcs-customer1.net/cert

PWS

Registration URL: https://pwscustomer1.net/admin#

Select Active Configuration for iOS

○ PCS ● PWS

For the client side details about domain discovery service, refer to the following topics in Pulse Secure documentation:

- Android Workspace Onboarding.
- iOS Workspace Onboarding.

Understanding Managed Devices and Managed Clients

Pulse Workspace supports two different modes of working with mobile devices:

- *Managed device* mode uses Mobile Device Management (MDM). This is the default mode, and the basis for all Pulse Workspace device enrollment before the 2.0.1901 release.
  - Corporate devices will have a single *Work partition*, containing all data and apps on the device.
  - Bring Your Own Devices (BYODs) support the use of personal devices, and will have both a *Work partition* and a *Personal partition*.
  - The admin can manage the Work partition any enrolled device, push apps and policies to the device, evaluate the device's compliance status, locate the device, and ultimately lock or wipe the Work partition of the device if necessary.
- *Managed client* mode does not use MDM. Currently, the admin can push policies to enrolled devices to enable VPN on Demand on the device.

  Note: *Managed client* mode is currently only supported on iOS devices.

Managed client mode is selected by setting the **Enable enrollment of managed iOS clients?** workspace property, see **"Workspaces" on page 149**.

- When **Enable enrollment of managed iOS clients?** is *False* (default), *managed device* mode is used.
- When **Enable enrollment of managed iOS clients?** is *True*, *managed client* mode is used.

For full details of managed clients, see **"Configuring Managed Clients" on page 95**.

Onboarding iOS BYOD Devices

This section describes the steps to provision a Bring Your Own Device (BYOD) mobile iOS device. BYOD devices are personal property which are then configured to contain separate areas for:

- Personal apps and data.
- Corporate apps and data.

When the Workspace administrator invites you to provision your device, you will receive a welcome email which contains instructions for provisioning your device.

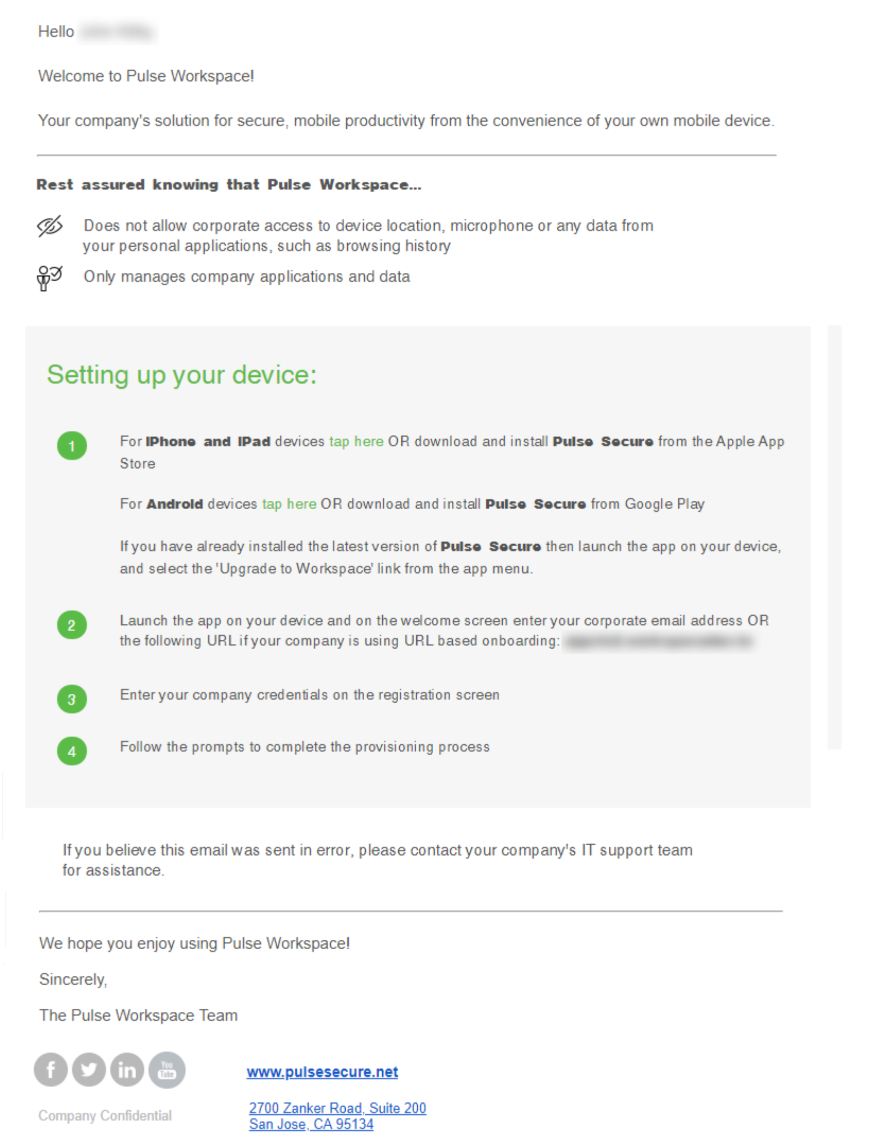
Based on the domain property setting, the registration workflow that follows the welcome email differs.

- **"Understanding Your SAML-Based Authentication Email" on page 44**.
- **"Understanding Your PIN-Based Authentication Email" on page 45**.
- **"Registering an iOS BYOD Device" on page 46**.

Understanding Your SAML-Based Authentication Email

Where your organization uses SAML authentication, you receive a welcome email. This is similar to the following:

FIGURE 42 Welcome Email: SAML Authentication



Hello [redacted]

Welcome to Pulse Workspace!

Your company's solution for secure, mobile productivity from the convenience of your own mobile device.

Rest assured knowing that Pulse Workspace...

Does not allow corporate access to device location, microphone or any data from your personal applications, such as browsing history

Only manages company applications and data

Setting up your device:

1. For **iPhone and iPad** devices tap here OR download and install **Pulse Secure** from the Apple App Store

   For **Android** devices tap here OR download and install **Pulse Secure** from Google Play

   If you have already installed the latest version of **Pulse Secure** then launch the app on your device, and select the 'Upgrade to Workspace' link from the app menu.

2. Launch the app on your device and on the welcome screen enter your corporate email address OR the following URL if your company is using URL based onboarding: [redacted]

3. Enter your company credentials on the registration screen

4. Follow the prompts to complete the provisioning process

If you believe this email was sent in error, please contact your company's IT support team for assistance.

We hope you enjoy using Pulse Workspace!

Sincerely,

The Pulse Workspace Team

www.pulsesecure.net

Company Confidential

2700 Zanker Road, Suite 200
San Jose, CA 95134

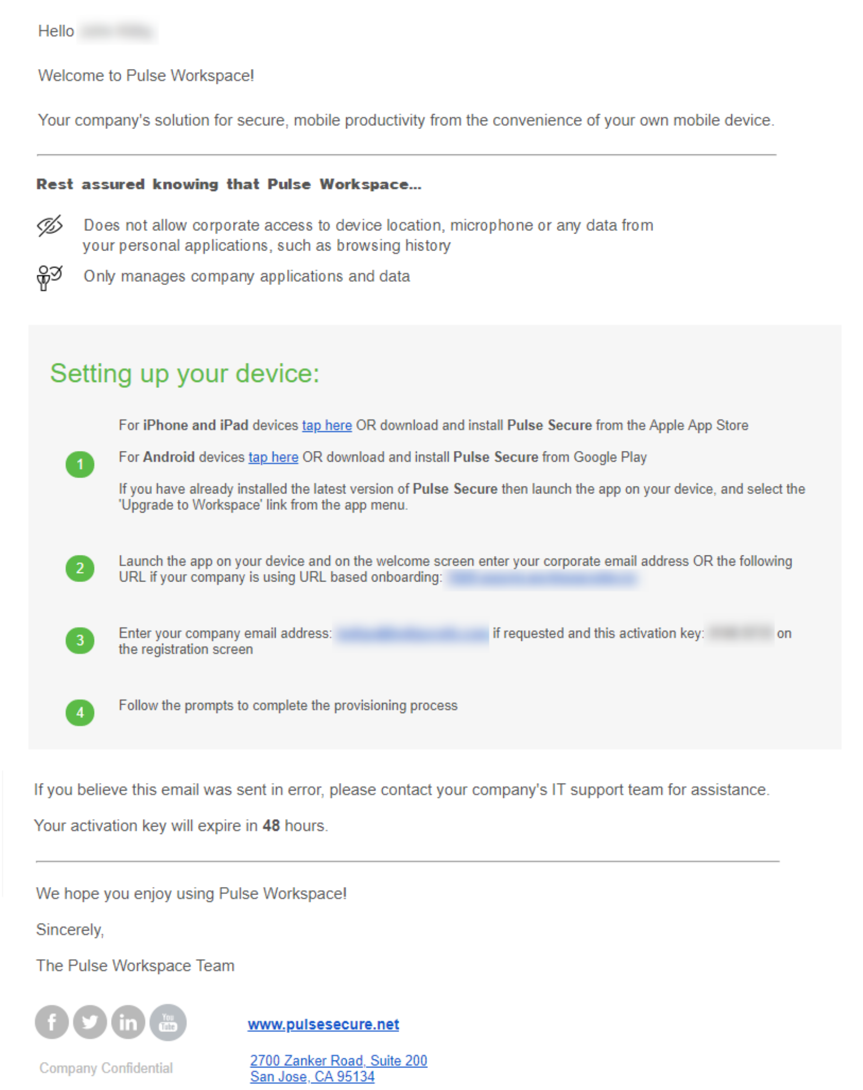
This email contains:

- A registration link to download and install Pulse Secure from Apple App Store for iPhone or iPad devices.
- An Enterprise URL.
- Instructions for completing the device registration.

Understanding Your PIN-Based Authentication Email

Where your organization does not use SAML authentication, you receive a welcome email. This is similar to the following:

FIGURE 43 Welcome Email: PIN Authentication



Hello [redacted]

Welcome to Pulse Workspace!

Your company's solution for secure, mobile productivity from the convenience of your own mobile device.

Rest assured knowing that Pulse Workspace...

Does not allow corporate access to device location, microphone or any data from your personal applications, such as browsing history

Only manages company applications and data

Setting up your device:

1. For **iPhone and iPad** devices tap here OR download and install **Pulse Secure** from the Apple App Store

   For **Android** devices tap here OR download and install **Pulse Secure** from Google Play

   If you have already installed the latest version of **Pulse Secure** then launch the app on your device, and select the 'Upgrade to Workspace' link from the app menu.

2. Launch the app on your device and on the welcome screen enter your corporate email address OR the following URL if your company is using URL based onboarding: [redacted]

3. Enter your company email address: [redacted] if requested and this activation key: [redacted] on the registration screen

4. Follow the prompts to complete the provisioning process

If you believe this email was sent in error, please contact your company's IT support team for assistance.

Your activation key will expire in **48** hours.

We hope you enjoy using Pulse Workspace!

Sincerely,

The Pulse Workspace Team

www.pulsesecure.net

Company Confidential

2700 Zanker Road, Suite 200
San Jose, CA 95134

This email contains:

- A registration link to download and install Pulse Secure from Apple App Store for iPhone or iPad devices.
- An Enterprise URL.
- A provisioning email address.
- A provisioning activation key.
- Instructions for completing the device registration.

Registering an iOS BYOD Device

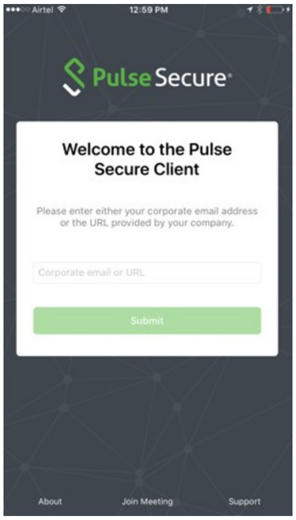
Note: Starting at iOS 12.2, Apple has changed the manual enrollment flow for Mobile Device Management (MDM), see **https://support.apple.com/en-us/HT209435**. As a result, installing the MDM profile involves some additional steps for end users who perform manual enrollment on their Apple device running iOS 12.2 and later. This change is applicable only for new Pulse Workspace user registrations.

To set up an iOS device when Pulse Secure is not installed on the device:

1. In your email, click the iOS registration link. This installs Pulse Secure.
2. Start Pulse Secure on your device.

   The Pulse Secure **Welcome** screen appears:

   FIGURE 44 Welcome

   Welcome to the Pulse Secure Client

   Please enter either your corporate email address or the URL provided by your company.

   On this screen:

   - Enter the Enterprise URL from your welcome email.
   - Click **Submit**.

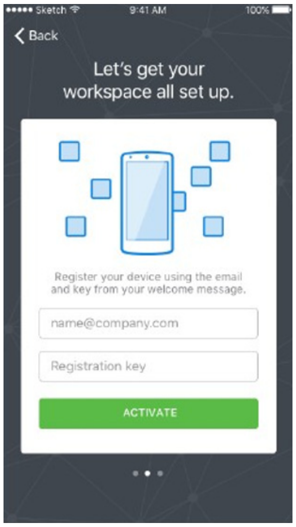
   The next step depends on whether you have SAML-based authentication.
3. (Optional) If you are using a SAML-based registration, the SAML **Login** screen appears.

   On this screen, enter your corporate user name and password and click **Sign In**.

   A BYOD policy **Agreement** page appears (skip step 4).

4. (Optional) If you are using PIN authentication, the following screen appears.

FIGURE 45 Entering your Key



●●●●● Sketch 9:41 AM 100%

Back

Let's get your workspace all set up.

Register your device using the email and key from your welcome message.

name@company.com

Registration key

ACTIVATE

On this screen:

- Enter your corporate email address.
- Enter your registration key from your welcome email.
- Click **Activate**.

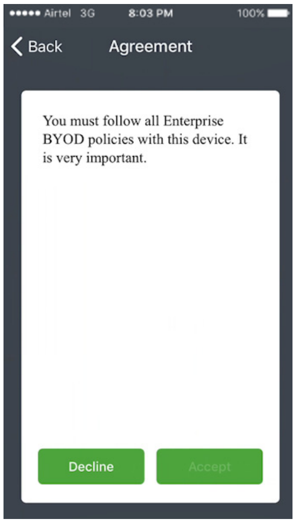
The client parses the domain and sends it to a discovery server to fetch the server URL. It then continues with Active Directory (AD) authentication with the server.

Note: To set up the Auto-Discovery experience, you will need to contact Pulse Secure Technical support through a DevOps ticket. After the needed information is provided (and validated), Technical Support will enable the Auto-Discovery experience for your Email Domain.

A BYOD policy **Agreement** page appears. (continue from step 5)

5. On the **Agreement** page, press the **Accept** button to accept the Enterprise BYOD policies.

FIGURE 46 Enterprise BYOD Policies

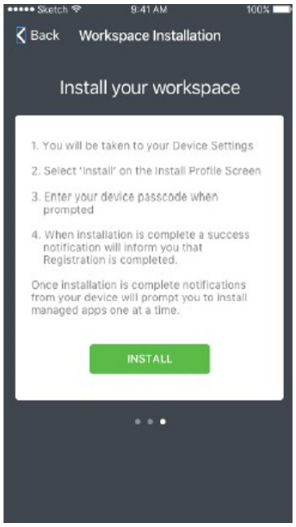


You must follow all Enterprise BYOD policies with this device. It is very important.

The **Install Your Workspace** page appears.

6. Press the **Install** button to begin workspace registration.

FIGURE 47 Workspace Installation



Install your workspace

1. You will be taken to your Device Settings
2. Select 'Install' on the Install Profile Screen
3. Enter your device passcode when prompted
4. When installation is complete a success notification will inform you that Registration is completed.

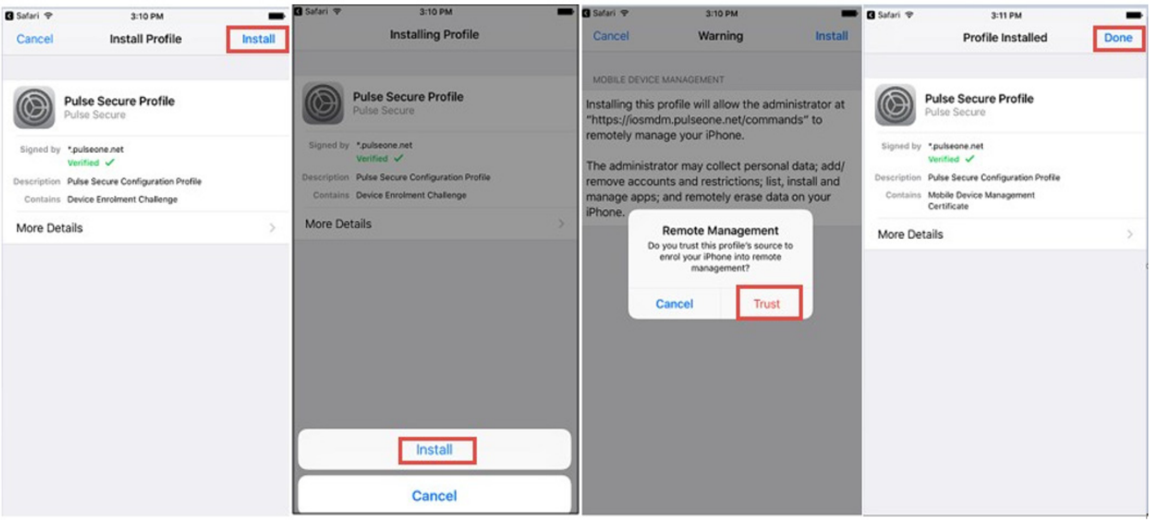
Once installation is complete notifications from your device will prompt you to install managed apps one at a time.

7. The next phase of this process depends on your iOS version.

   Note: To check the iOS version of your device, access **Settings > General > About**.

   - For iOS 12.1.4 or earlier, you are automatically prompted to install the Pulse Secure Profile Workspace Server certificate on the iOS device. Press **Install**, then **Install**, then **Trust**, and then **Done** to complete the process. For example:

     FIGURE 48 Installing the Pulse Secure Profile Workspace Server Certificate



Signed by *.pulseone.net
Verified ✓
Description Pulse Secure Configuration Profile
Contains Device Enrolment Challenge

Installing this profile will allow the administrator at "https://iosmdm.pulseone.net/commands" to remotely manage your iPhone.

The administrator may collect personal data; add/remove accounts and restrictions; list, install and manage apps; and remotely erase data on your iPhone.

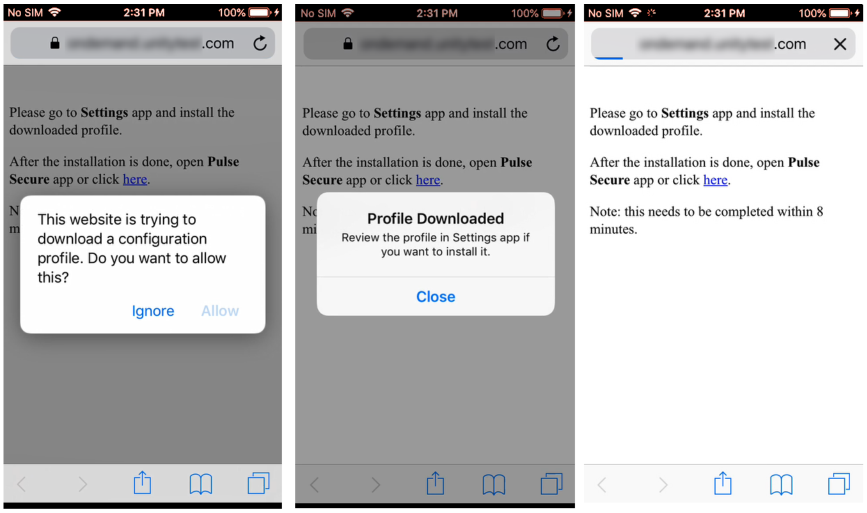
Do you trust this profile's source to enrol your iPhone into remote management?

Signed by *.pulseone.net
Verified ✓
Description Pulse Secure Configuration Profile
Contains Mobile Device Management Certificate

   - For iOS 12.2 or later, you are instructed to go to the **Settings** app and install the downloaded profile.

     Note: There is a time limited of eight minutes for the install operation.

     FIGURE 49 Downloading a Profile



Please go to **Settings** app and install the downloaded profile.

After the installation is done, open **Pulse Secure** app or click here.

This website is trying to download a configuration profile. Do you want to allow this?

Review the profile in Settings app if you want to install it.

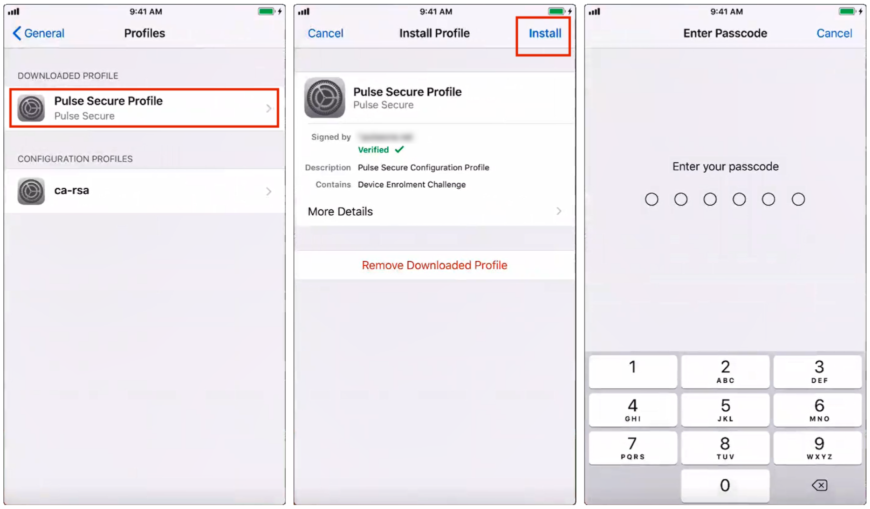
Note: this needs to be completed within 8 minutes.

     On the **iOS Device Registration** page, press **Allow**, and then **Close**.

     Note: Do not dismiss this screen. You will return to this screen later in this step.

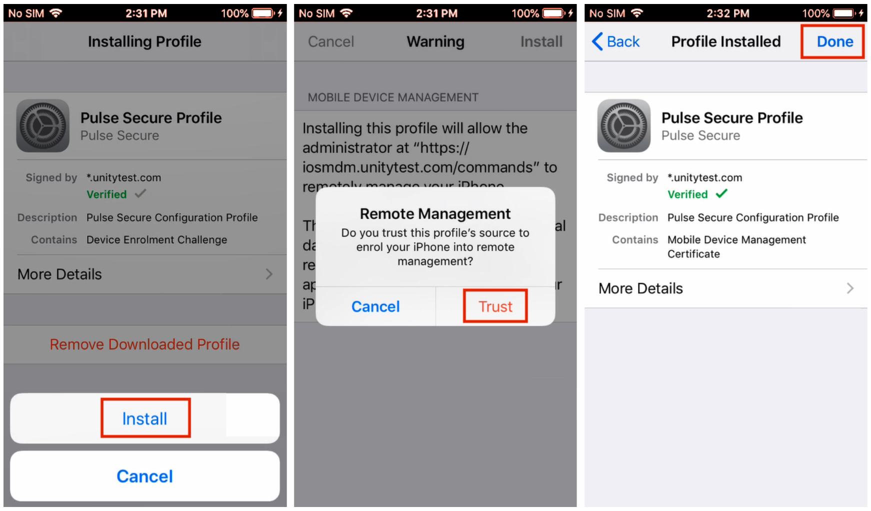
You must then manually access **Settings > General > Profiles**. Press the **Pulse Secure Profile**, then **Install**, and then enter your passcode.

FIGURE 50 Installing a Profile



Press **Install** to confirm the installation, then press **Trust**. Once the installation is complete, press **Done**.

FIGURE 51 Installing a Profile: Complete



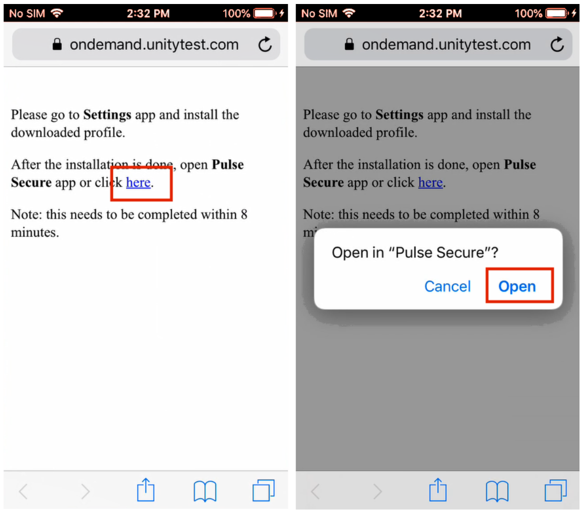
Installing this profile will allow the administrator at "https://iosmdm.unitytest.com/commands" to remotely manage your iPhone.

Remote Management

Do you trust this profile's source to enrol your iPhone into remote management?

You can then return to the **iOS Device Registration** page and click the hyperlink to complete and then press **Open** to complete this manual process.

FIGURE 52 Opening a Profile



No SIM 2:32 PM 100%

ondemand.unitytest.com

Please go to **Settings** app and install the downloaded profile.

After the installation is done, open **Pulse Secure** app or click here.

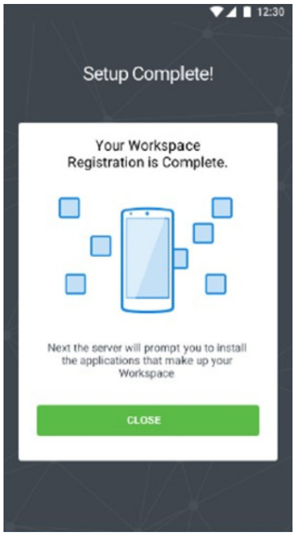
Note: this needs to be completed within 8 minutes.

Open in "Pulse Secure"?

Cancel Open

8. After the workspace registration is complete, press the **Close** button.

FIGURE 53 Setup Complete



12:30

Setup Complete!

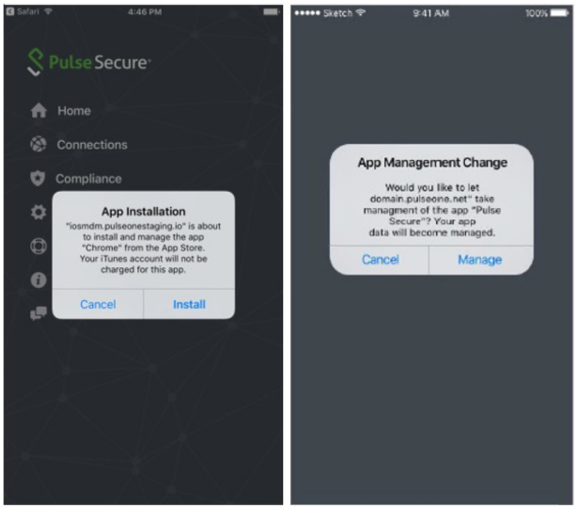
Your Workspace Registration is Complete.

Next the server will prompt you to install the applications that make up your Workspace

CLOSE

You may then be prompted to perform a variety of post-registration actions such as automatically installing applications, setting a device passcode or entering your email password. For example:

FIGURE 54 Post Enrollment Configuration



App Installation

"iosmdm.pulseonestaging.io" is about to install and manage the app "Chrome" from the App Store. Your iTunes account will not be charged for this app.

App Management Change

Would you like to let domain.pulseone.net" take managment of the app "Pulse Secure"? Your app data will become managed.

These actions will depend on:

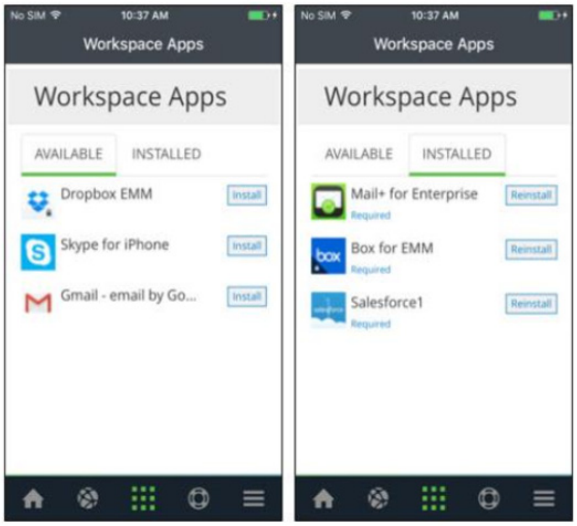
- Your enterprise security policy.
- Whether you are on a *managed device* or a *managed client*, see **"Understanding Managed Devices and Managed Clients" on page 42**. For example, managed clients will not install any applications after enrollment.

To install apps manually on a managed device:

1. Navigate to **Workspace Apps**.
2. Tap the **Installed** tab to view installed apps.

3. To install optional apps, tap the **Available** tab and press **Install** for each app you want to install.

FIGURE 55 Installed and Available Apps



After installation, the app will be listed in the **Installed** tab.

Onboarding Android BYOD Devices

This section describes the steps to provision a Bring Your Own Device (BYOD) Android device. BYOD devices are personal property which are then configured to contain separate areas for:

- Personal apps and data.
- Corporate apps and data.

When the Workspace administrator invites you to provision your mobile device, you will receive a welcome email which contains instructions for provisioning your device.

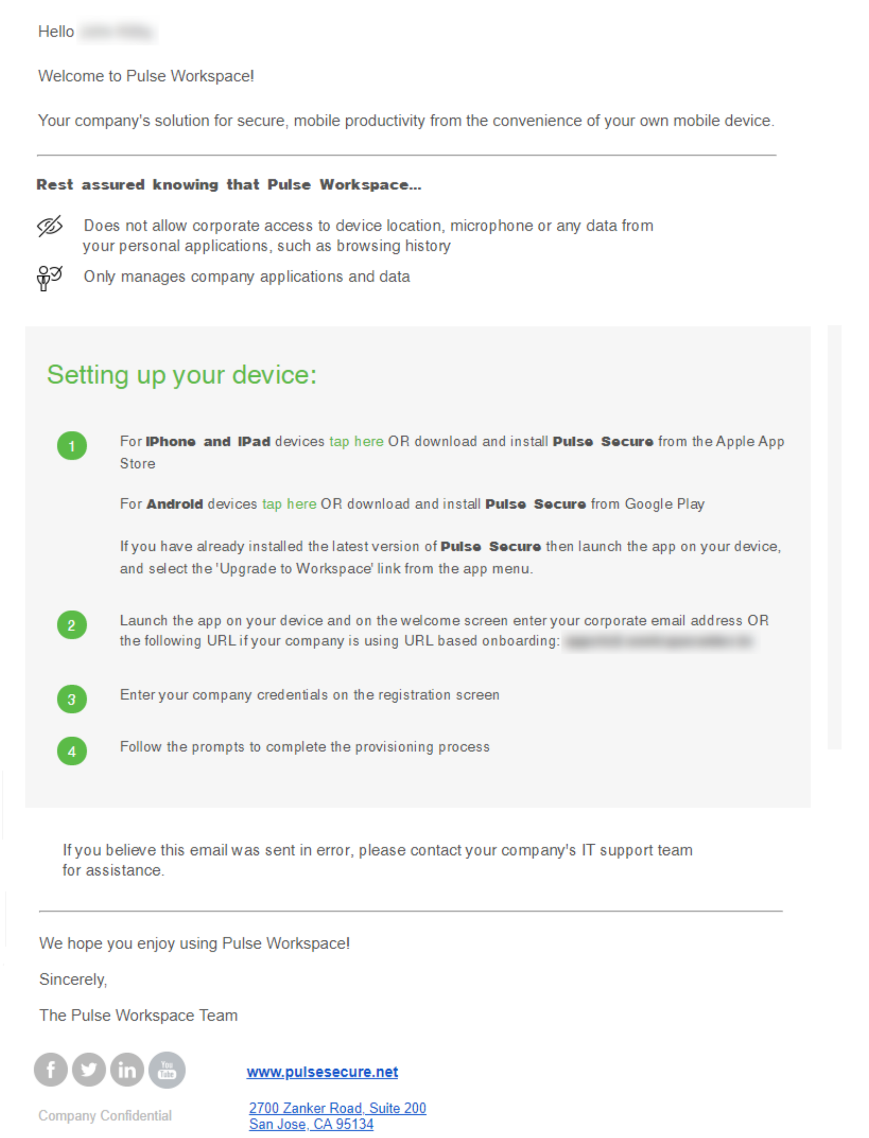
Based on the domain property setting, the registration workflow can be one of the following:

- **“Understanding Your SAML-Based Authentication Email” on page 54**.
- **“Understanding Your PIN-Based Authentication Email” on page 55**.
- **“Registering Your Android BYOD Device” on page 56**.

Understanding Your SAML-Based Authentication Email

Where your organization uses SAML authentication, you receive a welcome email. This is similar to the following:

FIGURE 56 Welcome Email: SAML Authentication



Hello [redacted]

Welcome to Pulse Workspace!

Your company's solution for secure, mobile productivity from the convenience of your own mobile device.

Rest assured knowing that Pulse Workspace...

Does not allow corporate access to device location, microphone or any data from your personal applications, such as browsing history

Only manages company applications and data

Setting up your device:

1. For **iPhone and iPad** devices tap here OR download and install **Pulse Secure** from the Apple App Store

   For **Android** devices tap here OR download and install **Pulse Secure** from Google Play

   If you have already installed the latest version of **Pulse Secure** then launch the app on your device, and select the 'Upgrade to Workspace' link from the app menu.

2. Launch the app on your device and on the welcome screen enter your corporate email address OR the following URL if your company is using URL based onboarding: [redacted]

3. Enter your company credentials on the registration screen

4. Follow the prompts to complete the provisioning process

If you believe this email was sent in error, please contact your company's IT support team for assistance.

We hope you enjoy using Pulse Workspace!

Sincerely,

The Pulse Workspace Team

www.pulsesecure.net

Company Confidential

2700 Zanker Road, Suite 200
San Jose, CA 95134

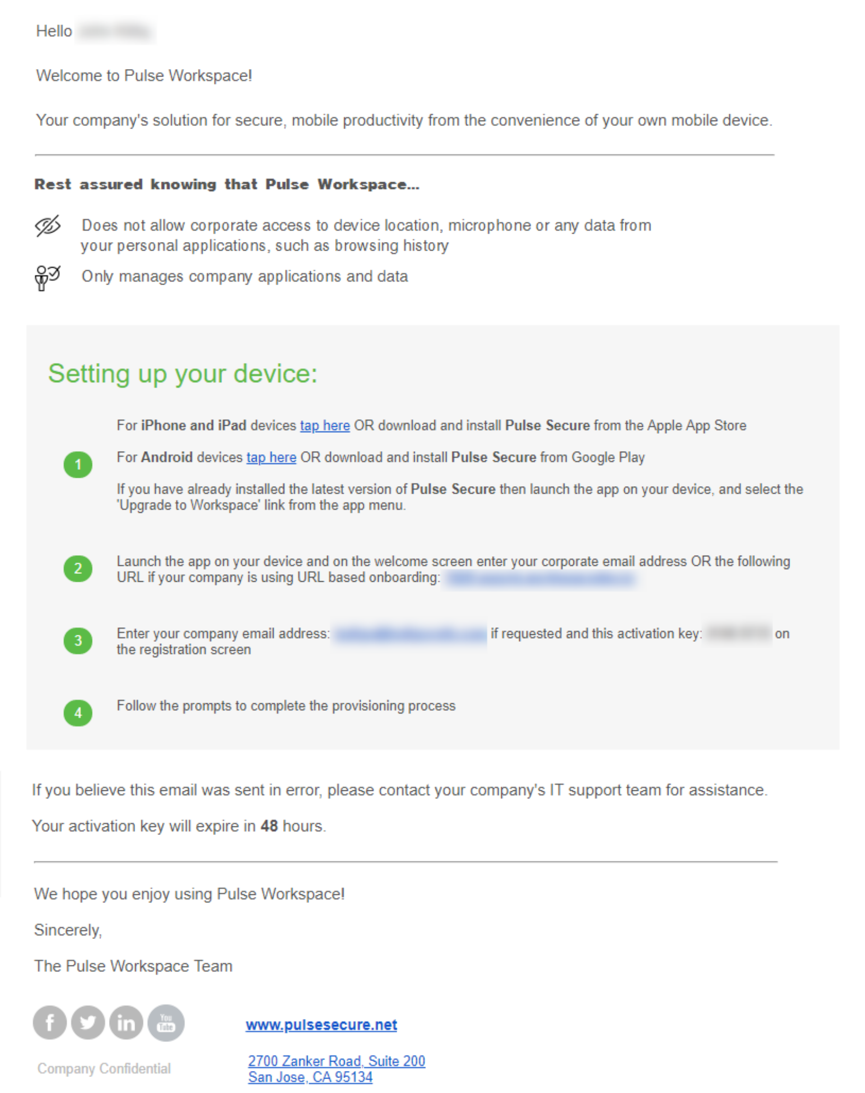
This email contains:

- A registration link to download and install Pulse Secure from the Google Play store.
- An Enterprise URL.
- Instructions for completing the device registration.

Understanding Your PIN-Based Authentication Email

Where your organization does not use SAML authentication, you receive a welcome email. This is similar to the following:

FIGURE 57 Welcome Email: PIN Authentication



Hello [redacted]

Welcome to Pulse Workspace!

Your company's solution for secure, mobile productivity from the convenience of your own mobile device.

Rest assured knowing that Pulse Workspace...

Does not allow corporate access to device location, microphone or any data from your personal applications, such as browsing history

Only manages company applications and data

Setting up your device:

1. For **iPhone and iPad** devices tap here OR download and install **Pulse Secure** from the Apple App Store

   For **Android** devices tap here OR download and install **Pulse Secure** from Google Play

   If you have already installed the latest version of **Pulse Secure** then launch the app on your device, and select the 'Upgrade to Workspace' link from the app menu.

2. Launch the app on your device and on the welcome screen enter your corporate email address OR the following URL if your company is using URL based onboarding: [redacted]

3. Enter your company email address: [redacted] if requested and this activation key: [redacted] on the registration screen

4. Follow the prompts to complete the provisioning process

If you believe this email was sent in error, please contact your company's IT support team for assistance.

Your activation key will expire in **48** hours.

We hope you enjoy using Pulse Workspace!

Sincerely,

The Pulse Workspace Team

Company Confidential

www.pulsesecure.net

2700 Zanker Road, Suite 200
San Jose, CA 95134

This email contains:

- A registration link to download and install Pulse Secure from the Google Play store.
- An Enterprise URL.
- A provisioning email address.
- A provisioning activation key.
- Instructions for completing the device registration.

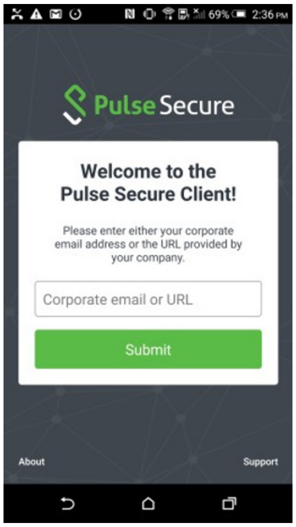
Registering Your Android BYOD Device

To set up your device when Pulse Secure is not installed on the device:

1. In your email, click the Android registration link. This installs Pulse Secure.
2. Start Pulse Secure on your device.

   The Pulse Secure **Welcome** screen appears. For example:

   FIGURE 58 Welcome

   Welcome to the Pulse Secure Client!

   Please enter either your corporate email address or the URL provided by your company.

   Corporate email or URL

3. On this screen:
   - Enter the Enterprise URL from your welcome email.
   - Click **Submit**.

   The next step depends on whether you have SAML-based authentication.

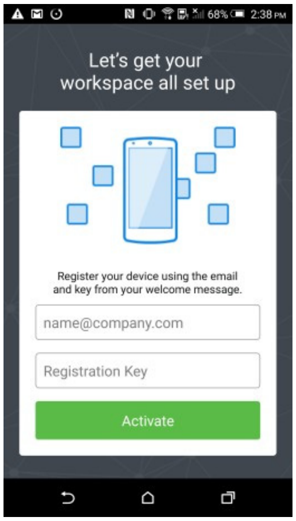
4. (Optional) If you are using a SAML-based registration, the SAML **Login** screen appears.

   On this screen, enter your corporate user name and password and click **Sign In**.

   A BYOD policy **Enterprise User Agreement** page appears (skip step 5).

5. (Optional) If you are using PIN authentication, the next screen appears. For example:

FIGURE 59 Registration Key



Let's get your workspace all set up

Register your device using the email and key from your welcome message.

name@company.com

Registration Key

On this screen:

- Enter your corporate email address.
- Enter your registration key from your welcome email.
- Click **Activate**.

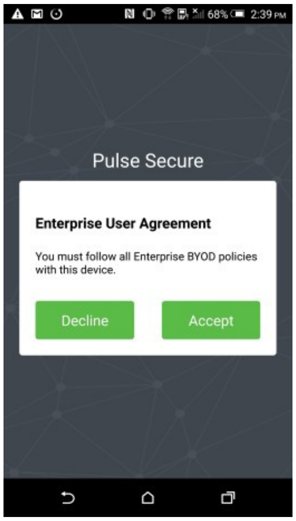
The client parses the domain and sends it to a discovery server to fetch the server URL. It then continues with Active Directory (AD) authentication with the server.

Note: To set up the Auto-Discovery experience, you will need to contact Pulse Secure Technical Support using a DevOps ticket. After the needed information is provided (and validated), Technical Support will enable the Auto-Discovery experience for your Email Domain.

A BYOD policy **Enterprise User Agreement** page appears (continue from step 6)

6. On the **Enterprise User Agreement** page, press the **Accept** button to accept the Enterprise BYOD policies.

   FIGURE 60 Enterprise User Agreement

   Pulse Secure

   Enterprise User Agreement

   You must follow all Enterprise BYOD policies with this device.

   The **Set Up Your Profile** page appears.

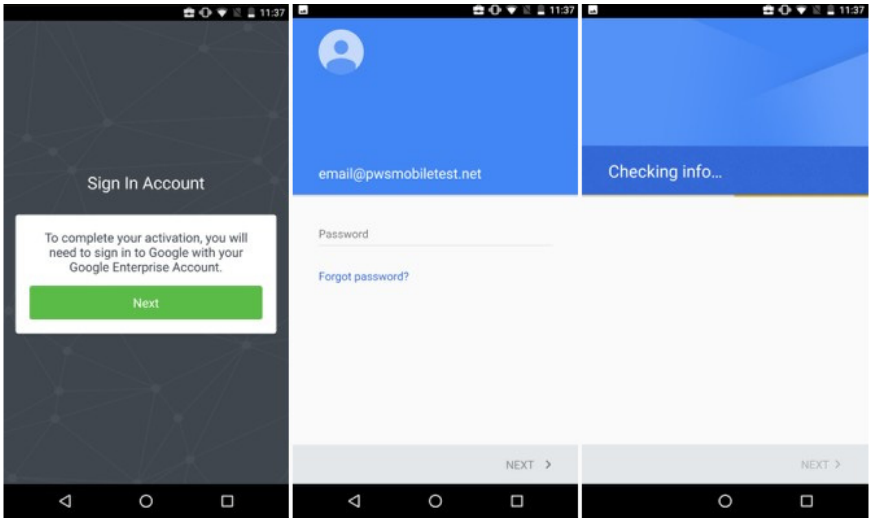
7. Click **Setup** and confirm with **OK**.

   Note: If the device is not encrypted, Google will prompt to encrypt the device with encrypt option and then will reboot the device.

8. You must now sign in to your Google account.

    - If the user's Google account does not exist, then user is prompted with the **Create Account** page.
    - If the Google account exists, the user is taken to the **Signing in Account** page. Press **NEXT** to sign into Google with your Google Enterprise Account.

FIGURE 61 Google Account

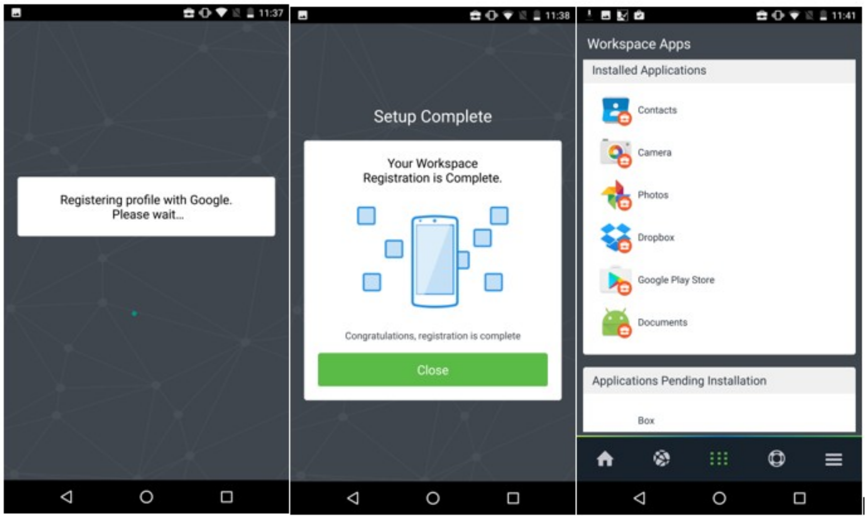


Sign In Account

To complete your activation, you will need to sign in to Google with your Google Enterprise Account.

9. After the Workspace registration is complete, the Workspace Apps will be installed automatically in the background.

FIGURE 62 Workspace Apps



Registering profile with Google. Please wait...

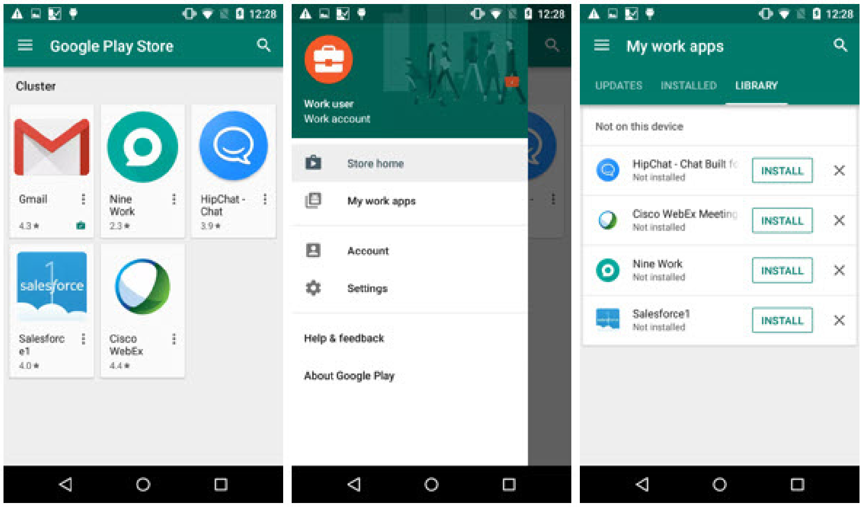
Setup Complete

Your Workspace Registration is Complete.

Congratulations, registration is complete

10. To install optional apps, select **Google Play Store > My Work Apps > Library** (This navigation option may vary from device to device).

FIGURE 63 Workspace Apps Library



Configuring Corporate-Owned iOS Devices

The Apple Deployment Program (ADP) enables you to deploy iOS devices that your business has purchased directly from Apple or from a participating Apple Authorized Reseller or carrier.

You can automatically enroll devices in mobile device management (MDM) without having to physically touch or prepare the devices before users get them. The use of MDM minimizes the setup process for users by removing specific steps from the Setup Assistant.

You can also control whether or not the user can remove the MDM profile from the device. For example, you can order the devices from Apple, configure all the management settings, and have the devices shipped directly to the user's home address. After the device is unboxed and activated, the device enrolls in your MDM and all management settings, apps, and books are ready for the user.

After enrolling in the program, administrators log in to the portal, link one or more MDM servers to the ADP account, and then associate specific devices to one of the MDM servers. The devices can then be assigned to users via MDM. After a device is activated, any MDM-specified configurations, restrictions, or controls are automatically installed.

- **"Enrolling in Apple Deployment Programs" on page 61**.
- **"Adding the Pulse Secure Application to the App Catalog" on page 62**.
- **"Setting Up the Apple Deployment Program" on page 62**.
- **"Enrolling an iOS Device" on page 71**.

Enrolling in Apple Deployment Programs

Before you begin using Apple Deployment Programs (ADP), you first need to enroll in the program. You must have the signing authority to enroll on behalf of your business or institution, as you will be responsible for agreeing to the terms and conditions for each program you access within ADP.

Note: Refer to Apple's **Device Enrollment Support Page** for the details of prerequisite steps for enrollment in the program.

To enroll in Apple Deployment Programs:

1. Go to the **Apple Deployment Programs** portal on your browser.
2. Create an agent account and provide an email address associated with your business or institution. This email address will be used to create your ADP Apple ID, which is required before signing into ADP.
3. Enable two-steps verification. A recovery key is sent, which you need to retain in case you forget your password or lose access to your devices. An email is sent when two-steps verification is enabled.
4. Provide additional business or institution information such as verification contact, business or institution information, Apple customer number, Reseller ID, and Customer ID.

Adding the Pulse Secure Application to the App Catalog

Before provisioning the device, you need to add the Pulse Secure iOS application to the App Catalog. To add the Pulse Secure application to app catalog, refer to **"Adding an iOS App to the App Catalog Manually" on page 154**, using the following app information:

- **Package**: *net.pulsesecure.pulsesecure*
- **App Location**: *Enter Download URL*
- **Download URL**: *https://itunes.apple.com/in/app/pulse-secure/id945832041?mt=8*
- **Title**: *Pulse Secure*
- **Creator**: *Pulse Secure*

Setting Up the Apple Deployment Program

After your enrollment is complete, go to the **Apple Deployment Programs** portal to prepare settings for your institutionally-owned devices. Complete the following steps:

1. Add administrator accounts for individuals who are authorized by your business to access the portal.
2. From the ADP portal, establish a virtual server for your MDM server or servers. Virtual servers in ADP are linked to your physical MDM servers. Each server must be known to Apple and authorized to manage your devices. A two-steps verification process is used to securely authorize an MDM server.
3. Assign devices to your virtual MDM servers by order number or by serial number. Only eligible devices will be available for assignment to your MDM server. You can also download a comma-separated value (CSV) file that contains the full list of all unassigned devices in a specific order.
4. After virtual MDM servers are set up and devices are assigned to them, you can review several aspects of your device assignment, including: Date of the assignment, Order numbers, Name of the MDM server to which the devices are assigned, Total number of devices, separated by device type. You can also download a CSV file containing all the serial numbers of the devices assigned to each MDM server.

This section describes the following procedures:

- **"Adding Administrators for ADP" on page 63**.
- **"Configuring for ADP on Pulse Workspace" on page 64**.
- **"Configuring the ADP Profile" on page 69**.
- **"Managing ADP Devices" on page 70**.
- **"Configuring Pulse Workspace for User Authentication" on page 71**.
- **"Enrolling an iOS Device" on page 71**.
- **"Renewing an Expired Apple Server Token" on page 73**.

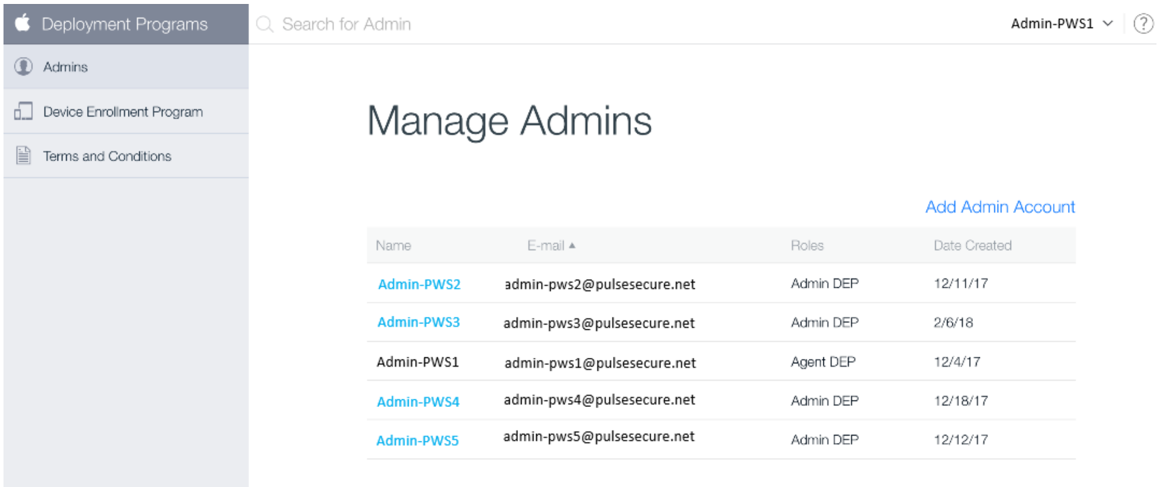
Adding Administrators for ADP

After you are enrolled to Apple Deployment Programs (ADP), you will be able to add additional administrator accounts for individuals who are authorized by your business or institution to access the portal.

To add administrator accounts:

1. Select **Admins** in the Apple Deployment Program portal.

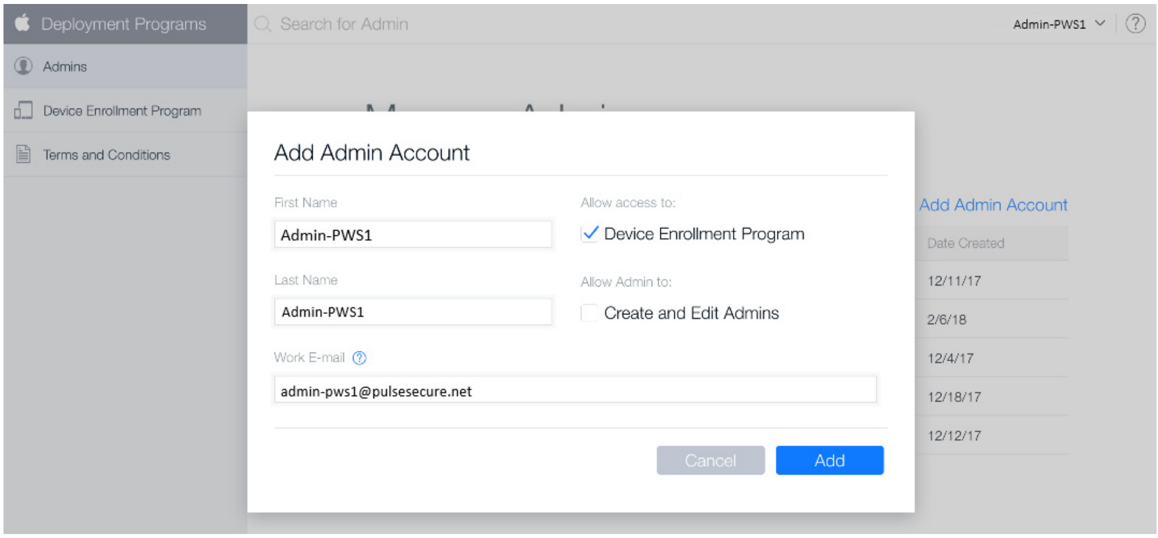
FIGURE 64 Apple Deployment Portal: Manage Admins



Name	E-mail ▲	Roles	Date Created
Admin-PWS2	admin-pws2@pulsesecure.net	Admin DEP	12/11/17
Admin-PWS3	admin-pws3@pulsesecure.net	Admin DEP	2/6/18
Admin-PWS1	admin-pws1@pulsesecure.net	Agent DEP	12/4/17
Admin-PWS4	admin-pws4@pulsesecure.net	Admin DEP	12/18/17
Admin-PWS5	admin-pws5@pulsesecure.net	Admin DEP	12/12/17

2. On the right-hand side, select **Add Admin Account**.

FIGURE 65 Apple Deployment Portal: Add Admin Account



Add Admin Account

First Name: Admin-PWS1

Last Name: Admin-PWS1

Work E-mail: admin-pws1@pulsesecure.net

Allow access to: ☑ Device Enrollment Program

Allow Admin to: □ Create and Edit Admins

3. Enter the admin details and click **Add**.

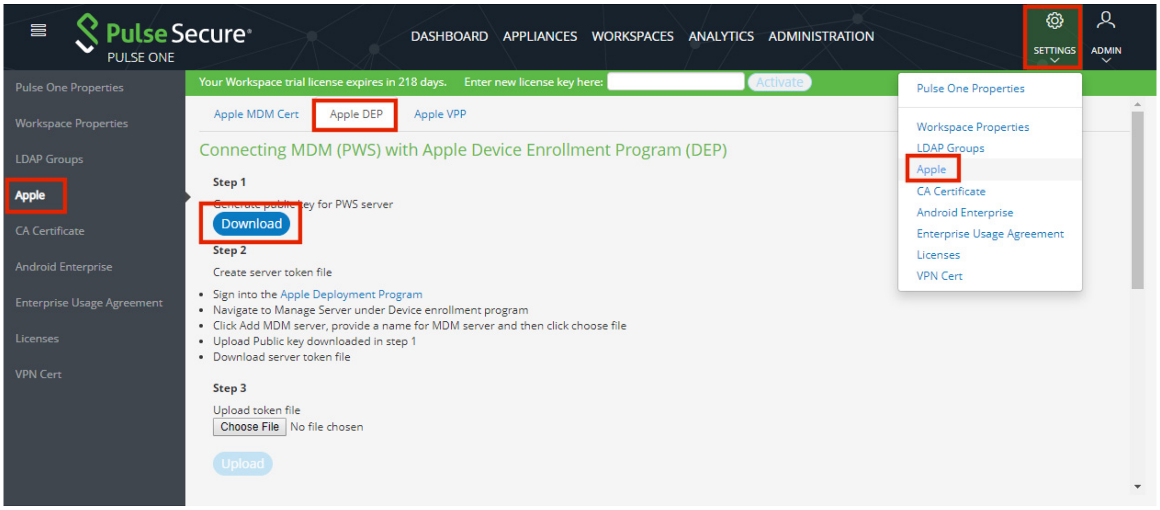
Configuring for ADP on Pulse Workspace

IT Administrators can configure multiple ADPs on Pulse Workspace server.

Before you start, you must download the public key certificate file from Pulse Workspace.

1. Log into Pulse Workspace.
2. Select **Settings > Apple** and select the **Apple DEP** tab.

FIGURE 66 Downloading Public Key



Your Workspace trial license expires in 218 days. Enter new license key here:

Connecting MDM (PWS) with Apple Device Enrollment Program (DEP)

Step 1

Generate public key for PWS server

Download

Step 2

Create server token file

- Sign into the Apple Deployment Program
- Navigate to Manage Server under Device enrollment program
- Click Add MDM server, provide a name for MDM server and then click choose file
- Upload Public key downloaded in step 1
- Download server token file

Step 3

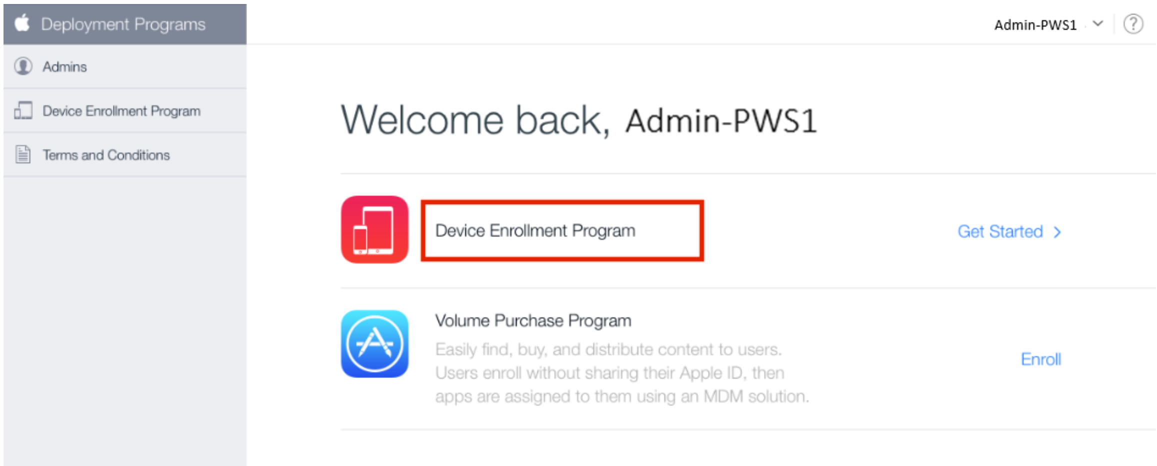
Upload token file

Choose File No file chosen

Upload

3. Select **Download** and save the public key file locally.
4. Access the Apple Deployment Program portal in your browser, and log in.
5. Select **Device Enrollment Program**.

FIGURE 67 Apple Deployment Portal: Deployment Programs



Welcome back, Admin-PWS1

Device Enrollment Program

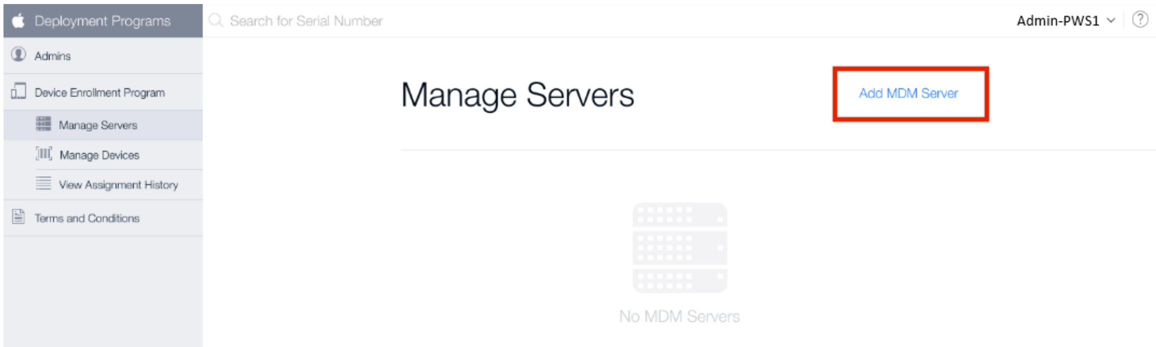
Volume Purchase Program

Easily find, buy, and distribute content to users. Users enroll without sharing their Apple ID, then apps are assigned to them using an MDM solution.

6. Select **Manage Servers**.

   The **Manage Servers** page appears.

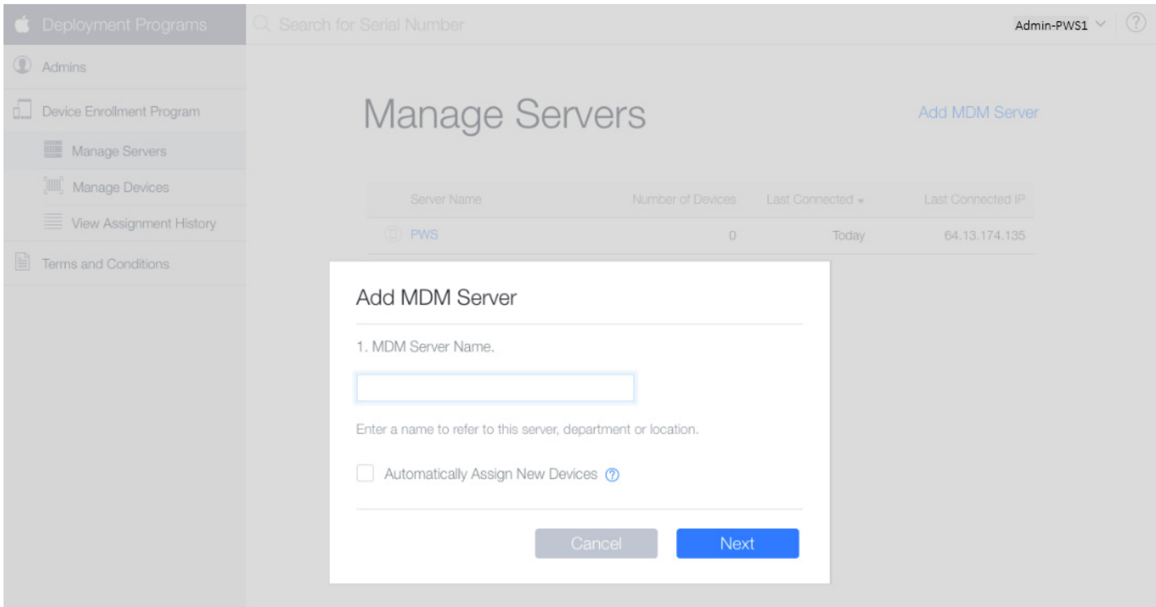
FIGURE 68 Apple Deployment Program: Manage Servers



7. Click **Add MDM Server**.

   The **Add MDM Server** dialog appears.

FIGURE 69 Apple Deployment Program: Add MDM Server



Server Name	Number of Devices	Last Connected	Last Connected IP
PWS	0	Today	64.13.174.135

Add MDM Server

1. MDM Server Name.

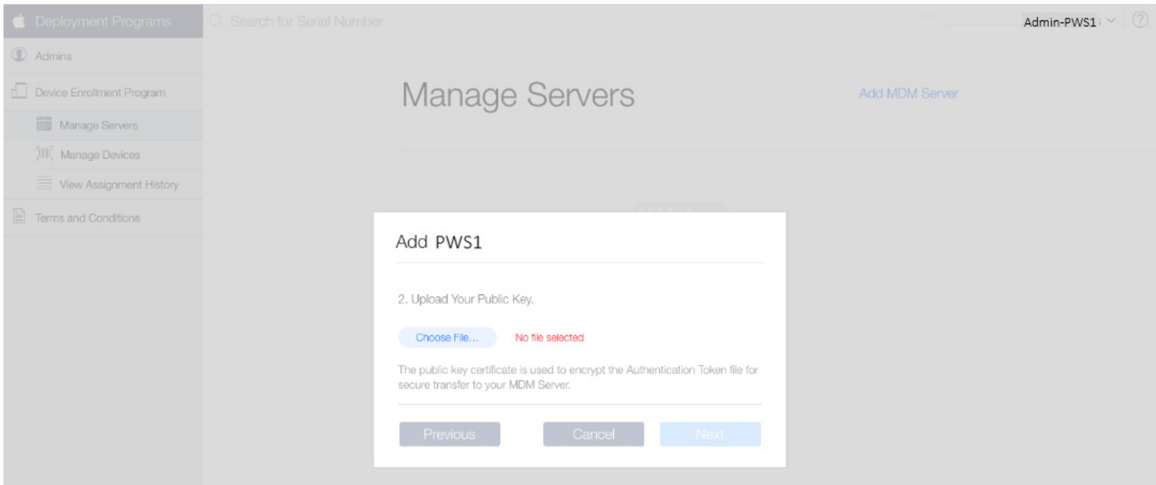
Enter a name to refer to this server, department or location.

☐ Automatically Assign New Devices

8. Enter an **MDM Server Name** for the Pulse Workspace server and click **Next**.

   The dialog updates.

   FIGURE 70 Apple Deployment Program: Upload Public Key



Add PWS1

2. Upload Your Public Key.

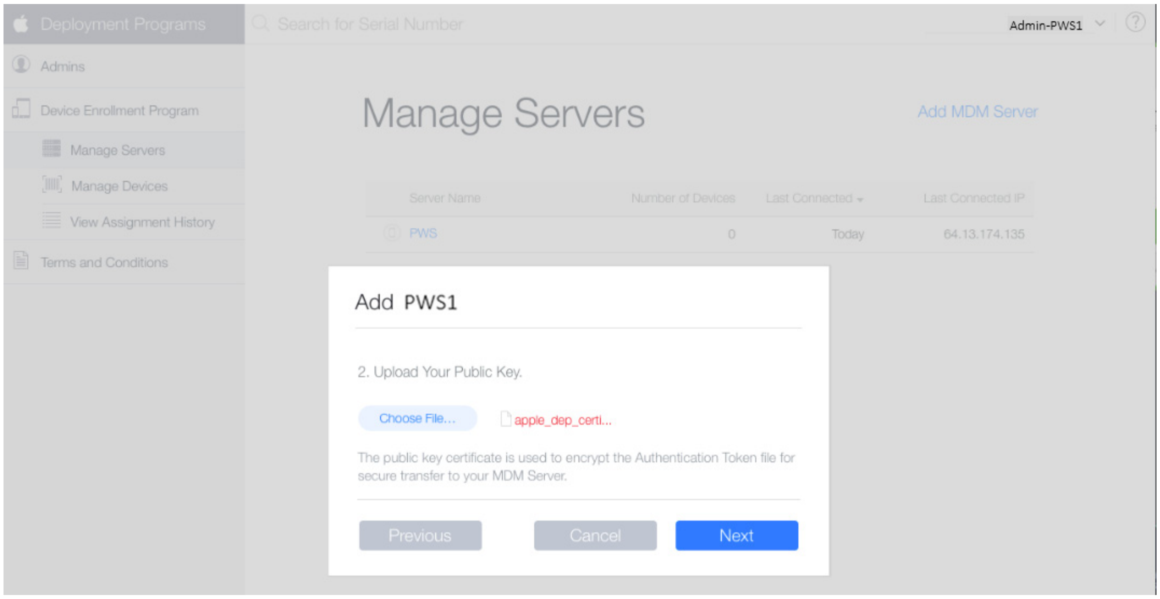
No file selected

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

9. Click **Choose File**, and select the public key file.

   The dialog updates.

   FIGURE 71 Apple Deployment Program: Upload Public Key



Server Name	Number of Devices	Last Connected	Last Connected IP
PWS	0	Today	64.13.174.135

Add PWS1

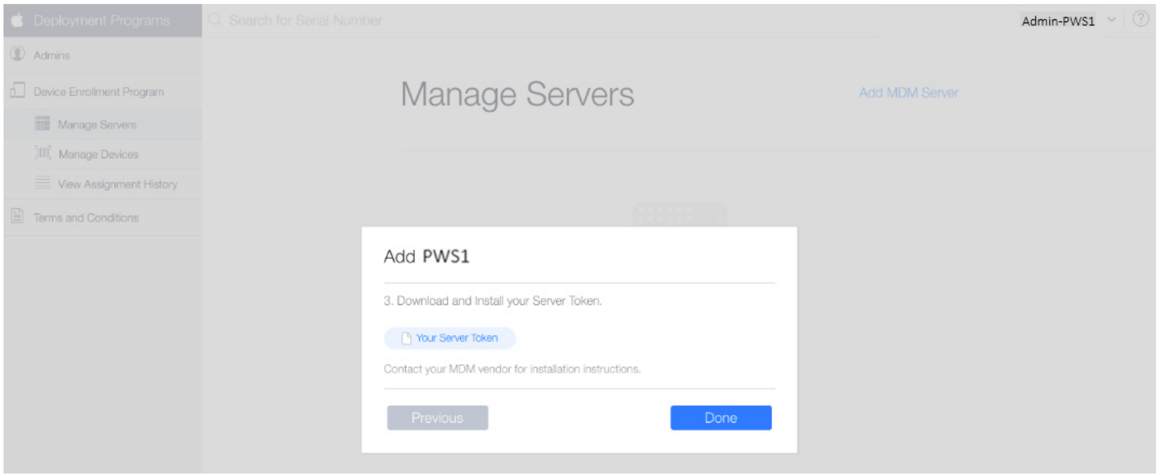
2. Upload Your Public Key.

apple_dep_certi...

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

10. Click **Next**.

FIGURE 72 Apple Deployment Program: Download Server Token



Add PWS1

3. Download and Install your Server Token.

Your Server Token

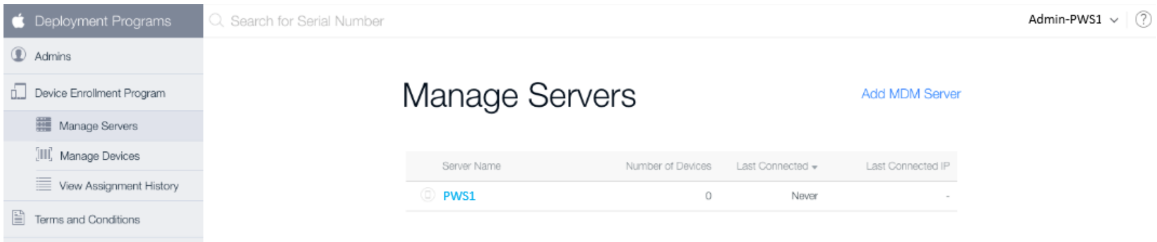
Contact your MDM vendor for installation instructions.

11. Click **Your Server Token** and save the token file locally.

12. Click **Done**.

The server is added successfully.

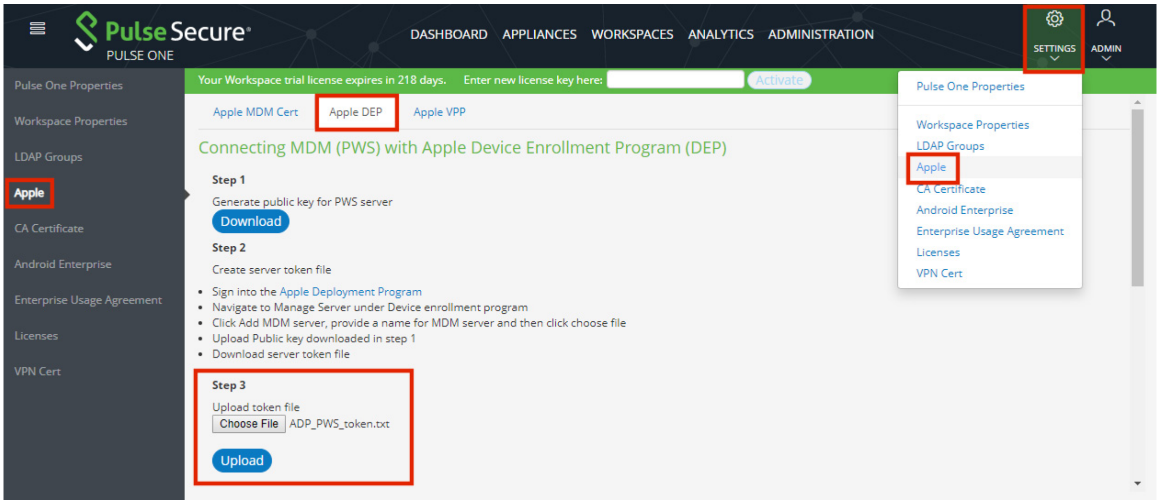
FIGURE 73 Apple Deployment Program: Server Added



Server Name	Number of Devices	Last Connected	Last Connected IP
PWS1	0	Never	-

13. On Pulse One, return to the **Apple DEP** tab.

FIGURE 74 Apple Deployment Program: Upload Token



Your Workspace trial license expires in 218 days. Enter new license key here:

Connecting MDM (PWS) with Apple Device Enrollment Program (DEP)

Step 1

Generate public key for PWS server

Step 2

Create server token file

- Sign into the Apple Deployment Program
- Navigate to Manage Server under Device enrollment program
- Click Add MDM server, provide a name for MDM server and then click choose file
- Upload Public key downloaded in step 1
- Download server token file

Step 3

Upload token file

ADP_PWS_token.txt

14. Click **Choose File** and locate the server token file.

15. **Upload** the server token.

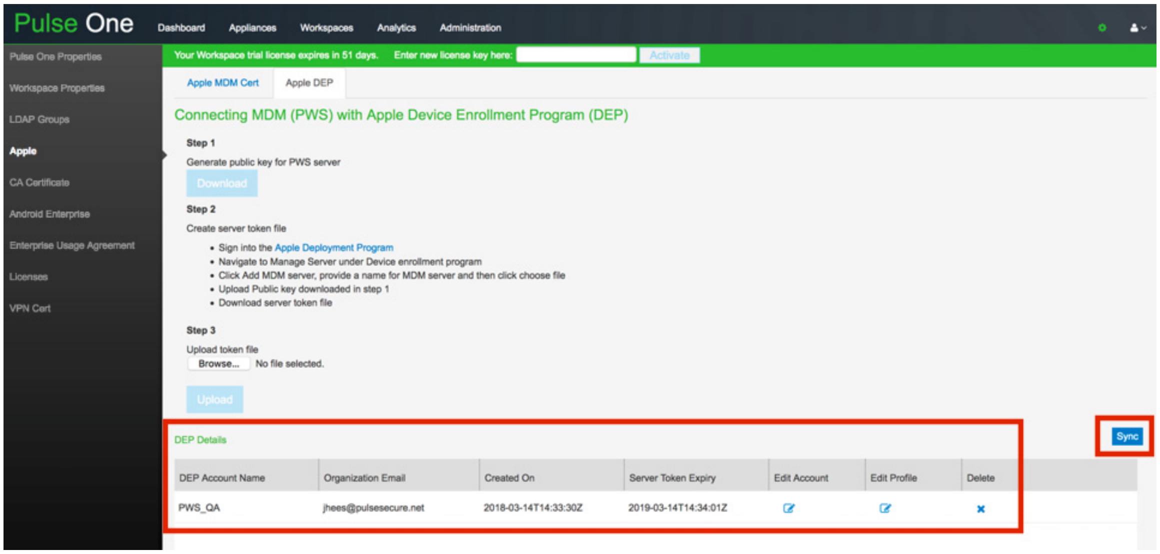
    After successful upload of the server token, the ADP profile page is displayed.

16. Make necessary configuration and click **Save**.

    Note: For configuration details, see **"Configuring the ADP Profile" on page 69**.

    The details are displayed in the Pulse Workspace console.

    FIGURE 75 Sync ADP Account Information



Your Workspace trial license expires in 51 days. Enter new license key here:

Connecting MDM (PWS) with Apple Device Enrollment Program (DEP)

Step 1

Generate public key for PWS server

Step 2

Create server token file

- Sign into the Apple Deployment Program
- Navigate to Manage Server under Device enrollment program
- Click Add MDM server, provide a name for MDM server and then click choose file
- Upload Public key downloaded in step 1
- Download server token file

Step 3

Upload token file

No file selected.

DEP Details

DEP Account Name	Organization Email	Created On	Server Token Expiry	Edit Account	Edit Profile	Delete
PWS_QA	jhees@pulsesecure.net	2018-03-14T14:33:30Z	2019-03-14T14:34:01Z	✎	✎	✖

17. Click the **Sync** button to sync the ADP account information with ADP portal.

    A confirmation dialog appears.

18. In the confirmation dialog, click **Yes**.

    Your account info will then be synchronized with the ADP portal.

    Pulse Workspace will sync automatically with the ADP portal one per hour.

Configuring the ADP Profile

IT Administrators configure the ADP enrollment profile that must be pushed to devices. This profile includes:

- **Name**: The name of the device enrollment profile. This is not visible to user.
- **Description**: The description of the device enrollment profile. This is not visible to user.
- **Department**: This information appears when users click About Configuration during activation.
- **Support Phone Number**: This information appears when the user clicks Need Help during activation.
- **Preparation Mode**: This state is set during enrollment and cannot be changed without factory reset of device:
  - *Supervised.*

    Note: This setting enables **Lock Enrollment profile to device** to be enabled.
  - *Unsupervised*
- **Lock Enrollment profile to device**:
  - *Enable* - disable management profile to be removed from settings.

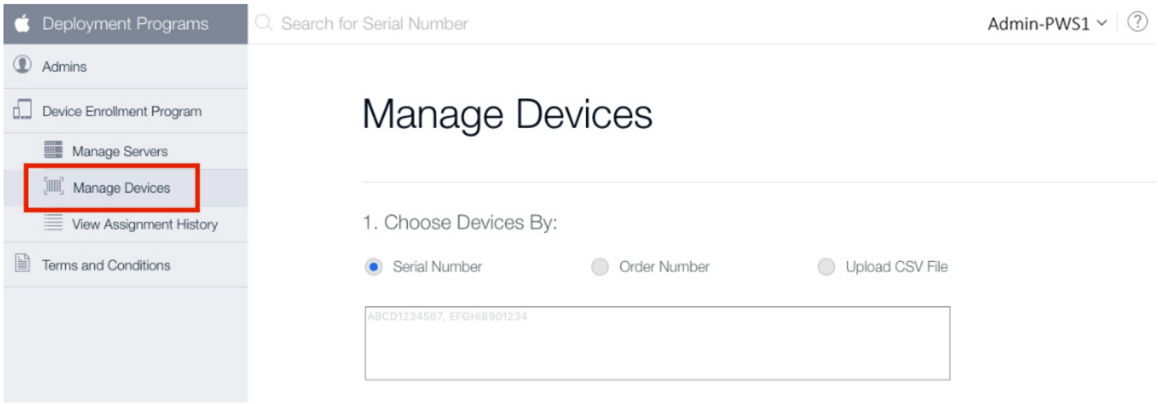
    Note: This setting requires **Preparation Mode** to be *Supervised*.
  - *Disable* - allows the management profile to be removed.
- **Setup Assistance**: Configures the settings that customize iOS setup assistance. The following settings are enabled:
  - *Passcode* - Prompt for passcode during activation.
  - *Location Services* - Prompt for the location service during activation.
  - *Restore* - Prompt for iCloud backup during activation.
  - *Apple ID* - Prompt users for an Apple ID when PWS attempts to install an app without an ID.
  - *Terms and Conditions* - Prompt users to accept Apple's terms and conditions during activation.
  - *Touch ID* - Prompt for Touch ID service during activation.
  - *Apple Pay* - Prompt for Apple pay service during activation.
  - *Zoom* - Prompt for Zoom service during activation.
  - *Siri* - Prompt for Siri service during activation.
  - *Send diagnostic data to Apple* - Prompt for this service during activation.

Managing ADP Devices

With the release of iOS 11, Apple provided businesses a means to add any existing iOS device to their Apple Deployment Program (ADP) account. You can add a device using Apple Configurator 2.5 or later and a wired connection to the iOS device. Apple Configurator can be downloaded from the Apple App Store.

1. Access the Apple Deployment Program portal in your browser, and log in.
2. Select **Manage Devices**.
3. Under **Choose Devices By**, select the method to define ADP enabled devices - **Serial Number**, **Order Number** or **Upload CSV File**.

FIGURE 76 Apple Deployment Programs: Choose Devices By



Manage Devices

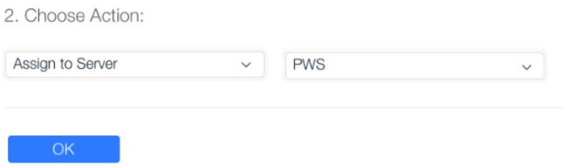
1. Choose Devices By:

● Serial Number ○ Order Number ○ Upload CSV File

ABCD1234567, EFGH8901234

4. Under **Choose Action**, select *Assign to Server*, and then select the configured MDM (PWS) server from the list.

FIGURE 77 Apple Deployment Programs: Select Configured MDM Server



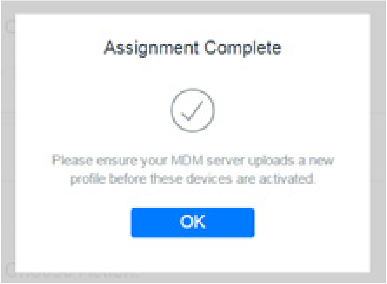
2. Choose Action:

Assign to Server | PWS

5. Click **OK**.

   A confirmation message appears. For example:

FIGURE 78 Apple Deployment Programs: MDM Server Complete



Assignment Complete

Please ensure your MDM server uploads a new profile before these devices are activated.

Configuring Pulse Workspace for User Authentication

This section describes Pulse Workspace configuration for SAML-based and Pin-based user authentication.

SAML-based Authentication

Pulse Workspace uses SAML authentication when SAML authentication is enabled, see the "Configuring Enterprise SSO Using SAML" chapter of the *Pulse One Administration Guide*.

When SAML is enabled, Pulse Workspace sends a login request to Pulse Connect Secure to verify the user.

To configure Pulse Workspace for SAML-based authentication, do the following:

1. Follow the steps described in the "Configuring Enterprise SSO Using SAML" chapter of the *Pulse One Administration Guide*.
2. On Pulse Workspace, navigate to **Settings > Apple > Apple DEP > Edit Profile**.
3. Provide the PCS Sign-In URL for SAML authentication and click **Save**.

   Note: For details about PCS Sign-In URL, refer to the "Sign-In Policies" chapter in the *Pulse Connect Secure Administration Guide*.

PIN-based Authentication

Pulse Workspace uses PIN-based authentication when SAML authentication is disabled, see the "Configuring Enterprise SSO Using SAML" chapter of the *Pulse One Administration Guide*.

To prepare Pulse Workspace for Pin-based authentication, do the following:

1. In Pulse Workspace, navigate to **Workspaces > Devices > Users**.
2. For each end user, create the required user/workspace, see **"Adding a User" on page 139**.

   Note: Retain the registration key for provisioning.

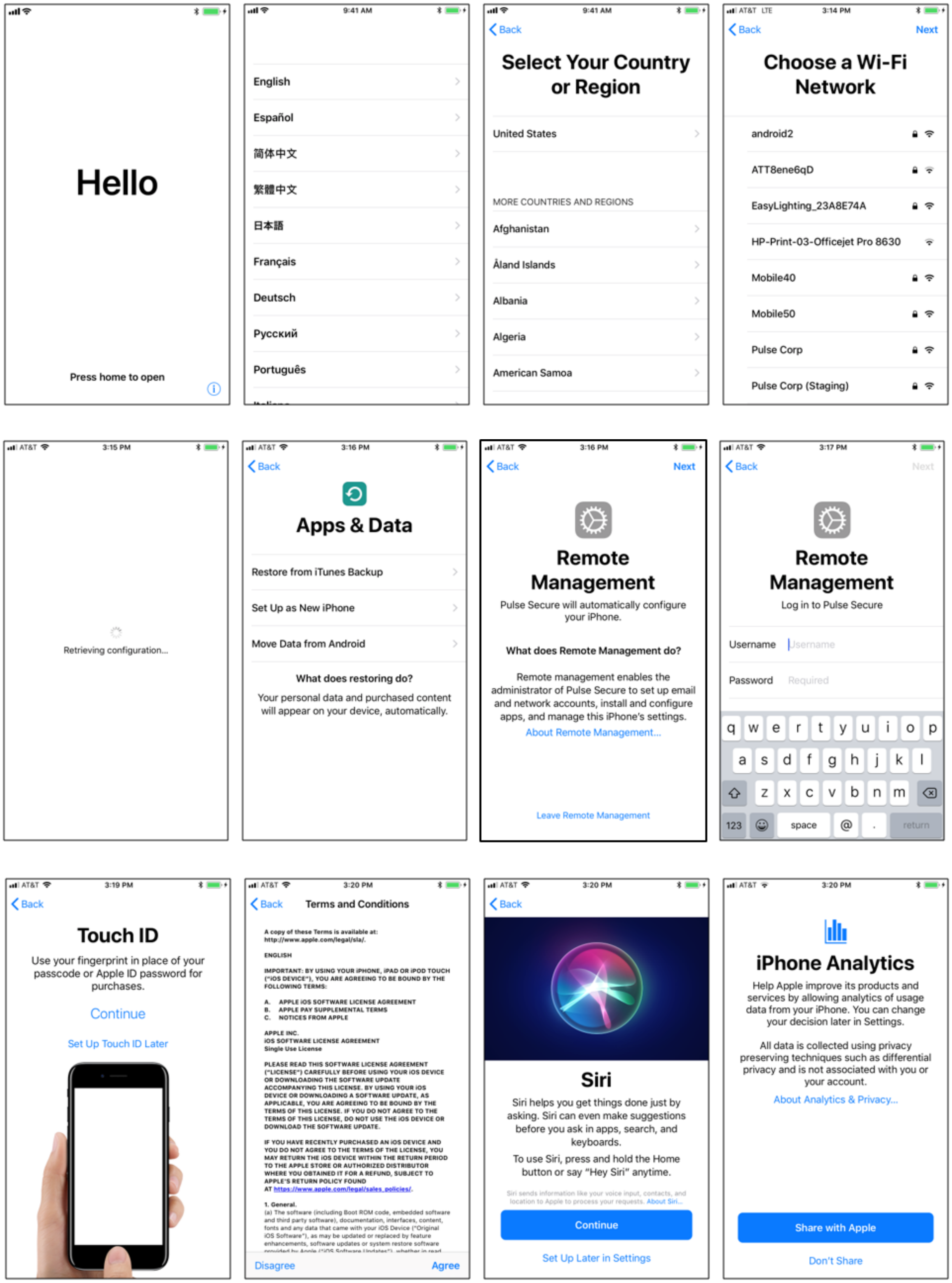
Enrolling an iOS Device

Once you have configured ADP for use, a registered end user can enroll an iOS device.

To do this, the user must power up the device, and follow the on-screen instructions through to completion.

For example:

FIGURE 79 iOS ADP Enrollment User Experience



What does restoring do?

Your personal data and purchased content will appear on your device, automatically.

Pulse Secure will automatically configure your iPhone.

What does Remote Management do?

Remote management enables the administrator of Pulse Secure to set up email and network accounts, install and configure apps, and manage this iPhone's settings.

Use your fingerprint in place of your passcode or Apple ID password for purchases.

A copy of these Terms is available at:
http://www.apple.com/legal/sla/.

ENGLISH

IMPORTANT: BY USING YOUR iPHONE, iPAD OR iPOD TOUCH ("iOS DEVICE"), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS:

A. APPLE iOS SOFTWARE LICENSE AGREEMENT
B. APPLE PAY SUPPLEMENTAL TERMS
C. NOTICES FROM APPLE

APPLE INC.
iOS SOFTWARE LICENSE AGREEMENT
Single Use License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR iOS DEVICE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR iOS DEVICE OR DOWNLOADING A SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE iOS DEVICE OR DOWNLOAD THE SOFTWARE UPDATE.

IF YOU HAVE RECENTLY PURCHASED AN iOS DEVICE AND YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE iOS DEVICE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT https://www.apple.com/legal/sales_policies/.

1. General.
(a) The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with your iOS Device ("Original iOS Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("iOS Software Updates"), whether in read

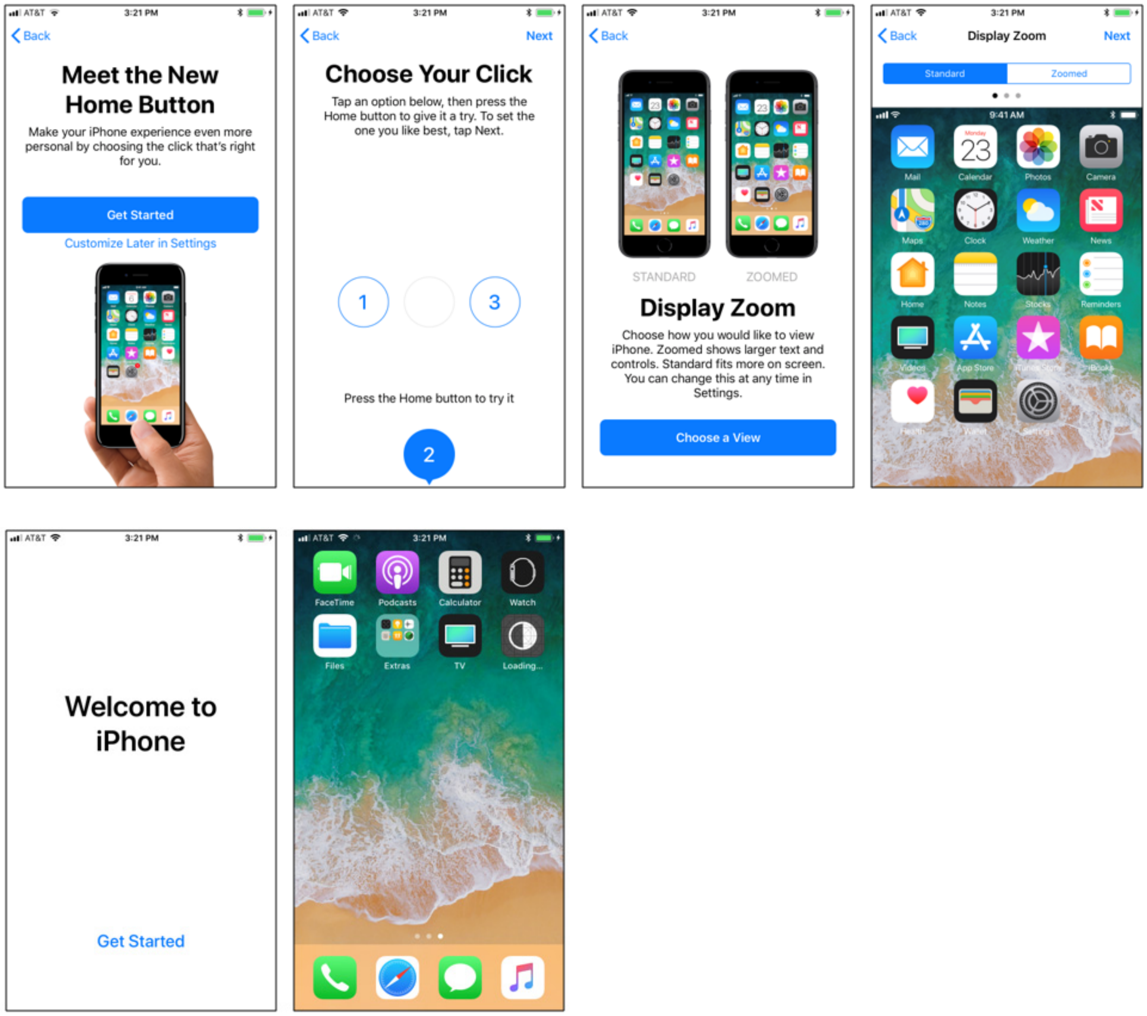
Siri helps you get things done just by asking. Siri can even make suggestions before you ask in apps, search, and keyboards.

To use Siri, press and hold the Home button or say "Hey Siri" anytime.

Siri sends information like your voice input, contacts, and location to Apple to process your requests. About Siri...

Help Apple improve its products and services by allowing analytics of usage data from your iPhone. You can change your decision later in Settings.

All data is collected using privacy preserving techniques such as differential privacy and is not associated with you or your account.



Meet the New Home Button

Make your iPhone experience even more personal by choosing the click that's right for you.

Choose Your Click

Tap an option below, then press the Home button to give it a try. To set the one you like best, tap Next.

Press the Home button to try it

Display Zoom

Choose how you would like to view iPhone. Zoomed shows larger text and controls. Standard fits more on screen. You can change this at any time in Settings.

Welcome to iPhone

Renewing an Expired Apple Server Token

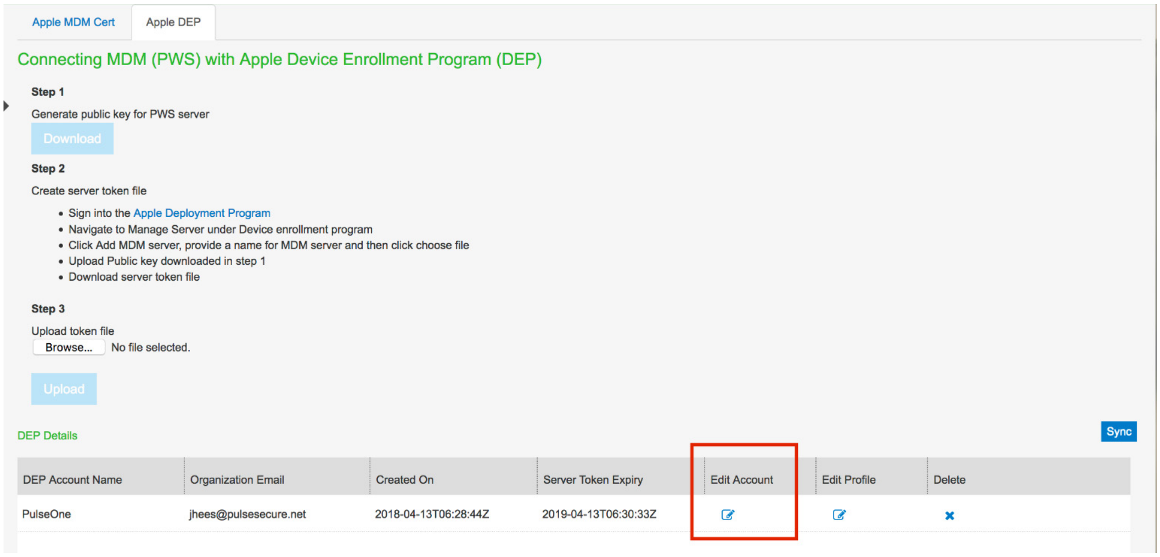
After Configuring ADP with Pulse Workspace, ADP details are displayed in the Pulse Workspace console and server token is valid for one year. Two weeks before the token expires, Pulse Workspace server will send notification to the administrator. In the ADP portal, the administrator can download the new token, and then upload it to Pulse Workspace server to extend the token validity.

To upload the new server token:

1. Log in to Pulse Workspace console.
2. Navigate to **Settings > Apple > Apple DEP**.

3. Click the **Edit Account** icon in the details table.

FIGURE 80 Apple Deployment Program: Connecting MDM



Connecting MDM (PWS) with Apple Device Enrollment Program (DEP)

Step 1

Generate public key for PWS server

Step 2

Create server token file

- Sign into the Apple Deployment Program
- Navigate to Manage Server under Device enrollment program
- Click Add MDM server, provide a name for MDM server and then click choose file
- Upload Public key downloaded in step 1
- Download server token file

Step 3

Upload token file

No file selected.

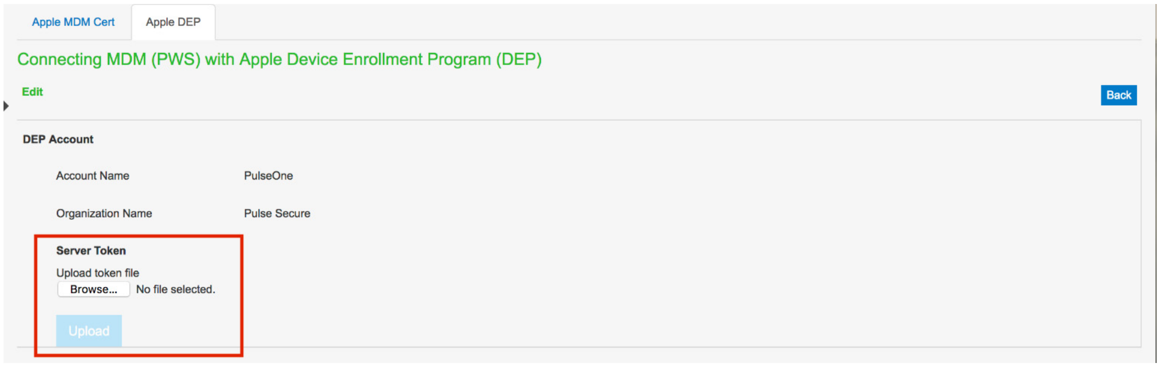
DEP Details

DEP Account Name	Organization Email	Created On	Server Token Expiry	Edit Account	Edit Profile	Delete
PulseOne	jhees@pulsesecure.net	2018-04-13T06:28:44Z	2019-04-13T06:30:33Z	✎	✎	✖

4. In the **Edit** page, click **Browse** and select the new token.

5. Click **Upload**.

FIGURE 81 Apple Deployment Program: Upload Token



Connecting MDM (PWS) with Apple Device Enrollment Program (DEP)

Edit

DEP Account

Account Name	PulseOne
Organization Name	Pulse Secure

Server Token

Upload token file

No file selected.

Configuring Corporate-Owned Android Devices

Pulse One supports Android Corporate-Owned Devices. A corporate-owned device is one that is supplied by your business to the user in a pre-configured state. The behavior of each device is dictated by the applicable policies set for each user by the administrator. The device contains approved apps and data; no personal apps or data are permitted.

Android For Work (AFW) provides a fast, streamlined way to deploy devices that your business has purchased directly from the manufacturer or carrier.

Registering a Corporate-Owned Android Device

The registration and configuration process for a Corporate-Owned Android Device will typically be performed by an administrator before the device is given to the user.

The process begins with a factory reset device. The process will vary to some extent depending on the device's manufacturer (for example: *Sony*, *Samsung*, *Huawei*, and so on) but the general process will remain consistent.

To register a corporate-owned Android device:

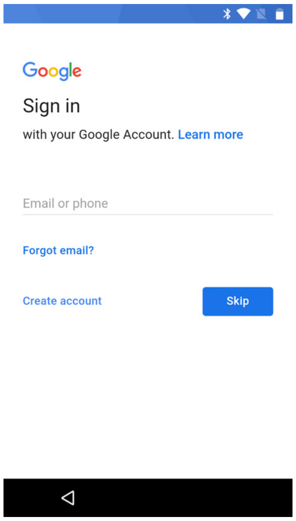
1. Log into the Pulse One appliance.
2. In the **Workspaces** menu, create (or edit) the required user. The user details should include:
   - The user's corporate email as the **Workspace Email**.
   - Your own email as the **Provisioning Email**, so that you receive the required registration information.
   - The required policy **Tags** for the user.
3. Add a user workspace to the user for the device.

   You will receive registration details at your own email address.
4. Power up the factory reset device.

   Specific details of this sequence will vary by manufacturer.
5. Join a WiFi network.

The **Sign In** screen appears.

FIGURE 82 Google Email



Google

Sign in

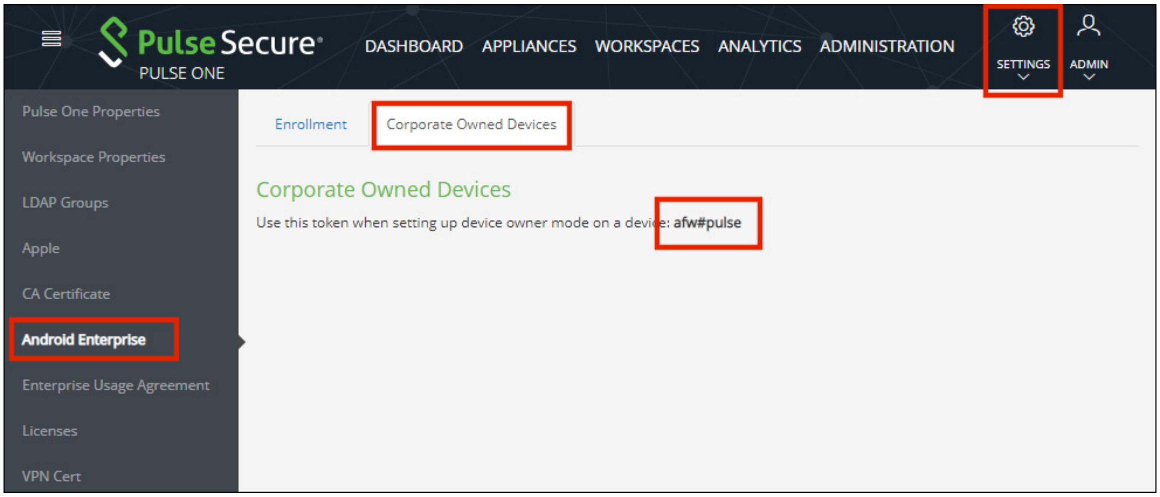
with your Google Account. Learn more

Email or phone

6. Do not enter an email. Instead, enter the value afw#pulse.

   This information is available on the **Android Enterprise** settings page.

FIGURE 83 Android Enterprise Settings



Corporate Owned Devices

Use this token when setting up device owner mode on a device: afw#pulse

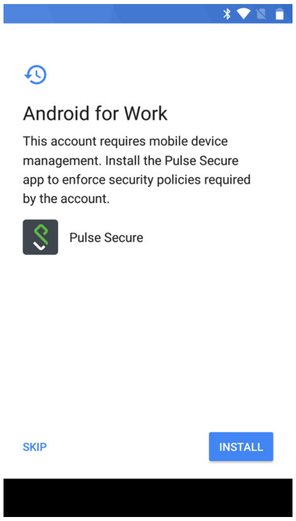
7. On the **Sign In** screen, press **Next**.

   A screen listing Google Services settings appears.

8. Do not change any settings. press **Next**.

   An **Android For Work** screen indicates that Pulse Secure will be used for mobile device management.

   FIGURE 84 Google Email

   Android for Work

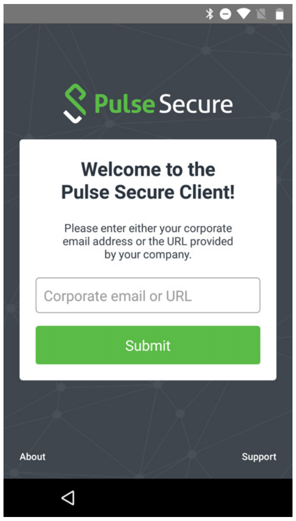
   This account requires mobile device management. Install the Pulse Secure app to enforce security policies required by the account.

9. Click **Install**.

   Pulse Secure downloads and installs.

   The Pulse Secure **Welcome** screen appears.

   FIGURE 85 Welcome

   Welcome to the Pulse Secure Client!

   Please enter either your corporate email address or the URL provided by your company.

10. On the Pulse Secure **Welcome** screen:

    - Enter the Enterprise URL from your welcome email.
    - Click **Submit**.

    The next step depends on whether you have SAML-based authentication.

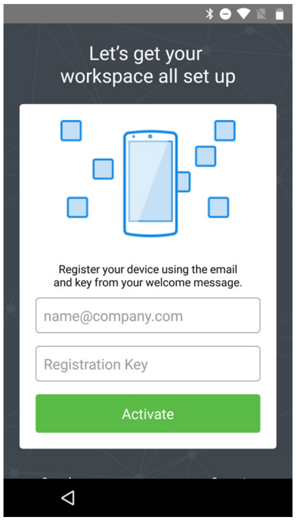
11. (Optional) If you are using a SAML-based registration, the SAML **Login** screen appears.

    On this screen, enter your corporate user name and password and click **Sign In**.

    A BYOD policy **Enterprise User Agreement** page appears (skip step 12).

12. (Optional) If you are using PIN authentication, the next screen appears. For example:

    FIGURE 86 Registration Key



Let's get your workspace all set up

Register your device using the email and key from your welcome message.

name@company.com

Registration Key

On this screen:

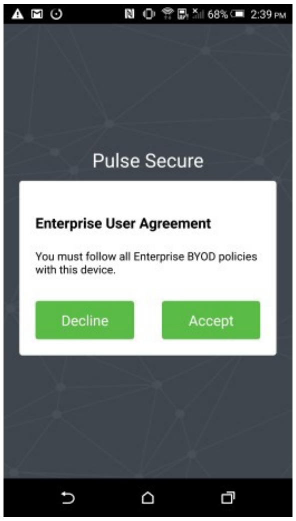
- Enter your corporate email address.
- Enter your registration key from your welcome email.
- Click **Activate**.

The client parses the domain and sends it to a discovery server to fetch the server URL. It then continues with Active Directory (AD) authentication with the server.

A BYOD policy **Enterprise User Agreement** page appears (continue from step 13).

13. On the **Enterprise User Agreement** page, press the **Accept** button to accept the Enterprise BYOD policies.

FIGURE 87 Enterprise User Agreement

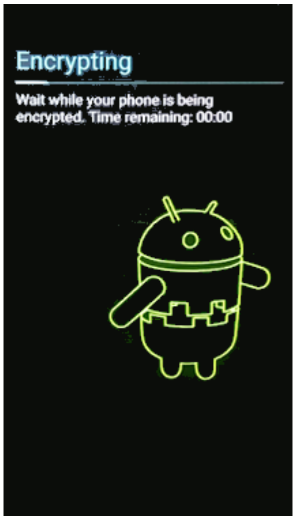


Enterprise User Agreement

You must follow all Enterprise BYOD policies with this device.

14. (Optional) If there is no default encryption on the device, a **Set Up Work Device** page indicates that encryption is required on the device. Click **Encrypt** and confirm until encryption begins. For example:

FIGURE 88 Encrypting



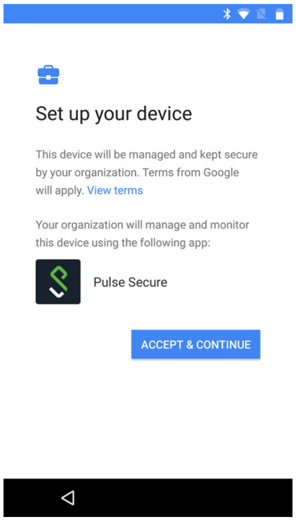
Encrypting

Wait while your phone is being encrypted. Time remaining: 00:00

When encryption completes, the device reboots.

A **Set Up Your Device** screen appears. For example:

FIGURE 89 Set Up Work Device



Set up your device

This device will be managed and kept secure by your organization. Terms from Google will apply. View terms

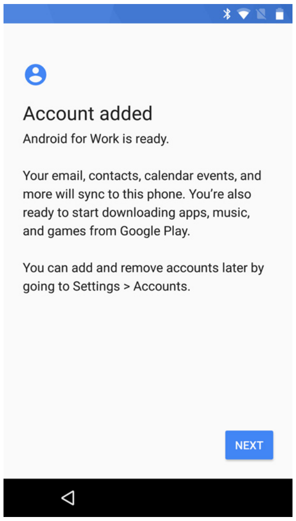
Your organization will manage and monitor this device using the following app:

Pulse Secure

15. Click **Accept and Continue**.

An **Account Added** completion screen for Android For Work appears. For example:

FIGURE 90 Account Added



Account added

Android for Work is ready.

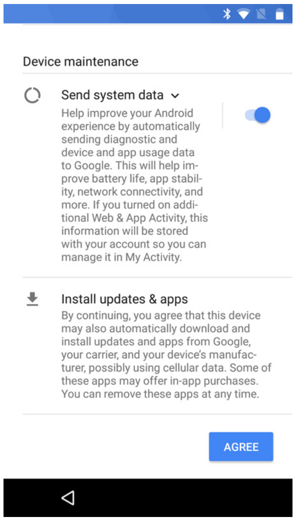
Your email, contacts, calendar events, and more will sync to this phone. You're also ready to start downloading apps, music, and games from Google Play.

You can add and remove accounts later by going to Settings > Accounts.

16. Click **Next**.

A series of screens enable you to complete the configuration of your device. For example:

FIGURE 91 Device Maintenance



Device maintenance

Send system data

Help improve your Android experience by automatically sending diagnostic and device and app usage data to Google. This will help improve battery life, app stability, network connectivity, and more. If you turned on additional Web & App Activity, this information will be stored with your account so you can manage it in My Activity.

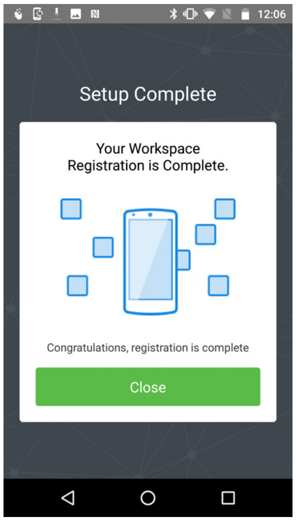
Install updates & apps

By continuing, you agree that this device may also automatically download and install updates and apps from Google, your carrier, and your device's manufacturer, possibly using cellular data. Some of these apps may offer in-app purchases. You can remove these apps at any time.

Work through these screens without making changes.

The **Setup Complete** page then appears.

FIGURE 92 Setup Complete



Setup Complete

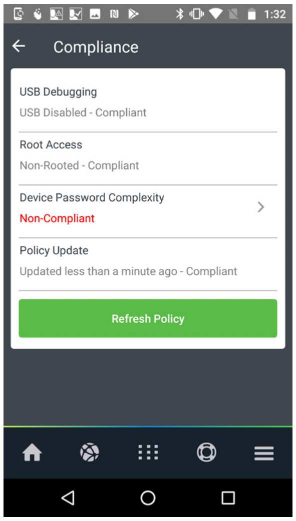
Your Workspace Registration is Complete.

Congratulations, registration is complete

17. Click **Close**.

The **Compliance** page of Pulse Secure then appears. This page presents a list of policy properties, and an indication whether the device is compliant. For example:

FIGURE 93 Compliance



USB Debugging
USB Disabled - Compliant

Root Access
Non-Rooted - Compliant

Device Password Complexity
Non-Compliant

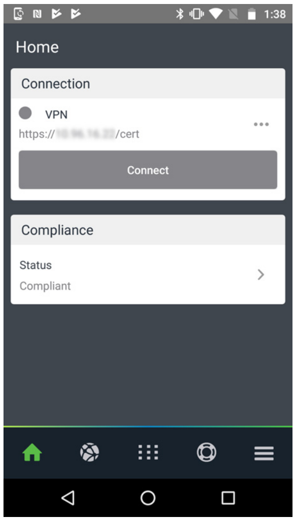
Policy Update
Updated less than a minute ago - Compliant

18. Make any required changes to bring your device into compliance.

    For example, if there is a device password requirement, and no device password is set, you can add a device password to bring the device into compliance.

    After this is complete, the Pulse Secure **Home** page then appears. For example:

FIGURE 94 Home

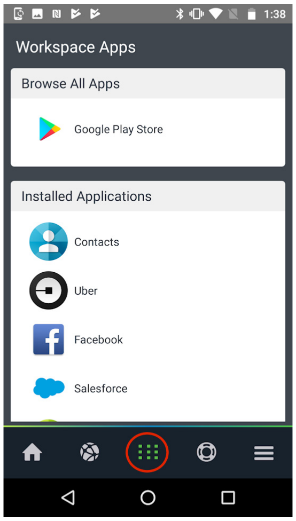


VPN
https://[redacted]/cert

Status
Compliant

19. Press ⠿ to see installed apps. For example:

FIGURE 95 Workspace Apps



Workspace Apps

Browse All Apps

Google Play Store

Installed Applications

Contacts

Uber

Facebook

Salesforce

The registration process is complete.

Configuring LDAP Auto-Provisioning

This section describes the required processes to configure LDAP auto-provisioning:

- “Overview: LDAP Auto-Provisioning” on page 84.
- “Configuring LDAP on Pulse Connect Secure” on page 84.
- “Configuring LDAP Auto-Provisioning” on page 92.

Overview: LDAP Auto-Provisioning

Enterprises manage Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) domain for end users to authenticate/authorize to their corporate resources like Outlook, access Share Point and so on. By implementing LDAP support using Pulse One/Workspace, enterprise end users can provision their device automatically with Pulse One console using their domain account.

Pulse One admins can validate the LDAP groups and map them to respective policies according to the corporate requirement. When end users provision their devices, they get the required policies pushed to device as per their user group membership configuration.

Pulse One server provides the self-registration portal for the enterprise users to submit their email to validate their email domain and user account with backend AD/LDAP server through Appliance. Appliance validates the user account using its account/email to deliver the registration email successfully to the end user's Inbox to proceed with the registration.

Configuring LDAP on Pulse Connect Secure

The LDAP configuration on Pulse Connect Secure includes the following tasks:

- “Creating an LDAP Server” on page 85.
- “Creating a Realm for LDAP” on page 86.
- “Creating a Role and Role Mapping for LDAP” on page 87.
- “Creating Sign-In Policies for LDAP” on page 89.
- “Registering the Appliance for LDAP” on page 90.
- “Selecting the Pulse Workspace Command Handler for LDAP” on page 91.

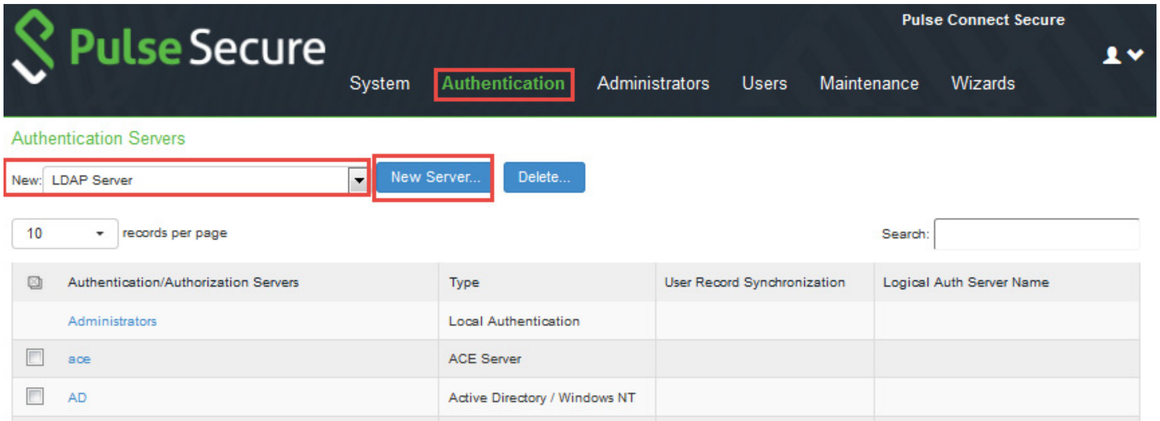
Creating an LDAP Server

To create an LDAP server:

1. Go to **Authentication > Auth Servers > New Server**.

   The **Authentication Servers** page appears.

   FIGURE 96 Create New LDAP Server



New: LDAP Server

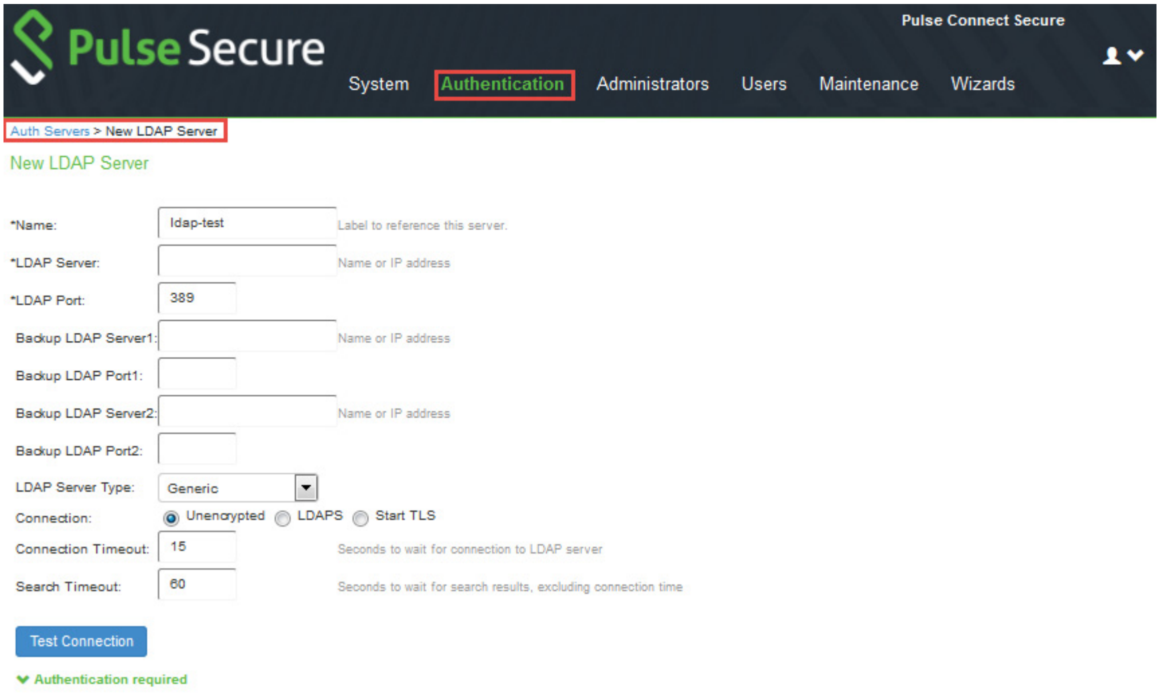
10 records per page

	Authentication/Authorization Servers	Type	User Record Synchronization	Logical Auth Server Name
	Administrators	Local Authentication		
□	ace	ACE Server		
□	AD	Active Directory / Windows NT		

2. Under **New**, select *LDAP Server* and then click **New Server**.

   The **New LDAP Server** page appears.

   FIGURE 97 Configure New LDAP Server



*Name:	ldap-test	Label to reference this server.
*LDAP Server:		Name or IP address
*LDAP Port:	389	
Backup LDAP Server1:		Name or IP address
Backup LDAP Port1:		
Backup LDAP Server2:		Name or IP address
Backup LDAP Port2:		
LDAP Server Type:	Generic	
Connection:	● Unencrypted ○ LDAPS ○ Start TLS	
Connection Timeout:	15	Seconds to wait for connection to LDAP server
Search Timeout:	60	Seconds to wait for search results, excluding connection time

3. Complete the configuration by doing the following:
   - Specify a **Name** to identify the server within the system.
   - Specify the **LDAP Server** hostname or its IP address.
   - Specify the required **LDAP Port** on the LDAP server:
     - **Default port number**: *389* (unencrypted connection).
     - **Default port number**: *636* (SSL connection).

   Note: For more configuration details, refer to the *Pulse Connect Secure Administration Guide*.

After this is complete, you can create a realm that includes the new LDAP server, see **“Creating a Realm for LDAP” on page 86**.

Creating a Realm for LDAP

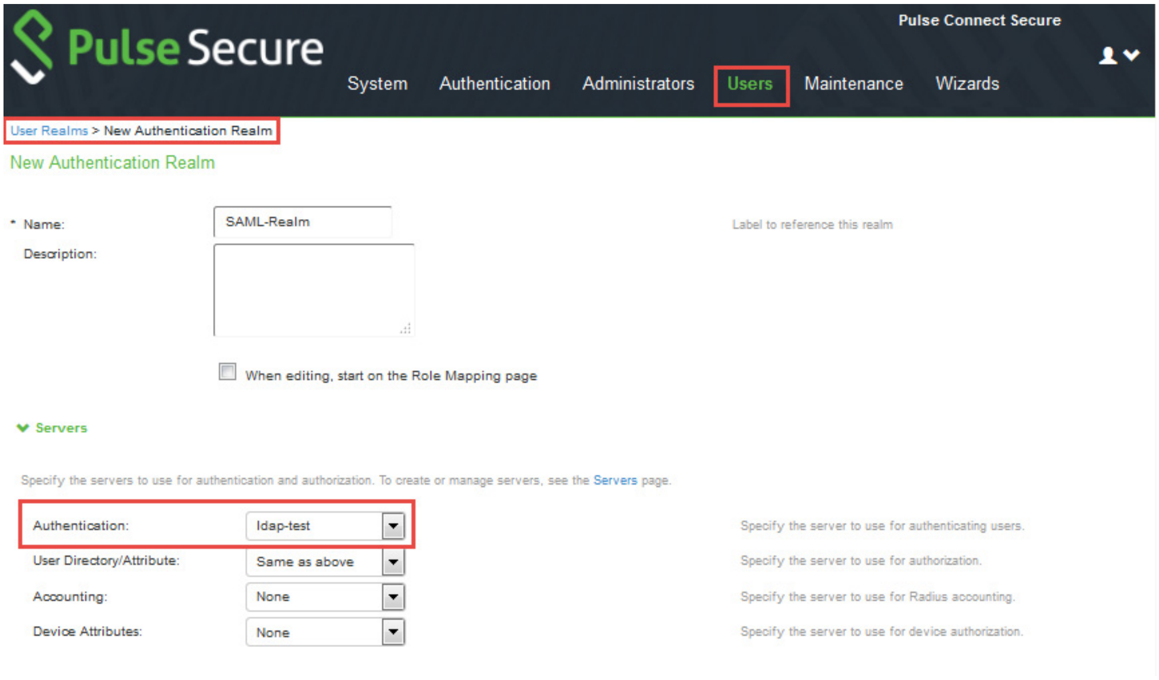
After you have created an LDAP server, you can create a realm that refers to the new server.

To create a realm:

1. Go to **Users > User Realms**.
2. On the **User Realms** page, click **New**.

   The **New Authentication Realms** page appears.

FIGURE 98 Create New Realm



User Realms > New Authentication Realm

New Authentication Realm

* Name:	SAML-Realm	Label to reference this realm
Description:		

□ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication:	ldap-test	Specify the server to use for authenticating users.
User Directory/Attribute:	Same as above	Specify the server to use for authorization.
Accounting:	None	Specify the server to use for Radius accounting.
Device Attributes:	None	Specify the server to use for device authorization.

3. Enter a **Name** to label this realm and (optionally) a **Description**.
4. Under **Servers**, for **Authentication**, select the LDAP server configured in the previous steps.

For more configuration details, refer to the *Pulse Connect Secure Administration Guide*.

After this is complete, you can create a role that includes the new realm, see **"Creating a Role and Role Mapping for LDAP" on page 87**.

Creating a Role and Role Mapping for LDAP

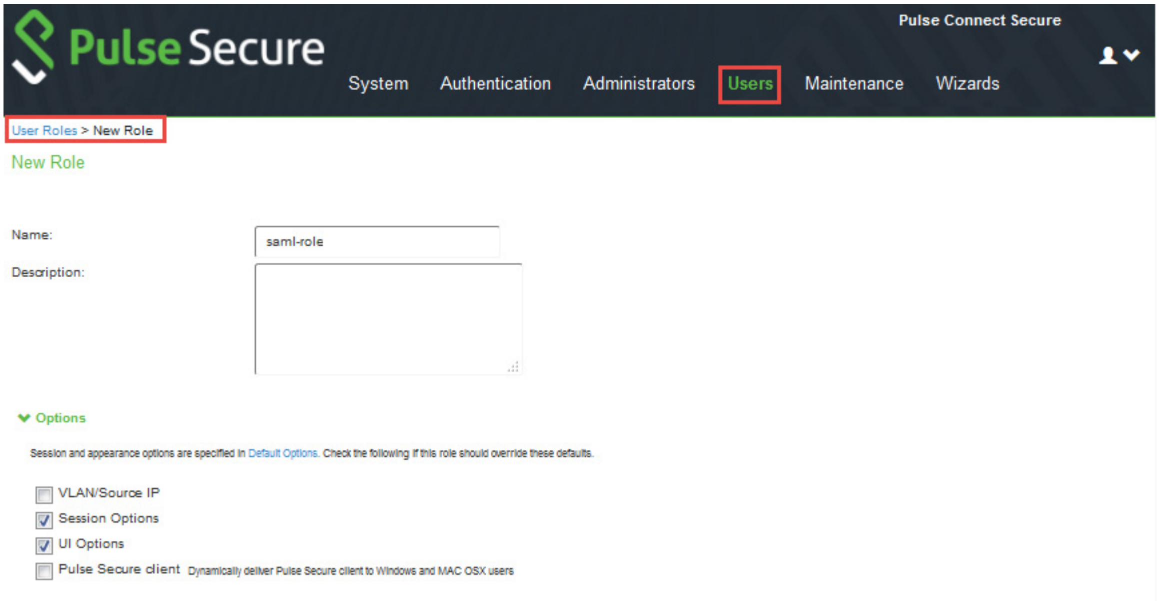
After you have created a realm, you can create a role that refers to the new realm.

To create a role and assign the role to the realm:

1. Go to **Users > User Roles**.
2. Click **New Role**.

   The **New Role** page appears.

   FIGURE 99 Create New Role



New Role

Name: saml-role

Description:

Options

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

☐ VLAN/Source IP
☑ Session Options
☑ UI Options
☐ Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

3. Enter a **Name** and (optionally) a **Description** and create the role.

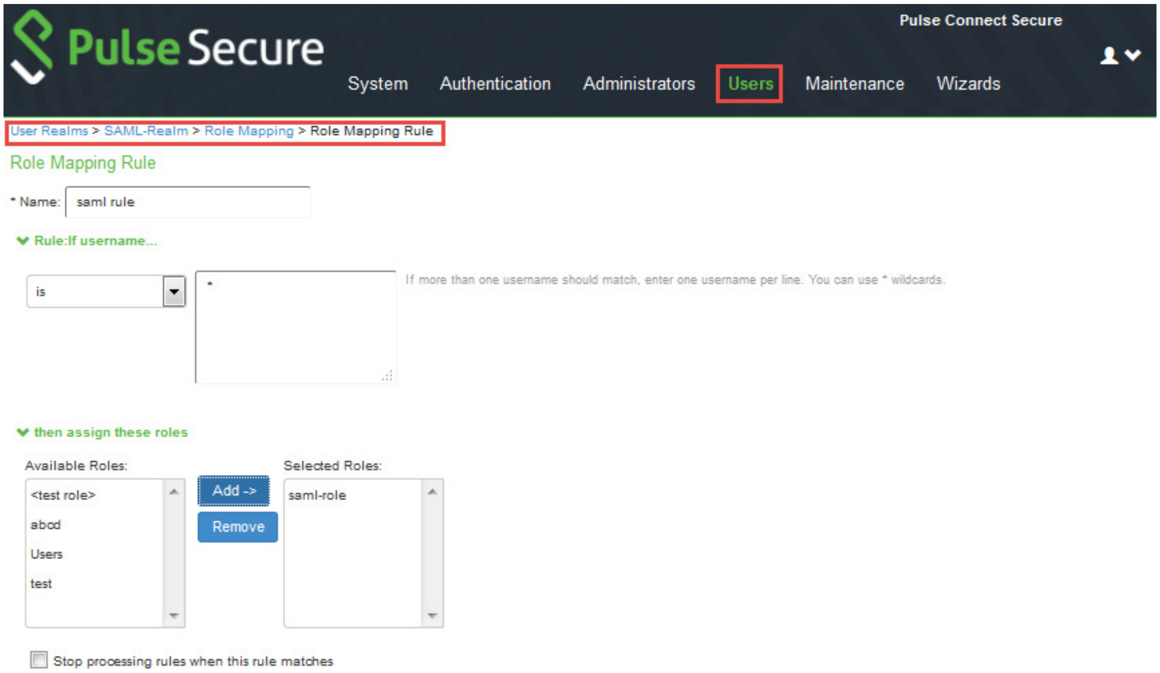
   Note: This name will be used in the list of roles on the **Roles** page.

   Note: For more configuration details, refer to the *Pulse Connect Secure Administration Guide*.

4. After creating the role, select the realm and then click the **Role Mapping** tab.

5. Click **New Rule** to access the **Role Mapping Rule** page.

FIGURE 100 Create Role Mapping Rule



User Realms > SAML-Realm > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name: saml rule

Rule:If username...

is

*

If more than one username should match, enter one username per line. You can use * wildcards.

then assign these roles

Available Roles:	Selected Roles:
<test role> abcd Users test	saml-role

□ Stop processing rules when this rule matches

Note: This page provides an in-line editor for defining the rule.

6. Specify a rule **Name**.

   Note: For more configuration details, refer to the *Pulse Connect Secure Administration Guide*.

7. Save the rule.

After this is complete, you can create a sign-in policy, see **“Creating Sign-In Policies for LDAP” on page 89**.

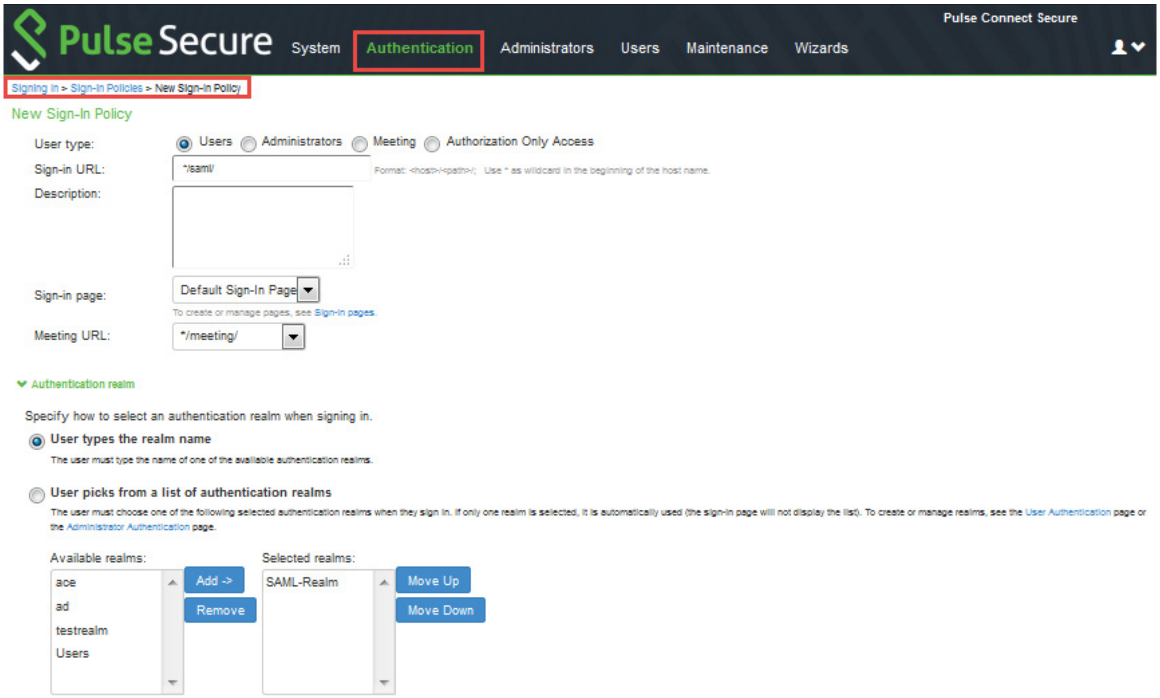
Creating Sign-In Policies for LDAP

To create Sign-in URL, do the following:

1. Go to **Authentication > Sign-in Policies**.

2. Create a new sign-in policy and attach the new realm created in **"Creating a Realm for LDAP" on page 86**.

FIGURE 101 Create Sign-In URL



New Sign-In Policy

User type: ● Users ○ Administrators ○ Meeting ○ Authorization Only Access

Sign-in URL: */saml/ Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: Default Sign-In Page

To create or manage pages, see Sign-in pages.

Meeting URL: */meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

● User types the realm name

The user must type the name of one of the available authentication realms.

○ User picks from a list of authentication realms

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the User Authentication page or the Administrator Authentication page.

Available realms: ace, ad, testrealm, Users

Selected realms: SAML-Realm

Note: For more configuration details, refer to the *Pulse Connect Secure Administration Guide*.

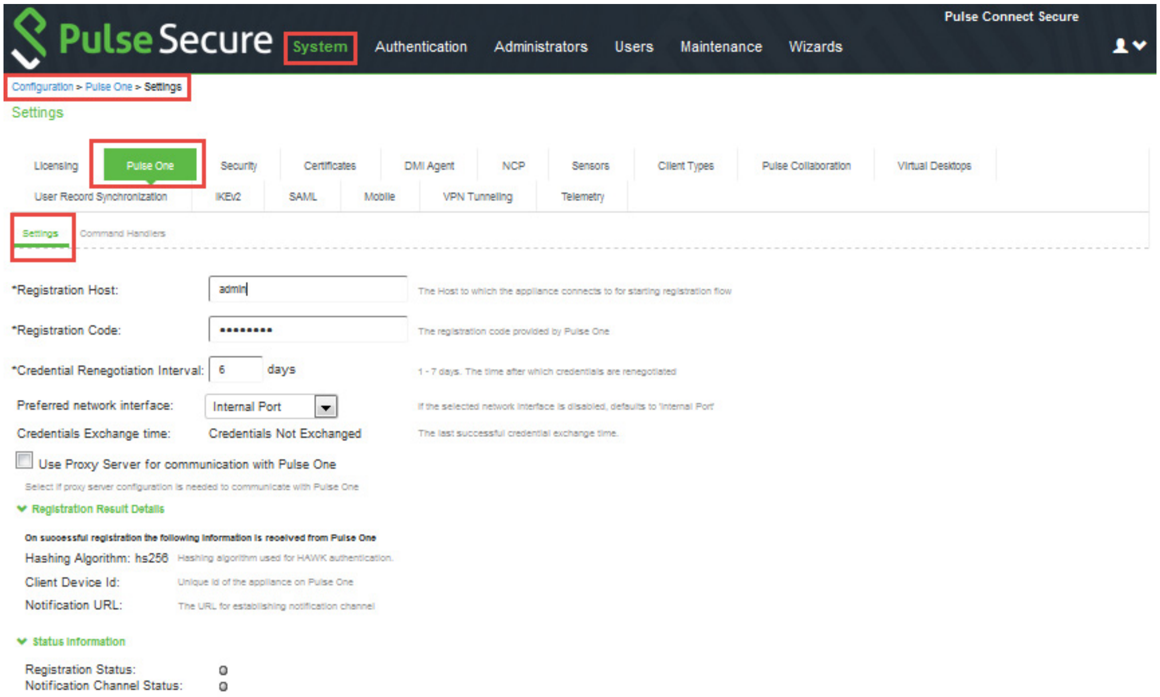
After this is complete, you can register the appliance, see **"Registering the Appliance for LDAP" on page 90**.

Registering the Appliance for LDAP

To register the Pulse Connect Secure appliance, do the following:

1. Go to **System > Configuration > Pulse One > Settings**.
2. Register the appliance by providing its **Registration Host** and **Registration Code**.

FIGURE 102 Register an Appliance



*Registration Host: admin — The Host to which the appliance connects to for starting registration flow

*Registration Code: ••••••••• — The registration code provided by Pulse One

*Credential Renegotiation Interval: 6 days — 1 - 7 days. The time after which credentials are renegotiated

Preferred network interface: Internal Port — If the selected network interface is disabled, defaults to 'Internal Port'

Credentials Exchange time: Credentials Not Exchanged — The last successful credential exchange time.

□ Use Proxy Server for communication with Pulse One

Select if proxy server configuration is needed to communicate with Pulse One

Registration Result Details

On successful registration the following information is received from Pulse One

Hashing Algorithm: hs256 — Hashing algorithm used for HAWK authentication.

Client Device Id: — Unique Id of the appliance on Pulse One

Notification URL: — The URL for establishing notification channel

Status Information

Registration Status: ○

Notification Channel Status: ○

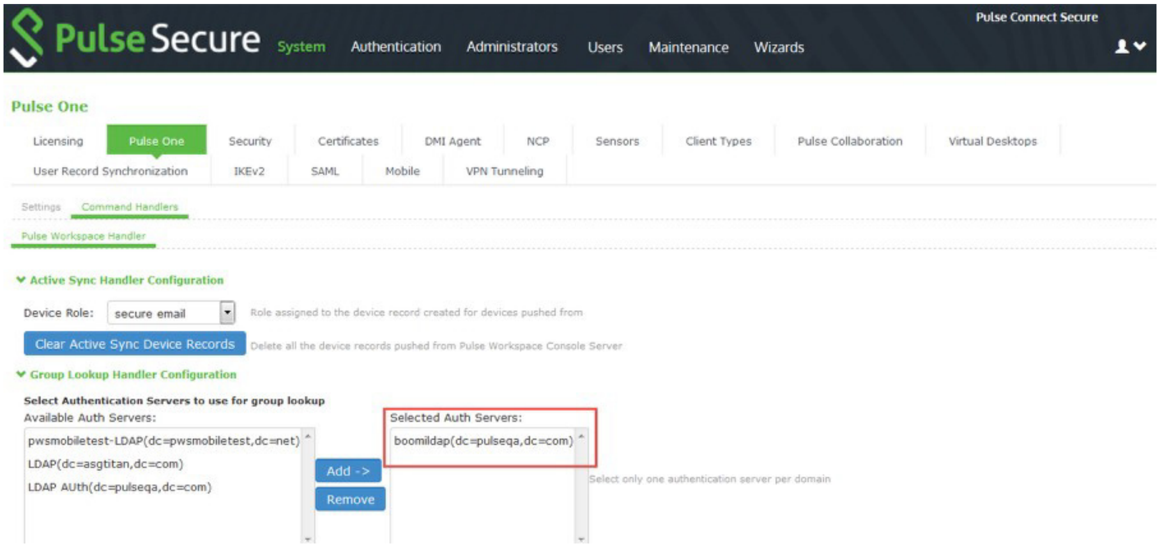
After this is complete, you can select the Pulse Workspace Command Handler for LDAP, see **"Selecting the Pulse Workspace Command Handler for LDAP" on page 91**.

Selecting the Pulse Workspace Command Handler for LDAP

To select a command handler:

1. Navigate to **System > Configuration > Pulse One > Command Handlers**.
2. Select the authentication server as **Group Lookup Handler**.

FIGURE 103 Pulse Workspace Handler



Device Role: secure email

Role assigned to the device record created for devices pushed from

Delete all the device records pushed from Pulse Workspace Console Server

Select Authentication Servers to use for group lookup

Available Auth Servers:

pwsmobiletest-LDAP(dc=pwsmobiletest,dc=net)
LDAP(dc=asgtitan,dc=com)
LDAP AUth(dc=pulseqa,dc=com)

Selected Auth Servers:

boomildap(dc=pulseqa,dc=com)

Select only one authentication server per domain

After this is complete, LDAP configuration on Pulse Connect Secure is complete. You can then proceed to **"Configuring LDAP Auto-Provisioning" on page 92**.

Configuring LDAP Auto-Provisioning

This section describes the steps to configure LDAP auto-provisioning:

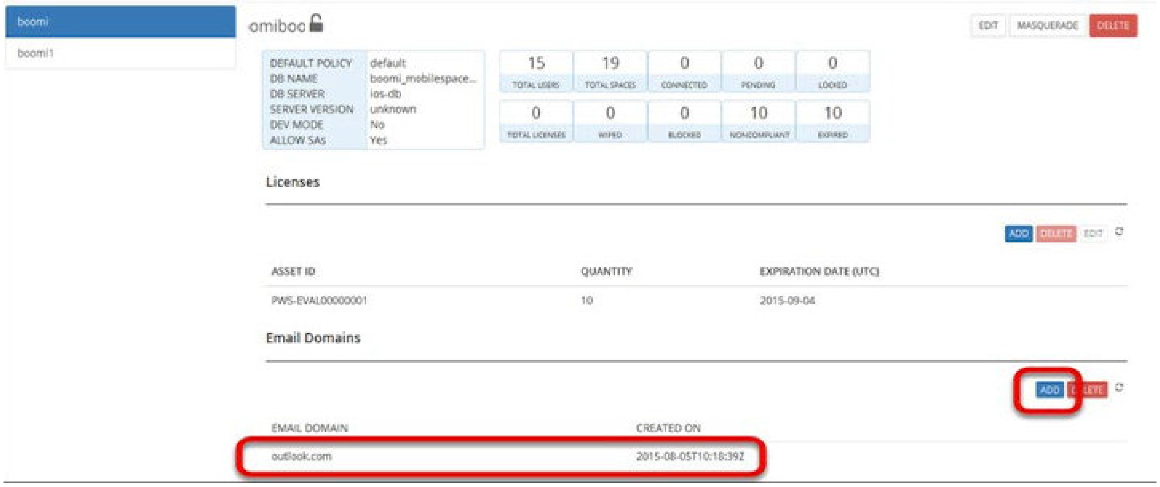
- "Creating an Email Domain Account" on page 92.
- "Adding an Appliance" on page 92.
- "Configuring the LDAP Provider Workspace Property" on page 93.
- "Adding an LDAP Group" on page 93.
- "Adding a Policy" on page 93.
- "Submitting a Corporate Email Address" on page 93.
- "Registering Mobile Devices" on page 94.

Creating an Email Domain Account

To create an email domain account:

1. Log in to the Domain Management server.
2. Create a new enterprise.
3. Add an Email domain account.

FIGURE 104 Add Email Domain Account



DEFAULT POLICY	default
DB NAME	boomi_mobilespace...
DB SERVER	ios-db
SERVER VERSION	unknown
DEV MODE	No
ALLOW SAs	Yes

TOTAL USERS	TOTAL SPACES	CONNECTED	PENDING	LOCKED
15	19	0	0	0

TOTAL LICENSES	WIPED	BLOCKED	NONCOMPLIANT	EXPIRED
0	0	0	10	10

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PWS-EVAL00000001	10	2015-09-04

EMAIL DOMAIN	CREATED ON
outlook.com	2015-08-05T10:18:39Z

Adding an Appliance

To add an appliance, follow the procedures described in the *Pulse One Administration Guide*.

Configuring the LDAP Provider Workspace Property

To configure the LDAP Provider workspace property:

1. On the Pulse One console, click the settings icon on top-right-corner of the page and select **Workspace Settings**.
2. Edit the **LDAP Provider** property to choose the registered appliance.
3. Click **Save**.

For full details of workspace properties, see **"Configuring Workspace Properties" on page 181**.

Adding an LDAP Group

To add an LDAP group, refer to **"Adding an LDAP Group" on page 15**.

Adding a Policy

When you create a policy, include the LDAP group.

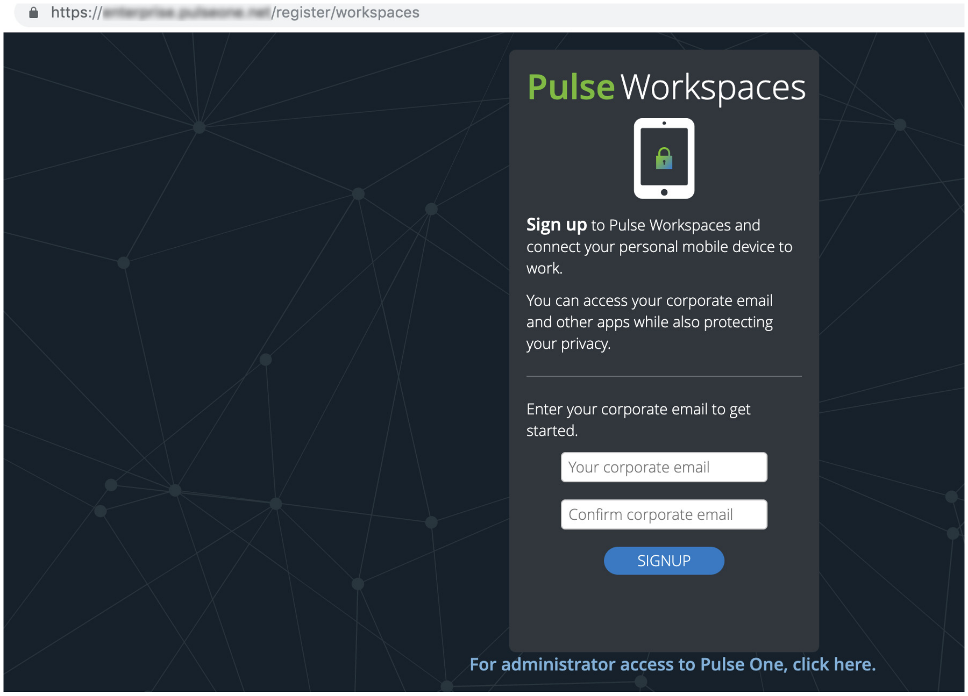
Refer to the **"Configuring an LDAP Group" on page 17**.

Submitting a Corporate Email Address

To submit a corporate email address for a device:

1. Open the registration portal: *https://<enterprise>/register/workspaces*

FIGURE 105 Submit Corporate Email



https://[redacted]/register/workspaces

Pulse Workspaces

Sign up to Pulse Workspaces and connect your personal mobile device to work.

You can access your corporate email and other apps while also protecting your privacy.

Enter your corporate email to get started.

For administrator access to Pulse One, click here.

2. Submit your corporate email ID to trigger the registration mail.

Once the corporate email is submitted, the below functional steps are processed:

- The domain will identify the enterprise that belongs to your Email domain.
- Pulse One sends a notification to PCS.
- PCS will request Pulse One for available groups and user name information.
- Pulse One responds to PCS with user account with available verified groups.
- PCS will check user's email, validate SAM account, and group membership with backend LDAP server.
- PCS will then respond to Pulse One to create a temporary record and generate an email to deliver to end user Inbox.

Registering Mobile Devices

After you submit a corporate email address, the required registration details are sent in an email. This includes the host URL and code to register the device.

The end user follows the instructions in the email to download and configure the Android/iOS Pulse Secure client on their device.

- For iOS devices, see **“Onboarding iOS BYOD Devices” on page 43**.
- For Android devices, see **“Onboarding Android BYOD Devices” on page 53**.

After successful registration by the end user, go to the Workspace and check if the LDAP groups are updated for the user according to the membership. The required policies will be pushed to the user's device according to the policies mapped to the user's group.

Groups and user membership validation notification will be sent every one hour and the periodic update will be done in 24 hours.

Configuring Managed Clients

Managed client mode of enrollment for mobile devices is one of two modes supported by Pulse Workspace, see **"Understanding Managed Devices and Managed Clients" on page 42**.

Managed client enrollment for mobile devices does not use Mobile Device Management (MDM). Instead, the admin can currently push policies manually from Pulse Workspace to enable *VPN on Demand* on a mobile device.

Note: The managed client mode is currently only supported on iOS devices.

- **"Enabling Managed Client Mode" on page 95**.
- **"Configuring VPN on Demand for Managed Clients" on page 95**.
- **"Enrolling Personal Devices as Managed Clients" on page 106**.

Enabling Managed Client Mode

To enable Pulse Workspace to enroll devices as managed clients, set the **Enable enrollment of managed iOS clients?** workspace property to *True*, see **"Workspaces" on page 149**.

Note: If the **Enable enrollment of managed iOS clients?** workspace property is *False*, Pulse Workspace will enroll devices as *managed devices*. Pulse Secure recommends that the **Enable enrollment of managed iOS clients?** workspace property setting is consistent.

Once managed client mode is enabled, you can configure VPN on Demand, see **"Configuring VPN on Demand for Managed Clients" on page 95**.

Configuring VPN on Demand for Managed Clients

After you have enabled managed client mode (see **"Enabling Managed Client Mode" on page 95**) you can enable VPN on Demand for *managed client* mobile devices, and configure it for use:

- **"Understanding VPN on Demand" on page 96**.
- **"Understanding VPN on Demand Rules Criteria" on page 97**.
- **"Understanding VPN on Demand Action Parameters" on page 98**.
- **"Enabling and Configuring VPN on Demand" on page 99**.

Understanding VPN on Demand

VPN On Demand lets mobile devices automatically establish a VPN connection on an as-needed basis, based on an ordered list of user-defined rules.

VPN On Demand rules are evaluated when the device's primary network interface changes. For example:

- When a mobile device switches to a different WiFi network, or
- When a mobile device switches from WiFi to cellular (in iOS), or
- When a mobile device switches from WiFi or Ethernet (in macOS).

Note: If the new interface is virtual, such as a VPN interface, VPN On Demand rules are ignored.

Each VPN on Demand rule has user-defined *rules criteria* that enable a match to be determined, see **"Understanding VPN on Demand Rules Criteria" on page 97**.

Each rule is evaluated in turn. If a rule matches, a specified *On Demand action* is performed for the rule. The supported On Demand actions are:

- *Connect*. Connects to the VPN when any of the specified rules criteria is met.
- *Evaluate Connection*. The VPN can be triggered based on connection requests to specific domains, rather than generally connecting/disconnecting based on the network interface. When any of the specified rules criteria is met, a list of action parameters is evaluated, see **"Understanding VPN on Demand Action Parameters" on page 98**. If any of the action parameters matches, the specified response is performed.
- *Disconnect*. Disconnects from the VPN when any of the specified rules criteria is met.
- *Ignore*. Leaves any existing VPN connection up, but does not create a new connection. This is performed when any of the specified rules criteria is met.

Once a rule matches, its On Demand action is performed, and all remaining rules in the list are not evaluated.

Note: In any rules list, a final rule should define a default response. That is, there should be no criteria, only an action that is appropriate for when the connection has not matched any of the previous rules.

Note: For a full technical description of VPN on Demand for iOS, see **https://help.apple.com/deployment/ios/#/iord4804b742**

Understanding VPN on Demand Rules Criteria

Each VPN on Demand rule can have one or more *rules criteria* which enables it to be evaluated as a match.

Note: Where you specify multiple rules criteria, the rule matches if at least one criterion matches.

Supported rules criteria are:

- *DNS Domain*. (Optional) A comma-separated list of search domains. If the configured DNS search domain of the current primary network is included in the list, the rule matches.

  A wildcard prefix (*) is supported. For example: **.example.com*

- *DNS Server*. (Optional) A comma-separated list of DNS server addresses. If all of the DNS server addresses currently configured for the primary interface are listed, the rule matches.

  A wildcard prefix (*) is supported. For example: *1.2.3.**

- *Interface Type*. (Optional) This can be set to:

  - *Cellular* (for iOS)
  - *Ethernet* (for macOS)
  - *Wi-Fi*

  If the primary interface hardware is of the type specified, the rule matches.

- *SSID*. (Optional) A comma-separated list of SSID network identifiers to match against the current WiFi network. If the network is a WiFi network and its SSID appears in the list, the rule matches.

- *URL Probe*. (Optional). A single URL to a trusted HTTPS server to probe for reachability. Redirection is not supported. If the server is reachable, the rule matches.

Note: You can also create a rule with no criteria, which provides a default response. This can be used as a standalone rule to enable all connections, or as a final rule in a list to disallow all connections by default after all other rules have failed to trigger.

Understanding VPN on Demand Action Parameters

Each VPN on Demand rule that has an On Demand action of *Evaluate Connection* must have one (or more) *action parameters* which enable the rule to be evaluated.

Note: If you specify multiple action parameters, *all* of them must match for the rule to match.

- *Domains*. (Required). A comma-separated list of the domains for which this evaluation applies.

  A wildcard prefix (*) is supported. For example: **.example.com*

- *Domain Action*. (Required) Defines VPN behavior for the domains. Supported values are:

  - *Connect If Needed*. Starts the VPN if DNS resolution for the domains fails. For example:

    - If the DNS server indicates it can’t resolve the domain name.
    - If the DNS response is redirected.
    - If the connection fails or times out.

  - *Never Connect*. Don’t trigger VPN for the domains.

- *Required DNS Server*. (Optional) A comma-separated list of IP addresses for DNS servers to be used for resolving the domains.

  Note: This parameter is available when the *Domain Action* action parameter is set to *Connect If Needed.*

  Note: These servers do not need to be part of the device’s current network configuration.

  Typically, you will configure an internal DNS server or a trusted external DNS server.

  If these DNS servers cannot be reached, the VPN is started.

- *Required URL Probe*. (Optional) An HTTP or HTTPS URL to probe.

  Note: This parameter is available when the *Domain Action* action parameter is set to *Connect If Needed.*

  If DNS resolution for this server succeeds, the probe must also succeed.

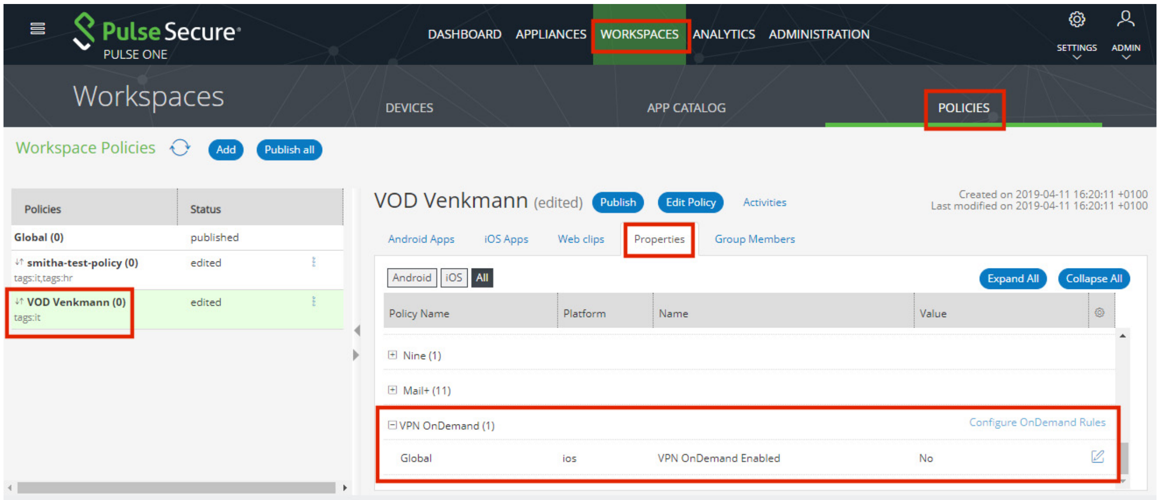
  If the probe fails, the VPN is started.

Enabling and Configuring VPN on Demand

To enable and configure VPN on Demand:

1. Log into Pulse One as an administrator.
2. Click the **Workspaces** menu and then the **Policies** tab.
3. In the **Policies** tab, select the required policy.
4. Select the **Properties** tab and expand the *VPN on Demand* group. For example:

FIGURE 106 VPN on Demand: Policy Properties



Policies	Status
Global (0)	published
smitha-test-policy (0) tags:it,tags:hr	edited
VOD Venkmann (0) tags:it	edited

VOD Venkmann (edited)

Created on 2019-04-11 16:20:11 +0100
Last modified on 2019-04-11 16:20:11 +0100

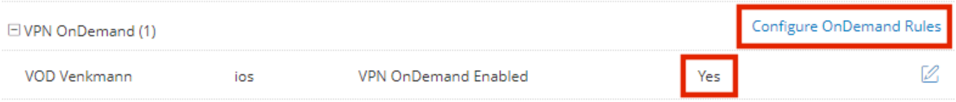
Policy Name	Platform	Name	Value
⊞ Nine (1)			
⊞ Mail+ (11)			
⊟ VPN OnDemand (1)			
Global	ios	VPN OnDemand Enabled	No

5. Set the **VPN OnDemand Enabled** property to *True*.

   Note: When the policy property **VPN OnDemand Enabled** is *True,* **Network Access** for this policy can only be configured as *Direct* (and not *Per app VPN*).

   The **Configure OnDemand Rules** control is then enabled.

FIGURE 107 VPN on Demand Enabled



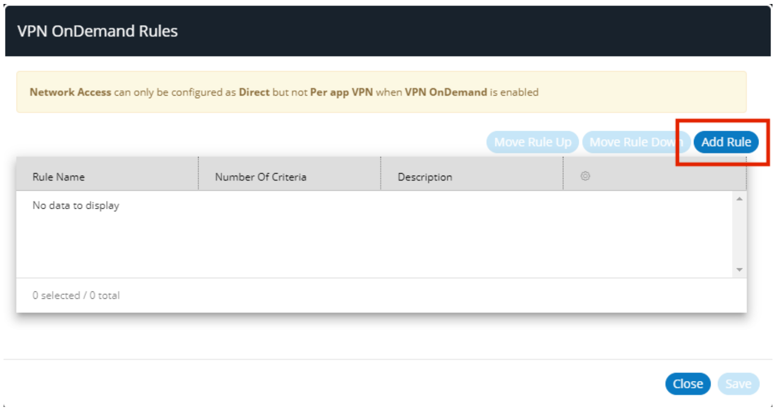
⊟ VPN OnDemand (1)

VOD Venkmann	ios	VPN OnDemand Enabled	Yes

6. Click **Configure OnDemand Rules**.

   The **VPN OnDemand Rules** dialog appears. This lists all defined rules for VPN On Demand. Initially, this list is empty. For example:

   FIGURE 108 VPN On Demand: List of Rules



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

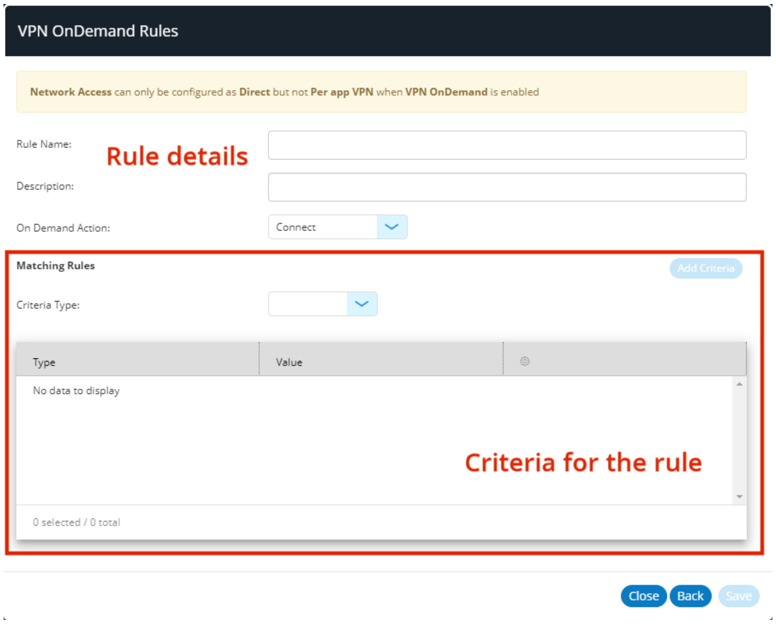
Rule Name	Number Of Criteria	Description
No data to display		

0 selected / 0 total

7. Click **Add Rule**.

   The **VPN OnDemand Rules** dialog updates to display a new panel for specifying a rule and its criteria. For example:

   FIGURE 109 VPN on Demand: Rule Definition



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name:

Description:

On Demand Action: Connect

Matching Rules

Criteria Type:

Type	Value
No data to display	

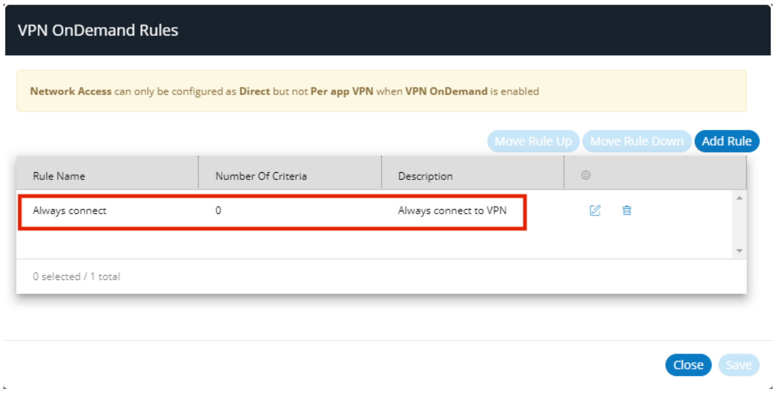
0 selected / 0 total

8. (Optional) To create a standalone rule that connects to the VPN for *all* domains/endpoints, you must define a rule with no specified criteria:

    - Enter a **Rule Name** and (optionally) a **Description**.
    - Set the **On Demand Action** to *Connect*.
    - Leave **Criteria Type** unset.
    - Click **Save**.

      The **VPN OnDemand Rules** dialog shows the rules list, with the new rule added. For example:

      FIGURE 110 VPN on Demand: General Open Rule



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name	Number Of Criteria	Description
Always connect	0	Always connect to VPN

0 selected / 1 total

9. (Optional) To create a rule that performs an On Demand action for one (or more) specific criteria:

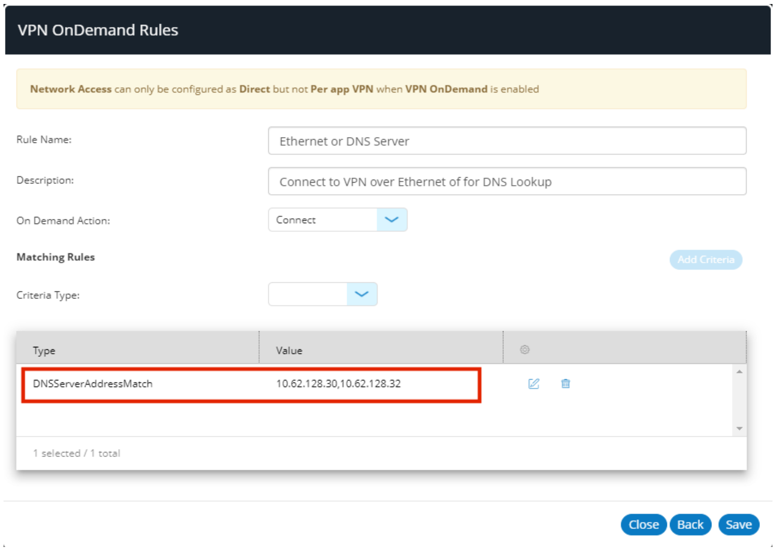
    Note: When you specify multiple criteria for a rule, any of the criteria must match for the rule to match.

    - Enter a **Rule Name** and (optionally) a **Description**.
    - Set the required **On Demand Action**, see **"Understanding VPN on Demand" on page 96**.

      Note: If you require an **On Demand Action** of *Evaluate Connection*, see the example later in this procedure.
    - Set the required **Criteria Type**, see **"Understanding VPN on Demand Rules Criteria" on page 97**.
    - Click **Add Criteria**.

The criteria is added to the list of rules criteria. For example:

FIGURE 111 VPN on Demand: Rule with One Condition



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name: Ethernet or DNS Server

Description: Connect to VPN over Ethernet of for DNS Lookup

On Demand Action: Connect

Matching Rules

Criteria Type:

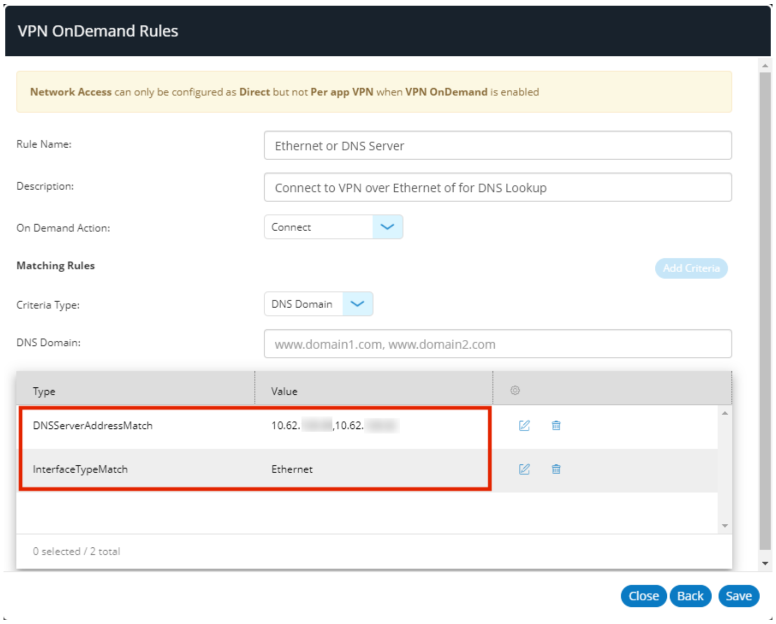
Type	Value
DNSServerAddressMatch	10.62.128.30,10.62.128.32

1 selected / 1 total

In the above example, a pair of DNS servers are specified. If both servers are configured for the primary interface, the criteria matches, and so the rule matches.

- Add additional criteria for this rule if required. For example:

FIGURE 112 VPN on Demand: Rule with Two Conditions



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name: Ethernet or DNS Server

Description: Connect to VPN over Ethernet of for DNS Lookup

On Demand Action: Connect

Matching Rules

Criteria Type: DNS Domain

DNS Domain: www.domain1.com, www.domain2.com

Type	Value
DNSServerAddressMatch	10.62.[redacted],10.62.[redacted]
InterfaceTypeMatch	Ethernet

0 selected / 2 total

In the above example, a second criteria tests if the primary interface is Ethernet.

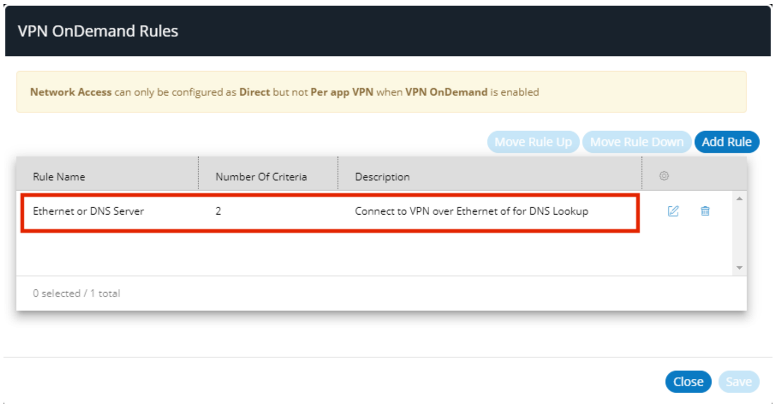
Note: Only one criteria for each **Criteria Type** is supported.

If at least one of the specified criteria matches, the rule is a match.

- (Optional) You can edit the condition by clicking **Edit** (✎).
- Click **Save**.

  The rule is added to the list of VPN on Demand rules:

  FIGURE 113 VPN on Demand: Rule with Criteria



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name	Number Of Criteria	Description
Ethernet or DNS Server	2	Connect to VPN over Ethernet of for DNS Lookup

0 selected / 1 total

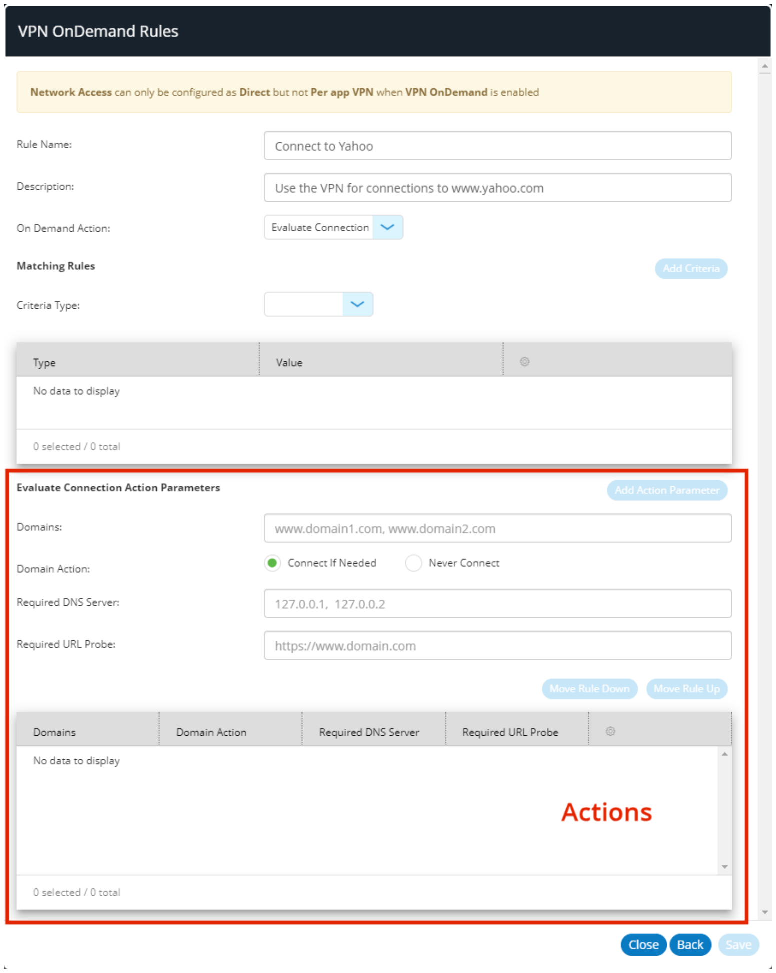
In this example, there are two criteria.

10. (Optional) To create a rule with action parameters:

    - Enter a **Rule Name** and (optionally) a **Description**.
    - Set the **On Demand Action** to *Evaluate connection*.

      The **VPN OnDemand Rules** dialog updates to include actions. For example:

      FIGURE 114 VPN on Demand: Rule with Action Parameters



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name: Connect to Yahoo

Description: Use the VPN for connections to www.yahoo.com

On Demand Action: Evaluate Connection

Matching Rules

Criteria Type:

Type	Value
No data to display	

0 selected / 0 total

Evaluate Connection Action Parameters

Domains: www.domain1.com, www.domain2.com

Domain Action: ● Connect If Needed ○ Never Connect

Required DNS Server: 127.0.0.1, 127.0.0.2

Required URL Probe: https://www.domain.com

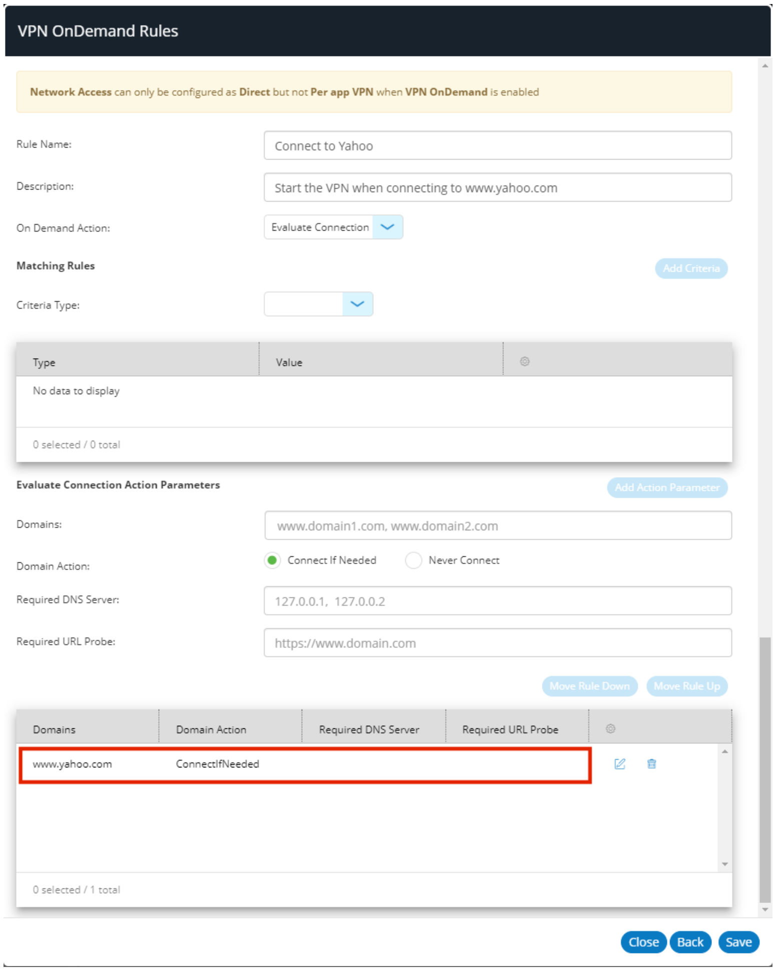
Domains	Domain Action	Required DNS Server	Required URL Probe
No data to display			

0 selected / 0 total

    - (Optional) Add one (or more) rules criteria, and add each to the list of criteria with **Add Criteria**. For details of criteria, see **“Understanding VPN on Demand Rules Criteria” on page 97**.

- Add one (or more) action parameters, and add each to the list of actions parameters with **Add Action Parameter**. For details of action parameters, see **"Understanding VPN on Demand Action Parameters" on page 98**. For example:

FIGURE 115 VPN on Demand: Rule with Action Parameter



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name: Connect to Yahoo

Description: Start the VPN when connecting to www.yahoo.com

On Demand Action: Evaluate Connection

Matching Rules

Criteria Type:

Type	Value
No data to display	

0 selected / 0 total

Evaluate Connection Action Parameters

Domains: www.domain1.com, www.domain2.com

Domain Action: ● Connect If Needed ○ Never Connect

Required DNS Server: 127.0.0.1, 127.0.0.2

Required URL Probe: https://www.domain.com

Domains	Domain Action	Required DNS Server	Required URL Probe
www.yahoo.com	ConnectIfNeeded		

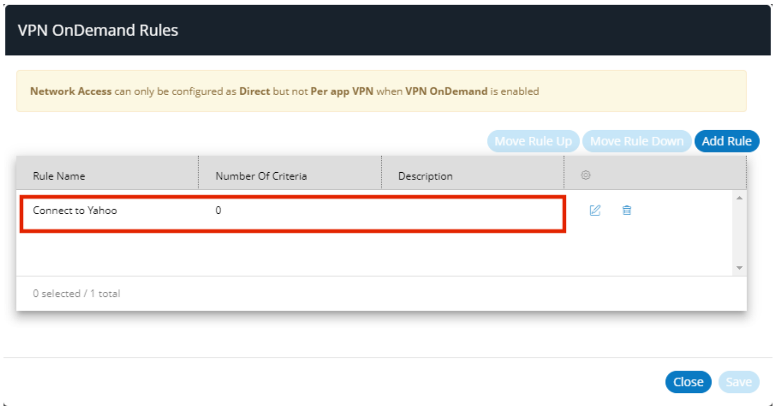
0 selected / 1 total

In this example, no rules criteria are specified, but a single action parameter activates the VPN when a connection to *www.yahoo.com* is requested.

- Click **Save**.

  The rule is added to the list of VPN on Demand rules. For example:

  FIGURE 116 VPN on Demand: Rule with Criteria



VPN OnDemand Rules

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Rule Name	Number Of Criteria	Description	⚙
Connect to Yahoo	0		✎ 🗑

0 selected / 1 total

11. (Optional) You can edit any rule by clicking its **Edit** (✎) icon.
12. (Optional) You can delete any rule by clicking its **Delete** (🗑) icon and confirming the deletion.
13. (Optional) You can change the order of rule using the **Move Rule Up** and **Move Rule Down** controls. Rules are always tested in the listed order.
14. Add a final rule that defines a default response for when none of the rules match. This rule will have an On Demand action but no criteria.

Once you have configured VPN on Demand for managed client devices, you can enroll devices using managed client mode, see **"Enrolling Personal Devices as Managed Clients" on page 106**.

Enrolling Personal Devices as Managed Clients

After you have configured VPN on Demand (see **"Configuring VPN on Demand for Managed Clients" on page 95**) you can enroll devices using *managed client* mode.

- **"Adding a Personal Device to Pulse Workspace as a Managed Client" on page 106**.
- **"Enrolling a Personal Mobile Device as a Managed Client" on page 107**.

Adding a Personal Device to Pulse Workspace as a Managed Client

This procedure describes how an administrator adds a user's personal mobile device to Pulse Workspace with the intention of it being used as a *managed client*. Before starting, the admin must:

- Enable managed client mode on Pulse Workspace, see **"Enabling Managed Client Mode" on page 95**.
- Configure VPN on Demand, see **"Configuring VPN on Demand for Managed Clients" on page 95**.

To add a user’s personal device to Pulse Workspace:

1. Log into the Pulse One appliance.
2. Select the **Workspaces** menu and then the **Devices** tab.
3. In the **Devices** tab, create (or edit) the required user. The user details should include:
   - The user’s corporate email as the **Workspace Email**.
   - The user’s personal email as the **Provisioning Email**, so that they will receive the required registration information in an email.
   - (Optional) Any required policy **Tags** for the user.
4. Click the **Add Workspace** tab, add device details, and click **Create**.

   The user will then receive registration details at their personal email address.

The user can then enroll their personal device as a managed client, see **“Enrolling a Personal Mobile Device as a Managed Client” on page 107**.

Enrolling a Personal Mobile Device as a Managed Client

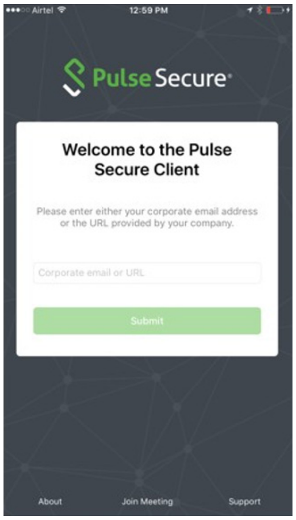
After a user’s personal mobile device is added to Pulse Workspace with the intention of it being used as a managed client, the user receives a registration email at their declared personal email address.

This procedure describes how the user then enrolls their personal device as a managed client.

1. In your email, click the iOS registration link. This installs Pulse Secure.
2. Start Pulse Secure on your device.

   The Pulse Secure **Welcome** screen appears.

   FIGURE 117 Welcome

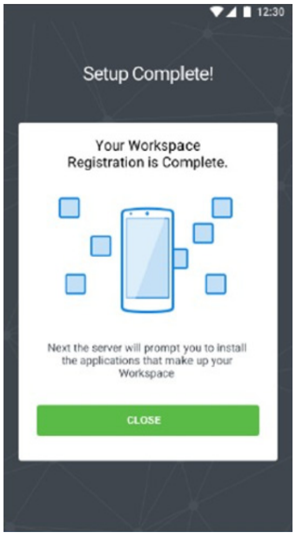


Welcome to the Pulse Secure Client

Please enter either your corporate email address or the URL provided by your company.

3. Perform the standard iOS BYOD enrollment procedure (see “Registering an iOS BYOD Device” on page 46) until the following screen appears:

FIGURE 118 Setup Complete



Setup Complete!

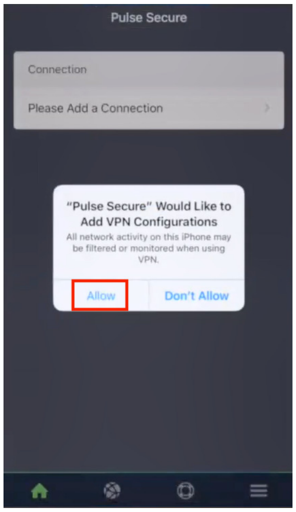
Your Workspace Registration is Complete.

Next the server will prompt you to install the applications that make up your Workspace

4. Click **Close**.

In the Pulse Secure client, the **Connection** screen appears.

FIGURE 119 Confirm VPN Config Policy



“Pulse Secure” Would Like to Add VPN Configurations

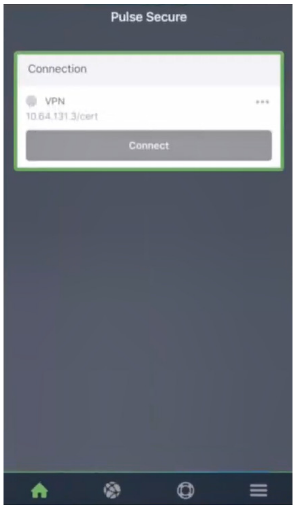
All network activity on this iPhone may be filtered or monitored when using VPN.

5. Press **Allow** to confirm the addition of the required VPN configuration policy.

   Note: If required, enter a PIN or perform a fingerprint confirmation to download the policy.

   The **Connection** screen updates to show the configured (but not currently active) VPN connection.

   FIGURE 120 VPN Connection

   Connection

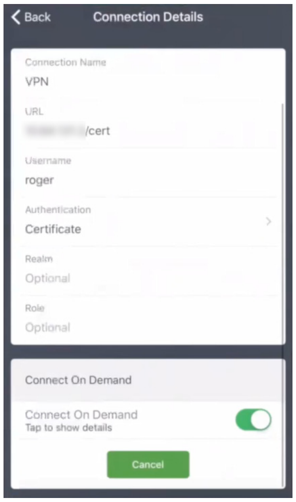
   VPN

   10.64.131.3/cert

6. Press the VPN to view its details.

   Note: This configuration cannot be updated on your device.

   FIGURE 121 VPN Configuration

   Connection Name: VPN

   URL: [redacted]/cert

   Username: roger

   Authentication: Certificate

   Realm: Optional

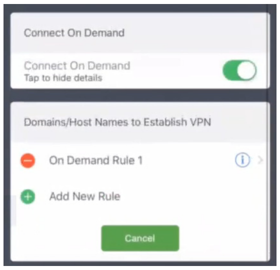
   Role: Optional

   Connect On Demand

   Connect On Demand: on
   Tap to show details

7. Press **Connect on Demand** to view configured VPN rules.

FIGURE 122 VPN Rules



Connect On Demand

Connect On Demand
Tap to hide details

Domains/Host Names to Establish VPN

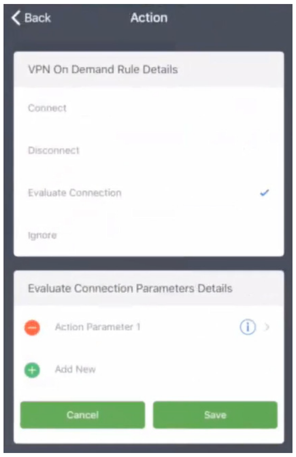
On Demand Rule 1

Add New Rule

Cancel

8. Press the configured rule (in this example, *On Demand Rule 1*) to view its details and actions.

FIGURE 123 VPN On Demand Rule Details



Back Action

VPN On Demand Rule Details

Connect

Disconnect

Evaluate Connection ✓

Ignore

Evaluate Connection Parameters Details

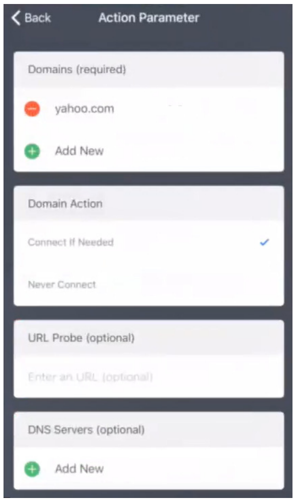
Action Parameter 1

Add New

Cancel Save

9. Press the configured action (in this example, *Action Parameter 1*) to view its details.

FIGURE 124 VPN On Demand Action Details



Back Action Parameter

Domains (required)

yahoo.com

Add New

Domain Action

Connect If Needed ✓

Never Connect

URL Probe (optional)

Enter an URL (optional)

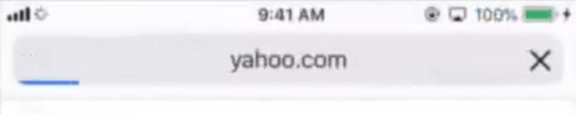
DNS Servers (optional)

Add New

In this example, the *yahoo.com* domain will connect to the VPN when it is started.

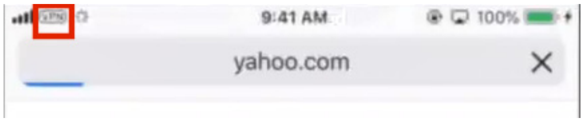
10. To test the VPN, start a browser and access the listed domain. (In this example, *yahoo.com*).

    FIGURE 125 Browser Accessing Domain

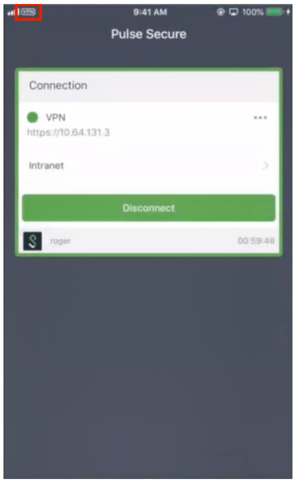
    The VPN will active and display the VPN icon at the top of the screen. For example:

    FIGURE 126 Browser Uses VPN

11. Return to the **Connection** screen to see the VPN in use.

    FIGURE 127 VPN Connection in Use

The VPN will disconnect automatically when it is not required, or you can press **Disconnect**.

Configuring Android Enterprise

Overview

Android Enterprise is a program for supporting enterprise use of Android, which consists of product features in Android, Google Play for Work, Managed Google Play Accounts and other productivity tools. The solutions built on Android Enterprise include data security, app security, device security, and so on.

An IT administrator needs to set up Android Enterprise before anyone can start using it. The setup differs depending on what type of account you have. Your account determines if you can use Google Mobile Management or a third-party EMM provider.

Note: On-Prem customers must contact Pulse Support for the Enterprise Service Account (ESA) credentials.

Pulse Workspace provides the following solutions:

- **Managed Google Play Accounts**: This helps customers who do not have a GSuite or Managed Google Account. Refer to the **Managed Google Play Help**.

- **Google Play for Work** or **Managed Google Account**: This helps GSuite or Managed Google Account customers to use Android for Work. For more details, refer to the **Android Enterprise Help**.

For details about setting up Managed Google Play Accounts and Google Play for Work, refer to the *Pulse One Cloud Administration Guide*.

Adding an Android App to the App Catalog

Many apps typically require some configuration on the device such as user information (email address), server information (URL, port), enable specific features (VPN), and so on. By defining these configurations in the admin console, the app can auto-configure with minimal user input and will simplify the setup process for end users.

This section describes the following activities:

- **"Viewing the App Catalog" on page 114**.

- **"Adding an Android App to the App Catalog from Google Play" on page 115**.

- **"Adding an Android App to the App Catalog Manually" on page 120**.

- **"Uploading an Android App to the App Catalog from Pulse One" on page 122**.

Note: Adding an app to the **App Catalog** does not automatically deliver apps to the user's device. The app must first be added to an appropriate policy, and the policy published.

Note: All configuration changes made to the app in the **App Catalog** are the defaults for the app. However, you can overwrite these after adding the app to a specific policy.

Viewing the App Catalog

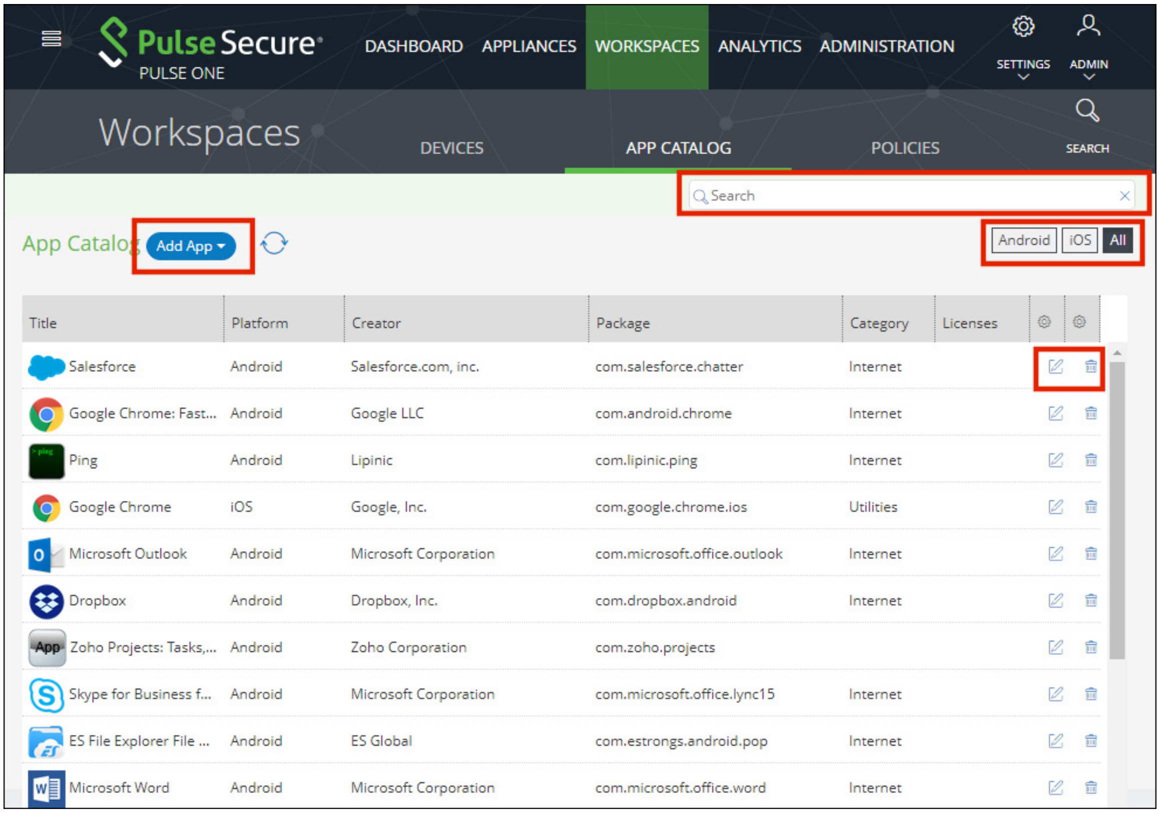
The **App Catalog** page lists the apps that have been added to the management console. On this page, you can see the app details or add a new app.

To view the app catalog:

1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab.

   The **App Catalog** page lists all apps in the catalog. For example:

FIGURE 128 App Catalog



Title	Platform	Creator	Package	Category	Licenses	⚙	⚙
Salesforce	Android	Salesforce.com, inc.	com.salesforce.chatter	Internet		✎	🗑
Google Chrome: Fast...	Android	Google LLC	com.android.chrome	Internet		✎	🗑
Ping	Android	Lipinic	com.lipinic.ping	Internet		✎	🗑
Google Chrome	iOS	Google, Inc.	com.google.chrome.ios	Utilities		✎	🗑
Microsoft Outlook	Android	Microsoft Corporation	com.microsoft.office.outlook	Internet		✎	🗑
Dropbox	Android	Dropbox, Inc.	com.dropbox.android	Internet		✎	🗑
Zoho Projects: Tasks,...	Android	Zoho Corporation	com.zoho.projects			✎	🗑
Skype for Business f...	Android	Microsoft Corporation	com.microsoft.office.lync15	Internet		✎	🗑
ES File Explorer File ...	Android	ES Global	com.estrongs.android.pop	Internet		✎	🗑
Microsoft Word	Android	Microsoft Corporation	com.microsoft.office.word	Internet		✎	🗑

On this page:

- **Search** – This enables you to filter the apps list.
- **Android / iOS / All** – This enables you to filter the app list by platform.
- **Add App** – This enables you to add apps from Google Play, Apple App Store or manually.
- **App Catalog** – Displays information about each app in the system.
- **Edit** (✎) – This enables you to edit the settings for an app.
- **Delete** (🗑) – This enables you to delete an app from the **App Catalog**.

  Note: You must remove the app from all policies before you can delete it.

Adding an Android App to the App Catalog from Google Play

To add an Android app to the **App Catalog** from Google Play:

1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab.

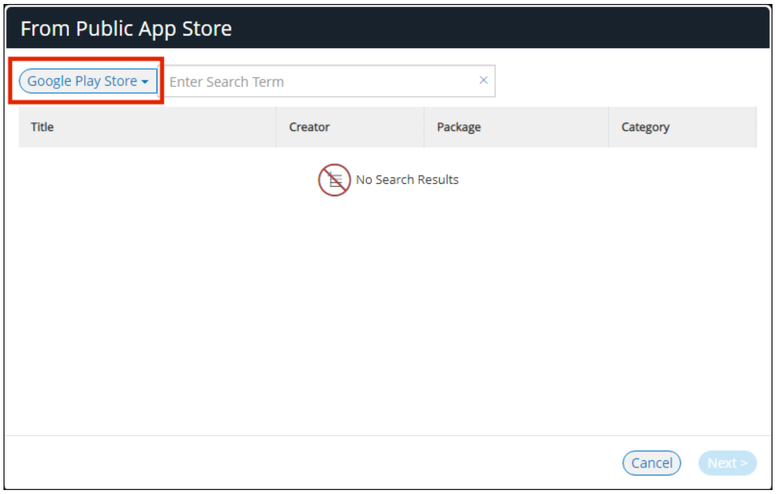
   The **App Catalog** page appears.

   Note: Ensure the app you are going to add is not listed.
3. In the **App Catalog** page, click **Add App** and then select **Add App From Store**.

   The **From Public App Store** dialog appears.
4. In the **From Public App Store** dialog, select Google Play Store.

   Note: For information about enabling international apps stores, see "Workspaces" on page 182.

   FIGURE 129 Add App From Google Play Store



From Public App Store

Google Play Store ▾ | Enter Search Term ×

Title	Creator	Package	Category

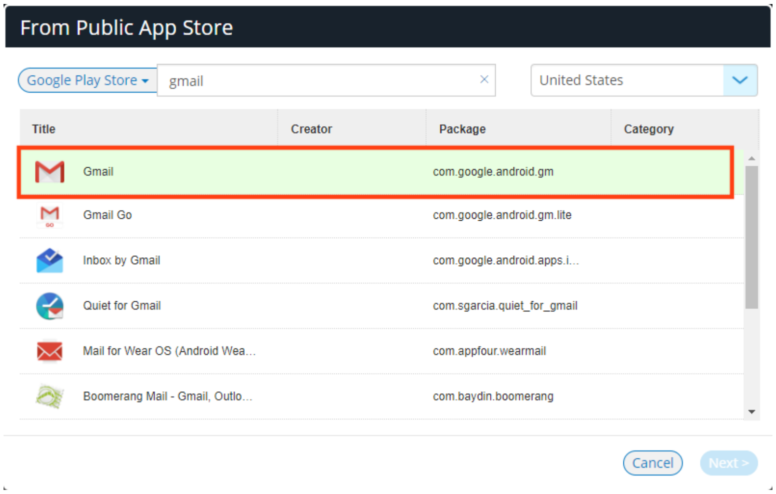
No Search Results

5. Type the name of the app in the **Search** box and press Enter.

   A list of apps is displayed based on the search criteria.

6. Select the required app from the apps list and click **Next**.

   FIGURE 130 Select App from Search Result



From Public App Store

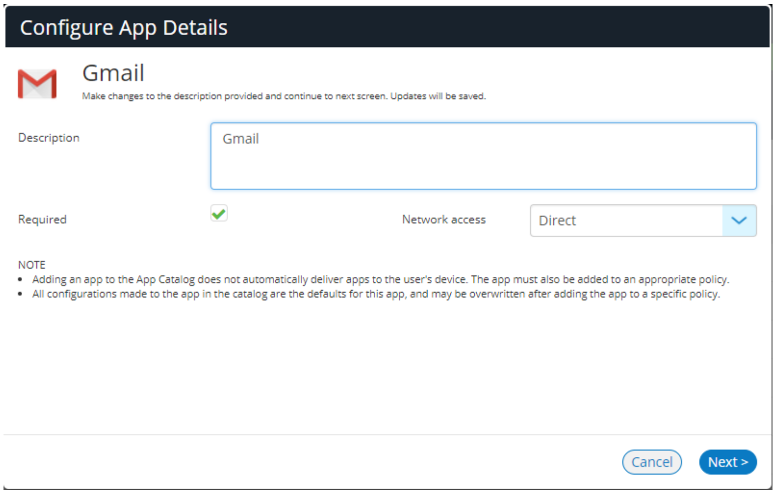
Title	Creator	Package	Category
Gmail		com.google.android.gm	
Gmail Go		com.google.android.gm.lite	
Inbox by Gmail		com.google.android.apps.i...	
Quiet for Gmail		com.sgarcia.quiet_for_gmail	
Mail for Wear OS (Android Wea...		com.appfour.wearmail	
Boomerang Mail - Gmail, Outlo...		com.baydin.boomerang	

   The **Configure App Details** dialog appears.

7. In the **Configure App Details** dialog:

   - Change the **Description** if required.
   - Select the **Required** check box if the app should be pushed automatically upon enrollment.
   - If you access the app through VPN, then set **Network access** to *Require VPN*.

   FIGURE 131 Configure App Details



Configure App Details

Gmail

Make changes to the description provided and continue to next screen. Updates will be saved.

Description: Gmail

Required: ☑

Network access: Direct

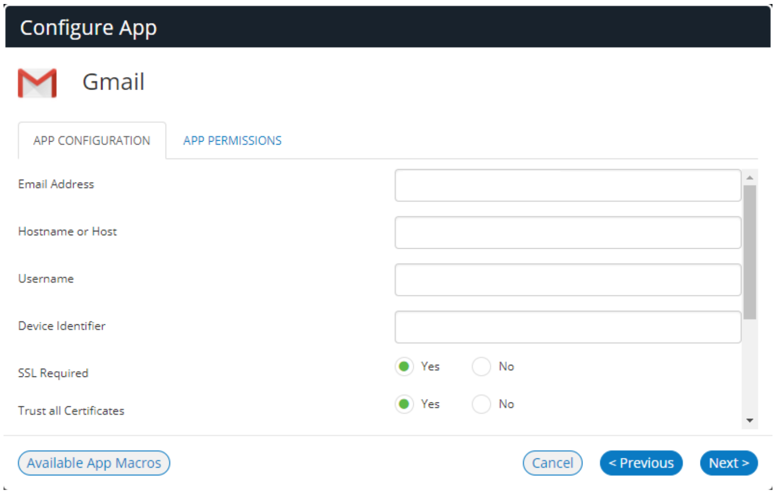
NOTE

- Adding an app to the App Catalog does not automatically deliver apps to the user's device. The app must also be added to an appropriate policy.
- All configurations made to the app in the catalog are the defaults for this app, and may be overwritten after adding the app to a specific policy.

- Click **Next**.

  The **Configure App** dialog appears:

  FIGURE 132 Configure App

  Email Address

  Hostname or Host

  Username

  Device Identifier

  SSL Required ● Yes ○ No

  Trust all Certificates ● Yes ○ No

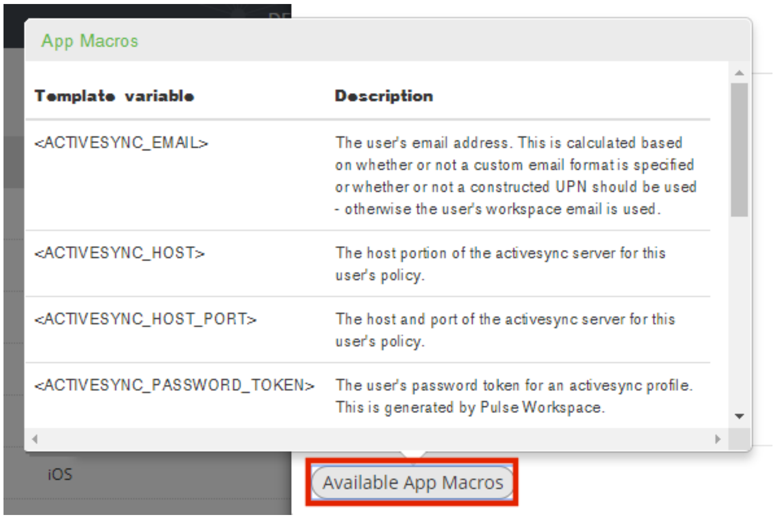
8. In the **Configure App** dialog:

- Specify the **Email address** that will be used by the app.

  Typically, you will specify an app macro such as *<USER_WORKSPACE_EMAIL>* or *<ACTIVESYNC_EMAIL>*.

  To view app macros, click the **Available App Macros** switch:

  FIGURE 133 Available App Macros

Template variable	Description
<ACTIVESYNC_EMAIL>	The user's email address. This is calculated based on whether or not a custom email format is specified or whether or not a constructed UPN should be used - otherwise the user's workspace email is used.
<ACTIVESYNC_HOST>	The host portion of the activesync server for this user's policy.
<ACTIVESYNC_HOST_PORT>	The host and port of the activesync server for this user's policy.
<ACTIVESYNC_PASSWORD_TOKEN>	The user's password token for an activesync profile. This is generated by Pulse Workspace.

- Specify a **Hostname or Host** for the app.

  Typically, you will specify an app macro such as *<ACTIVESYNC_HOST>* or *<ACTIVESYNC_HOST_PORT>*.

- Specify a **Username** for the app.

  Typically, this will be an app macro such as <*USER_USERNAME*> or <*ACTIVESYNC_USERNAME*>.

- Specify a **Device Identifier** for the app.

  Typically, this will be an app macro such as <*DEVICE_ACTIVESYNC_ID*>.

- Select whether **SSL** is required to access the app.

  If True, end-to-end encryption is required when accessing the app from a device.

- Select whether to **Trust All Certificates**.

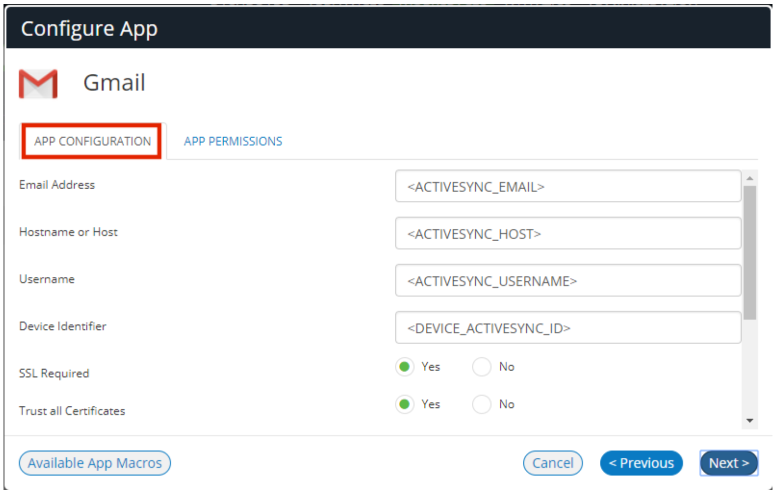
  If True, no certificate checks are performed.

- Specify a managed **Login Certificate Alias** if required.
- Select whether to **Allow Unmanaged Accounts** to access the app.
- (Optional) Specify a **Default Email Signature**.

  This can include an app macro such as <*USER_DISPLAY_NAME*>.

- Specify a **Default Sync Window** for devices. This is expressed as minutes.

FIGURE 134 App Configuration Complete



Configure App

Gmail

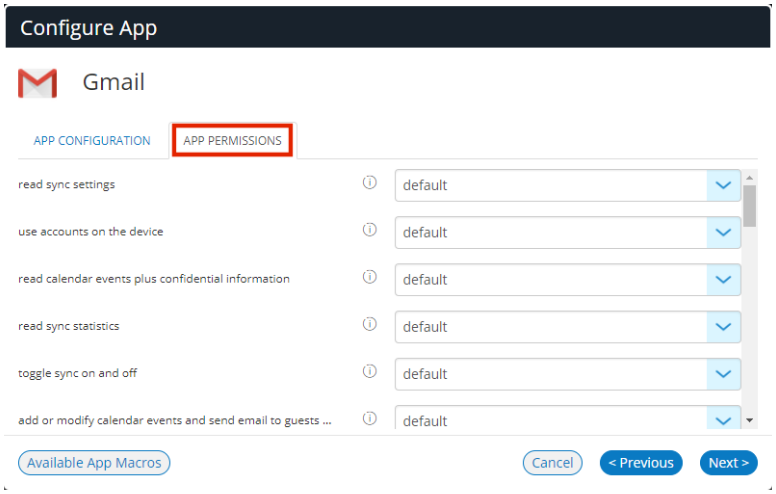
APP CONFIGURATION | APP PERMISSIONS

Email Address	<ACTIVESYNC_EMAIL>
Hostname or Host	<ACTIVESYNC_HOST>
Username	<ACTIVESYNC_USERNAME>
Device Identifier	<DEVICE_ACTIVESYNC_ID>
SSL Required	● Yes ○ No
Trust all Certificates	● Yes ○ No

- Click **Next**.

If additional permissions are required for the app, the **Configure App** dialog updates. In the **App Permissions** tab, select the required permissions for the app and click **Next**. For example:

FIGURE 135 Configure App Permissions

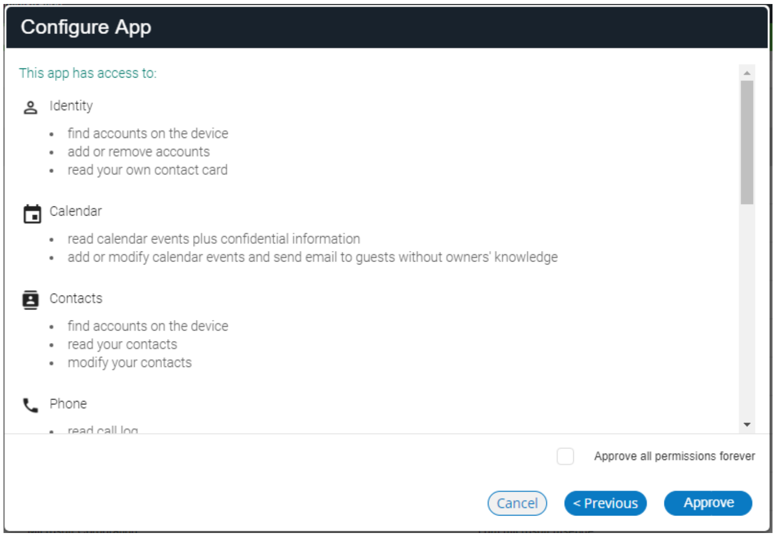


read sync settings	default
use accounts on the device	default
read calendar events plus confidential information	default
read sync statistics	default
toggle sync on and off	default
add or modify calendar events and send email to guests ...	default

Note: For information about app permission properties, see **"Workspaces" on page 182**.

An approval dialog appears. This lists the permissions that will be set for the app using the specified settings. For example:

FIGURE 136 Approve App Permissions



This app has access to:

Identity

- find accounts on the device
- add or remove accounts
- read your own contact card

Calendar

- read calendar events plus confidential information
- add or modify calendar events and send email to guests without owners' knowledge

Contacts

- find accounts on the device
- read your contacts
- modify your contacts

Phone

- read call log

□ Approve all permissions forever

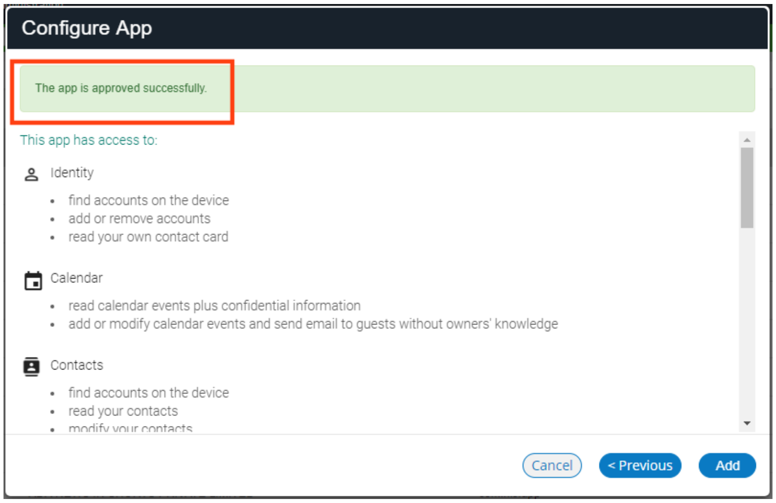
9. (Optional) Click **Approve all permissions forever** to create open-ended approval of permissions for the app.

Note: All revoked (or newly-added) permissions will be granted by default if this check box is selected.

10. In the approval dialog, click **Approve**.

    A confirmation message appears.

    FIGURE 137 App Added



Configure App

The app is approved successfully.

This app has access to:

Identity

- find accounts on the device
- add or remove accounts
- read your own contact card

Calendar

- read calendar events plus confidential information
- add or modify calendar events and send email to guests without owners' knowledge

Contacts

- find accounts on the device
- read your contacts
- modify your contacts

11. Click **Add** to add the app from Google Play to the **App Catalog**.

    Note: Adding an app to the **App Catalog** does not automatically deliver apps to the user's device. The app must also be added to an appropriate policy.

    Note: All configuration changes made to the app in the **App Catalog** are the defaults for the app. However, you can overwrite these after adding the app to a specific policy.

The next step is to add the app to a specific policy. For details, see **"Adding an Android App to a Policy" on page 130**.

Adding an Android App to the App Catalog Manually

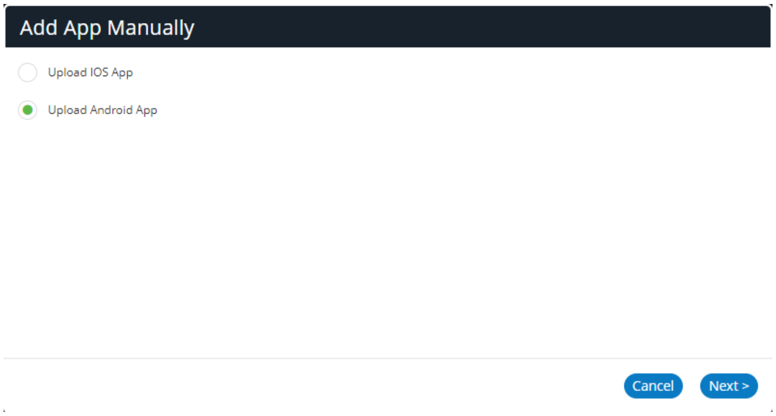
To add an Android app to the **App Catalog** manually:

1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab. The **App Catalog** page appears.

3. In the **App Catalog** page, click **Add App** and then select **Add App Manually**.

   The **Add App Manually** dialog appears.

   FIGURE 138 Add Android App Manually



Add App Manually

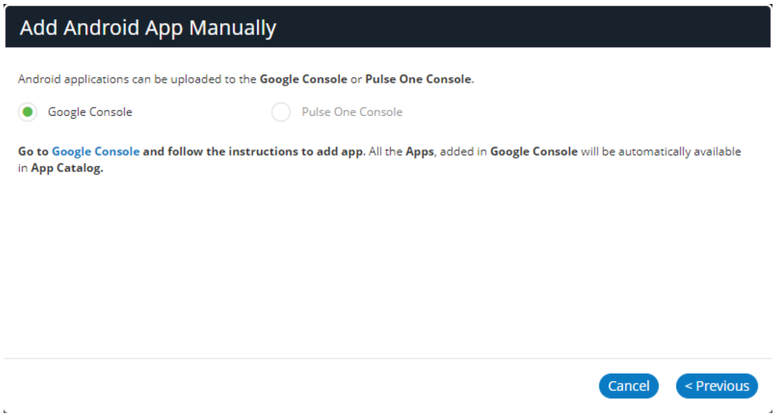
○ Upload IOS App

● Upload Android App

4. Select **Upload Android App** and click **Next**.

   The **Add Android App Manually** dialog appears.

   FIGURE 139 Add Android App Manually



Add Android App Manually

Android applications can be uploaded to the **Google Console** or **Pulse One Console**.

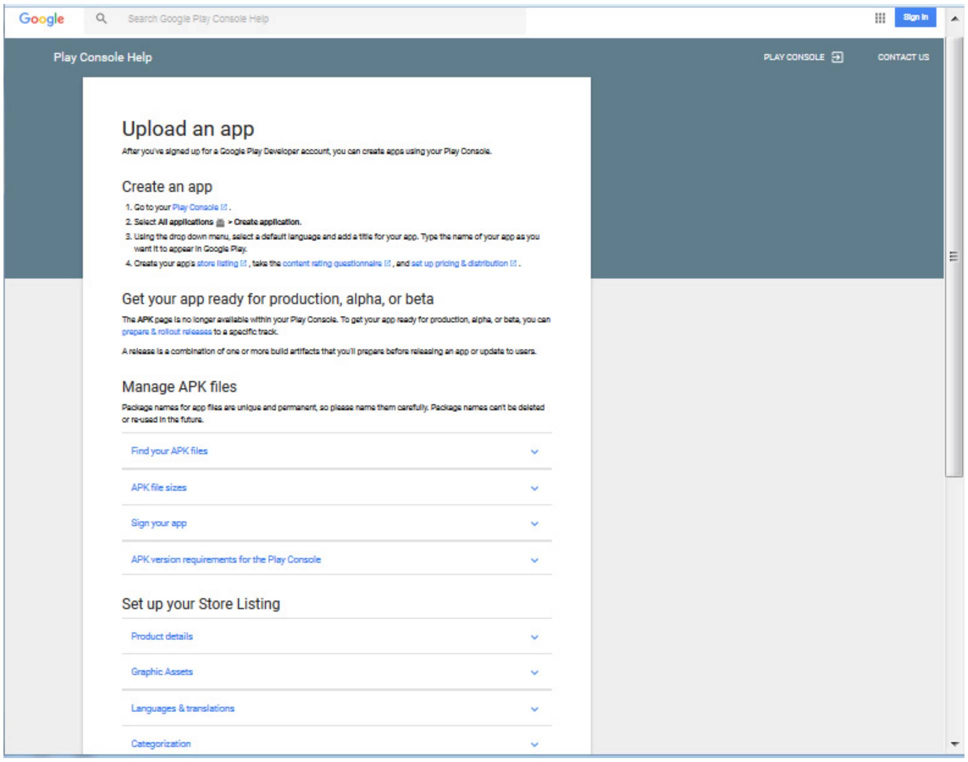
● Google Console ○ Pulse One Console

Go to Google Console and follow the instructions to add app. All the **Apps**, added in **Google Console** will be automatically available in **App Catalog**.

5. In the **Add Android App Manually** window, select **Google Console**.
6. Select the **Google Console** hyperlink.
7. Log in with Google enterprise credentials.

8. Follow the Google instructions to upload the APK, publish the app, publish the content rating and pricing, and publish the custom app.

FIGURE 140 Upload an Android App



Upload an app

After you've signed up for a Google Play Developer account, you can create apps using your Play Console.

Create an app

1. Go to your Play Console.
2. Select **All applications** > **Create application.**
3. Using the drop down menu, select a default language and add a title for your app. Type the name of your app as you want it to appear in Google Play.
4. Create your app's store listing, take the content rating questionnaire, and set up pricing & distribution.

Get your app ready for production, alpha, or beta

The **APK** page is no longer available within your Play Console. To get your app ready for production, alpha, or beta, you can prepare & rollout releases to a specific track.

A release is a combination of one or more build artifacts that you'll prepare before releasing an app or update to users.

Manage APK files

Package names for app files are unique and permanent, so please name them carefully. Package names can't be deleted or re-used in the future.

Set up your Store Listing

After publication, it takes approximately four hours to appears in the Pulse Workspace **App Catalog**.

9. (Optional) Click **Edit** to modify the app, and follow the steps described in **"Adding an Android App to the App Catalog from Google Play" on page 115**.

The next step is to add the app to a specific policy. For details, see **"Adding an Android App to a Policy" on page 130**.

Uploading an Android App to the App Catalog from Pulse One

You can add an Android app to the App Catalog from Pulse One. To do this, you upload an Android app APK to Pulse One manually. The app is then added automatically to the Google Play Store for your Google developer account. After the app is approved on Google Play Store, it is added automatically to your Pulse One App Catalog.

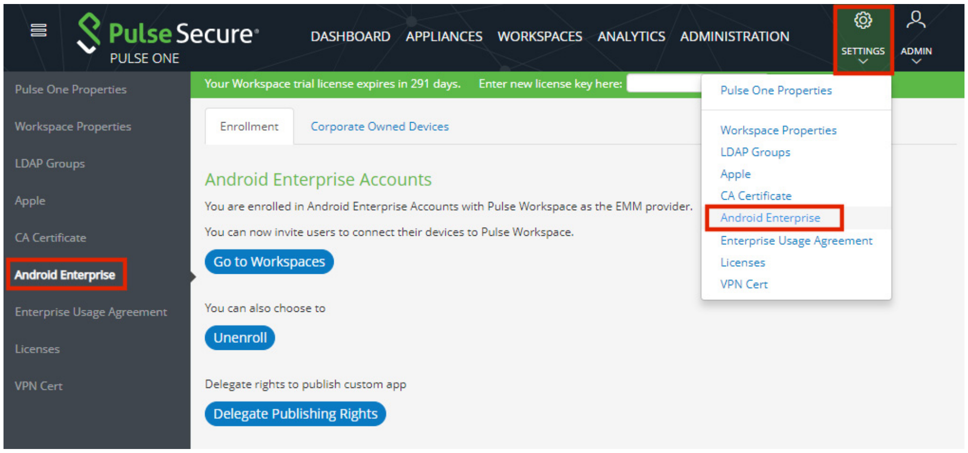
Before you can upload an APK, you must delegate publishing rights from Android Enterprise to Pulse One.

Note: You cannot delegate publishing rights for Android app upload when your Android Enterprise is enrolled using the Google Apps setup method.

To delegate publishing rights from Android Enterprise to Pulse One:

1. Click the **Settings** icon on top-right-corner of the page and select **Android Enterprise**.

   FIGURE 141 Android Enterprise Properties

   Your Workspace trial license expires in 291 days. Enter new license key here:

   Android Enterprise Accounts

   You are enrolled in Android Enterprise Accounts with Pulse Workspace as the EMM provider.

   You can now invite users to connect their devices to Pulse Workspace.

   You can also choose to

   Delegate rights to publish custom app

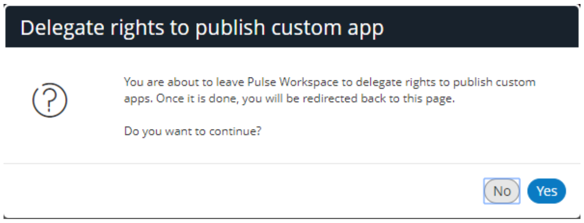
   The **Android Enterprise Accounts** page appears.

   Note: Ensure that your Google developer account is enrolled in Android Enterprise Accounts with Pulse Workspace as the Enterprise Mobility Management (EMM) provider (see the notification above). If it is not, you must click **Enroll** and follow the Google process.

2. Click **Delegate Publishing Rights**.

   A confirmation dialog appears.

   FIGURE 142 Delegate Publishing Rights

   Delegate rights to publish custom app

   You are about to leave Pulse Workspace to delegate rights to publish custom apps. Once it is done, you will be redirected back to this page.

   Do you want to continue?

3. Click **Yes**.

4. Log in with required Google developer credentials.

   A Google Play confirmation screen appears.

5. Confirm that you want to publish private apps.

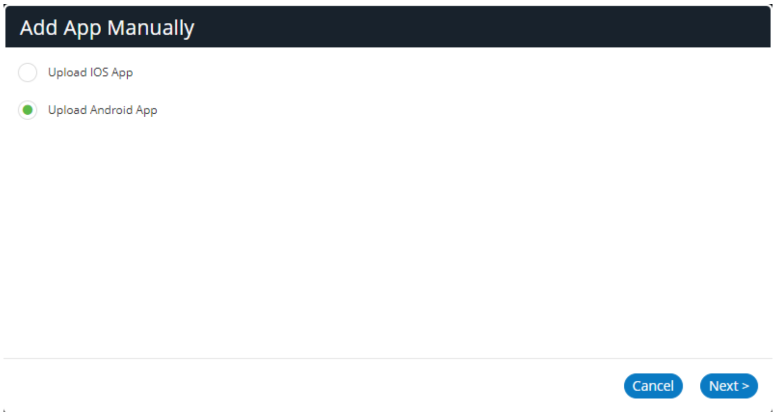
   The delegate rights process is complete.

To add an Android app to the App Catalog from Pulse One:

1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab. The **App Catalog** page appears.
3. In the **App Catalog** page, click **Add App** and then select **Add App Manually**.

   The **Add App Manually** dialog appears.

   FIGURE 143 Add Android App Manually

   Add App Manually

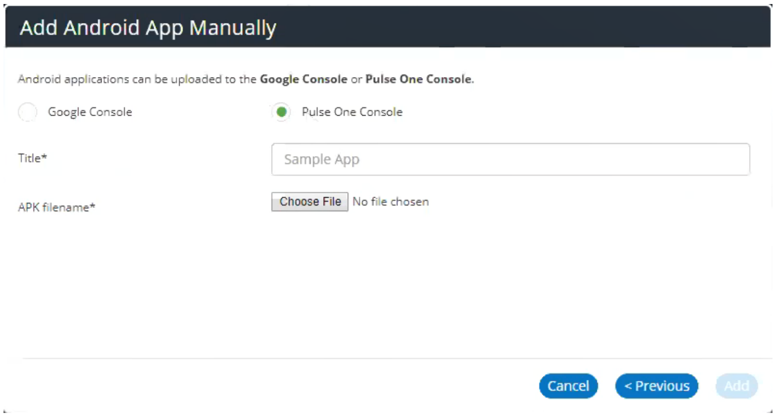
   ○ Upload IOS App

   ● Upload Android App

4. Select **Upload Android App** and click **Next**.

   The **Add Android App Manually** dialog appears.

   FIGURE 144 Add Android App Manually

   Add Android App Manually

   Android applications can be uploaded to the **Google Console** or **Pulse One Console**.

   ○ Google Console ● Pulse One Console

   Title* Sample App

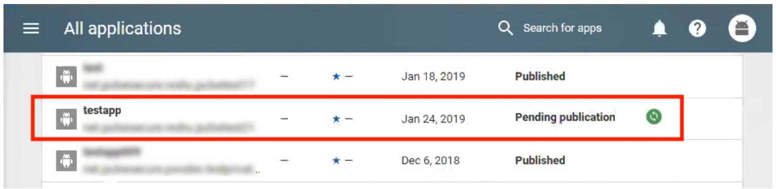
   APK filename* Choose File No file chosen

5. In the **Add Android App Manually** window, select **Pulse One Console**.
6. Enter a **Title** for the app.
7. Click **Choose File** and locate the required Android APK filename.

8. Click **Add**.

   The APK is uploaded automatically to the Google Play console in an Pending publication state. For example:

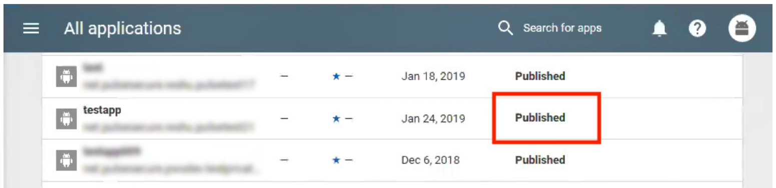
FIGURE 145 Uploaded Android App Unpublished



[redacted]	–	★ –	Jan 18, 2019	Published
testapp [redacted]	–	★ –	Jan 24, 2019	Pending publication
[redacted]	–	★ –	Dec 6, 2018	Published

The approval and publication can takes up to ten minutes. After publication, the state updates:

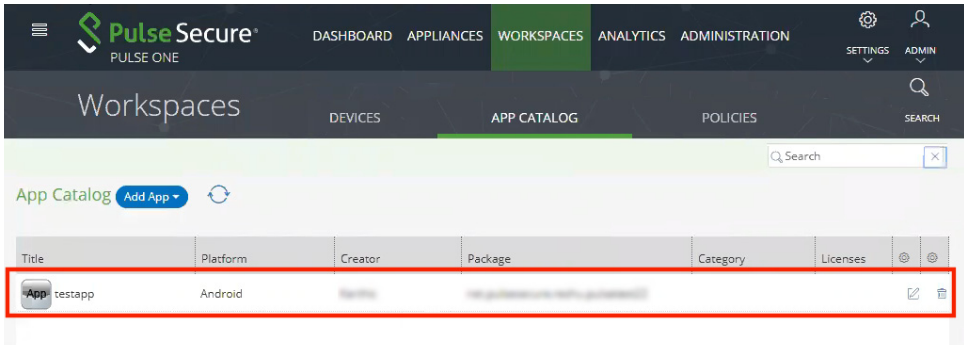
FIGURE 146 Uploaded Android App Published



[redacted]	–	★ –	Jan 18, 2019	Published
testapp [redacted]	–	★ –	Jan 24, 2019	Published
[redacted]	–	★ –	Dec 6, 2018	Published

After the app is published on the Google Play console, it is added automatically to the App Catalog on Pulse One. For example:

FIGURE 147 Uploaded Android App Added to App Catalog



Title	Platform	Creator	Package	Category	Licenses
App testapp	Android	[redacted]	[redacted]		

After the app is in the App Catalog, you can add the app to a specific policy. For details, see **"Adding an Android App to a Policy" on page 130**.

Uploading Your In-House or Enterprise Apps using Google Play Console

To distribute an internal (in-house) Android app to the users under the corporate domain, the app needs to be published on Google Play Store and then restricted to users under the corporate Domain.

This section details the following steps:

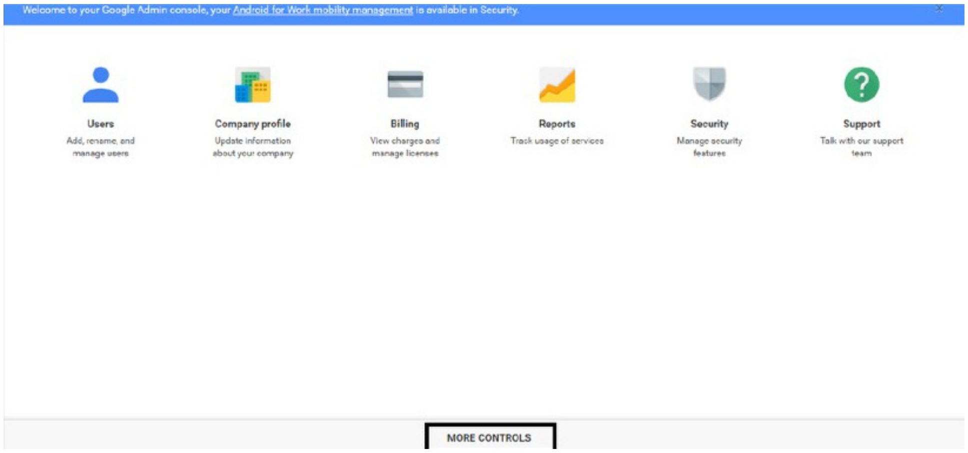
- "Logging into the Google Play Admin Console" on page 126.
- "Publishing a Private App on the Google Play Store" on page 127.
- "Approving a Private App for AFW Provisioning" on page 129.

Logging into the Google Play Admin Console

To log into the Google Admin Play console:

1. Sign in to Google Play Admin Console at https://admin.google.com.
2. Select **More Controls > APPS > Additional Google Services**.

FIGURE 148 Google Play Admin Console

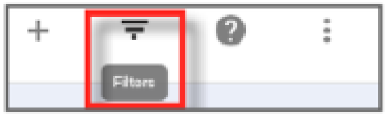


Welcome to your Google Admin console, your Android for Work mobility management is available in Security.

Users
Add, rename, and manage users
Company profile
Update information about your company
Billing
View charges and manage licenses
Reports
Track usage of services
Security
Manage security features
Support
Talk with our support team
MORE CONTROLS

3. Click the **Wifi** Icon to open the filter panel.

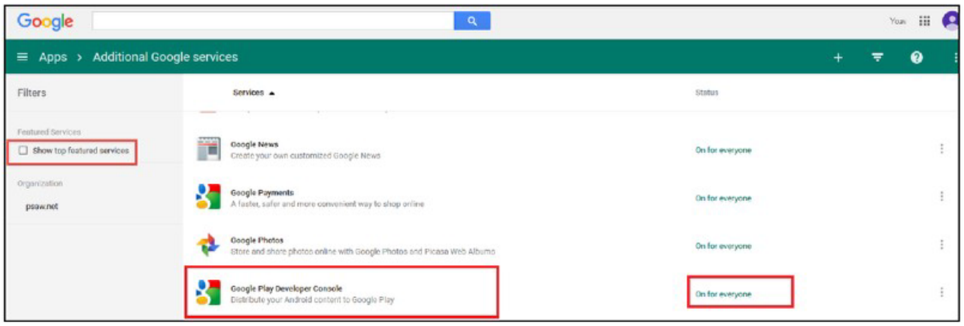
FIGURE 149 Wifi Icon



4. Under **Featured Services** filter, clear the **Show top featured services** check box.

5. Enable the **Google Play Developer Console service** by clicking the **On for everyone** status.

FIGURE 150 Additional Google Services

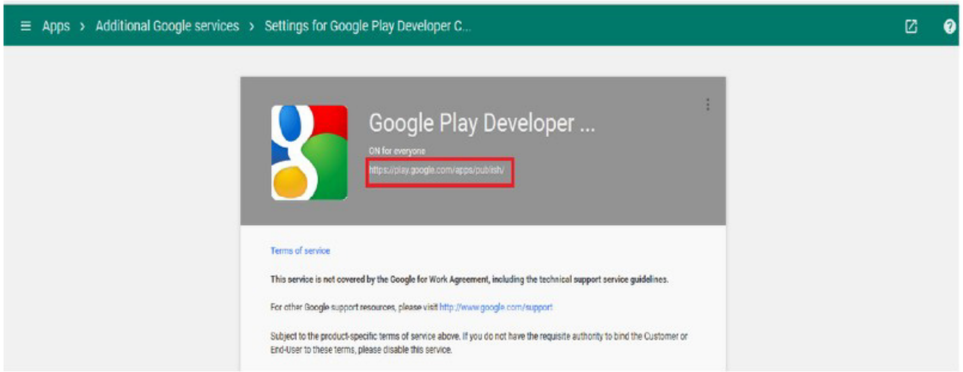

Google
You
Apps › Additional Google services
Filters
Featured Services
□ Show top featured services
Organization
psaw.net

Services ▲	Status
Google News Create your own customized Google News	On for everyone
Google Payments A faster, safer and more convenient way to shop online	On for everyone
Google Photos Store and share photos online with Google Photos and Picasa Web Albums	On for everyone
Google Play Developer Console Distribute your Android content to Google Play	On for everyone

Publishing a Private App on the Google Play Store

1. Launch the link https://play.google.com/apps/publish/ to upload the private app.

FIGURE 151 Publish the Private App on Google Play Store


Apps › Additional Google services › Settings for Google Play Developer C...
Google Play Developer ...
ON for everyone
https://play.google.com/apps/publish/
Terms of service

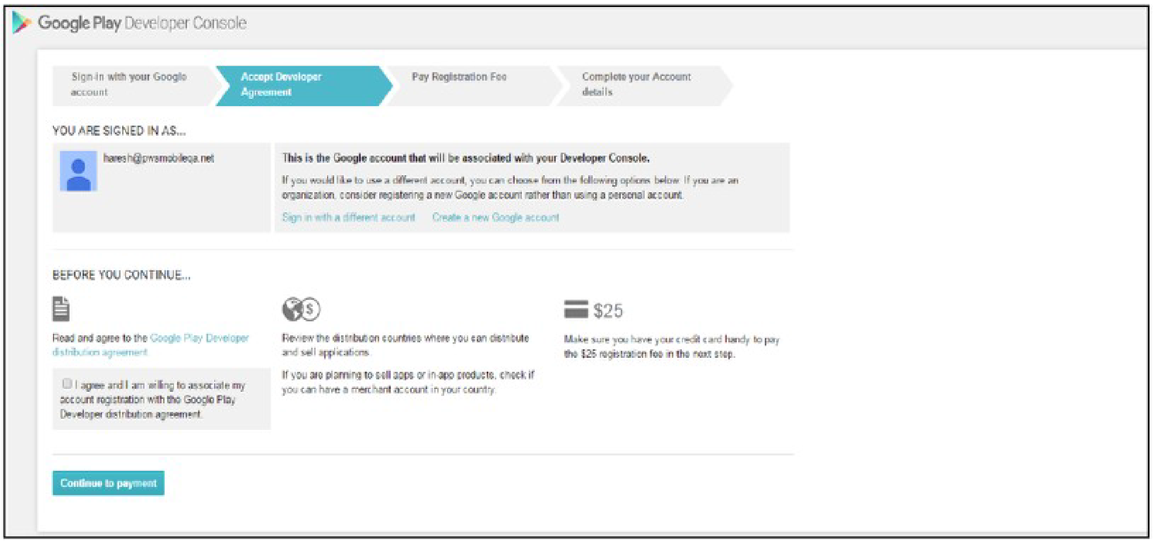
This service is not covered by the Google for Work Agreement, including the technical support service guidelines.

For other Google support resources, please visit http://www.google.com/support

Subject to the product-specific terms of service above. If you do not have the requisite authority to bind the Customer or End-User to these terms, please disable this service.

2. If required, pay the registration fee. The registration may take up to 48 hours to complete.

FIGURE 152 Accept Developer Agreement


Google Play Developer Console
Sign-in with your Google account
Accept Developer Agreement
Pay Registration Fee
Complete your Account details
YOU ARE SIGNED IN AS...
haresh@pwsmobileqa.net
Sign in with a different account
Create a new Google account
BEFORE YOU CONTINUE...
$25
Continue to payment

This is the Google account that will be associated with your Developer Console.

If you would like to use a different account, you can choose from the following options below. If you are an organization, consider registering a new Google account rather than using a personal account.

Read and agree to the Google Play Developer distribution agreement.

□ I agree and I am willing to associate my account registration with the Google Play Developer distribution agreement.

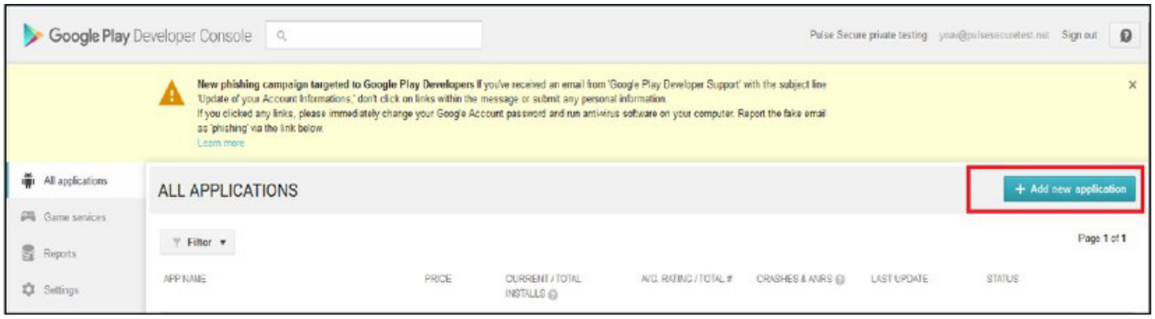
Review the distribution countries where you can distribute and sell applications.

If you are planning to sell apps or in-app products, check if you can have a merchant account in your country.

Make sure you have your credit card handy to pay the $25 registration fee in the next step.

3. Click the **Add new application** button and upload the APK. Add the required graphics and other mandatory information.

FIGURE 153 Add New Application

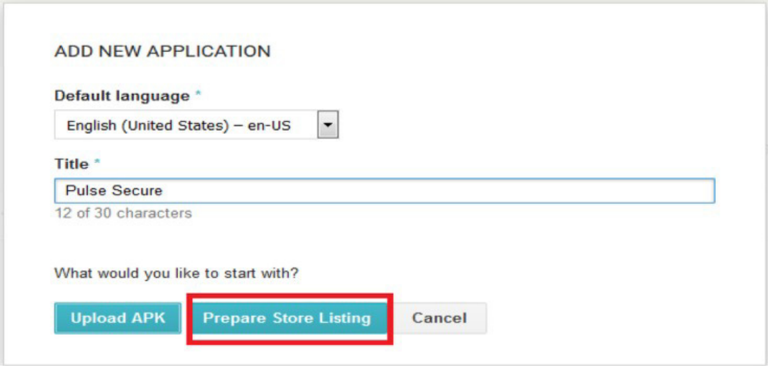


New phishing campaign targeted to Google Play Developers If you've received an email from 'Google Play Developer Support' with the subject line 'Update of your Account Informations,' don't click on links within the message or submit any personal information.
If you clicked any links, please immediately change your Google Account password and run anti-virus software on your computer. Report the fake email as 'phishing' via the link below.
Learn more

4. In the **Add New Application** page, select the language and enter a title for the application.

5. Click the **Prepare Store Listing** button.

FIGURE 154 Prepare Store Listing



ADD NEW APPLICATION

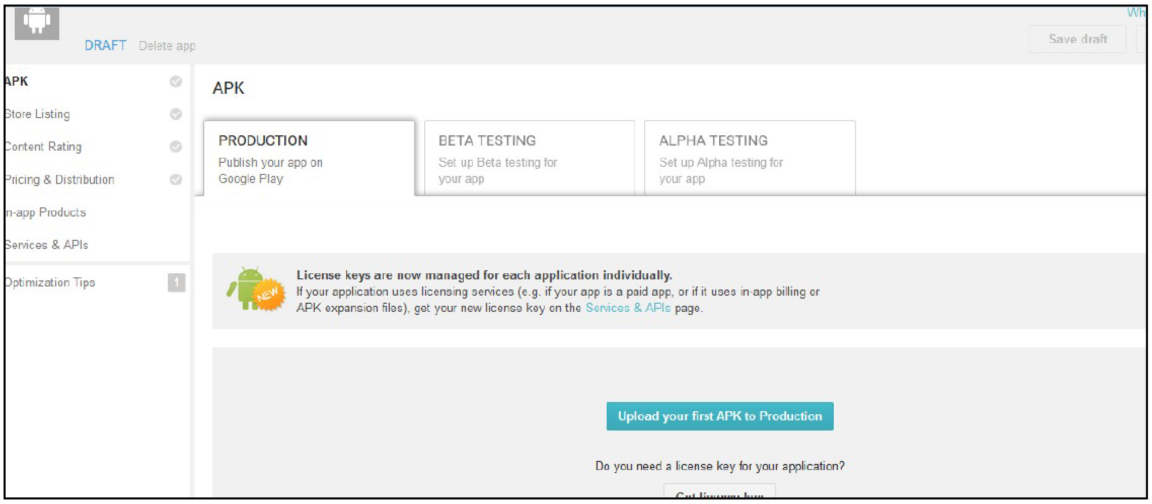
Default language *
English (United States) – en-US

Title *
Pulse Secure
12 of 30 characters

What would you like to start with?

6. Upload the new APK by clicking on the **Upload your first APK to Production** button.

FIGURE 155 Upload APK to Production

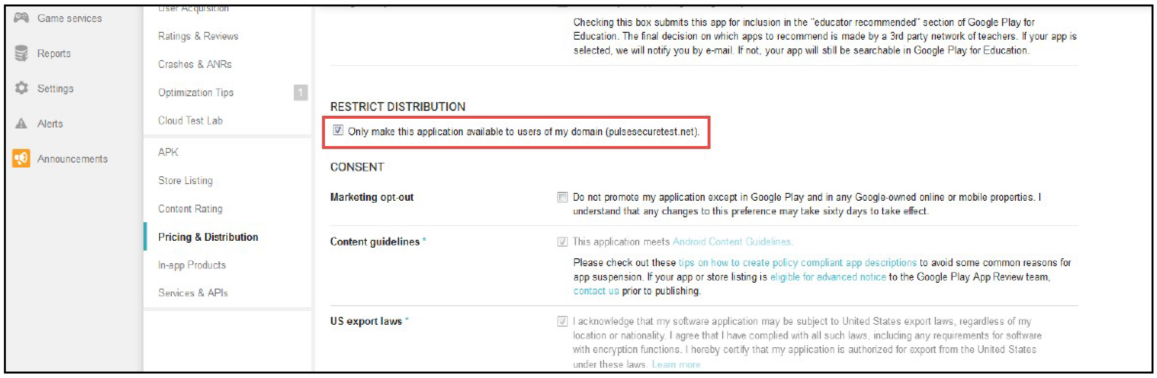


License keys are now managed for each application individually.
If your application uses licensing services (e.g. if your app is a paid app, or if it uses in-app billing or APK expansion files), get your new license key on the Services & APIs page.

Do you need a license key for your application?

7. Under **Pricing & Distribution**, select the **Only make this app available to users of my Google apps domain name** check box.

FIGURE 156 Restrict Distribution



Checking this box submits this app for inclusion in the "educator recommended" section of Google Play for Education. The final decision on which apps to recommend is made by a 3rd party network of teachers. If your app is selected, we will notify you by e-mail. If not, your app will still be searchable in Google Play for Education.

RESTRICT DISTRIBUTION

☑ Only make this application available to users of my domain (pulsesecuretest.net).

CONSENT

Marketing opt-out □ Do not promote my application except in Google Play and in any Google-owned online or mobile properties. I understand that any changes to this preference may take sixty days to take effect.

Content guidelines * ☑ This application meets Android Content Guidelines.

Please check out these tips on how to create policy compliant app descriptions to avoid some common reasons for app suspension. If your app or store listing is eligible for advanced notice to the Google Play App Review team, contact us prior to publishing.

US export laws * ☑ I acknowledge that my software application may be subject to United States export laws, regardless of my location or nationality. I agree that I have complied with all such laws, including any requirements for software with encryption functions. I hereby certify that my application is authorized for export from the United States under these laws. Learn more

Approving a Private App for AFW Provisioning

To approve a private app for AFW provisioning:

1. After uploading your app on the Play Store, sign in to your Pulse One console.
2. Add and approve this app for AFW provisioning. Then verify if the app is installed on the client.

   Refer the following Google support page for the procedure to distribute apps in your organization.

   - https://support.google.com/a/answer/2494992?hl=en

Configuring Policy Settings

This section describes the following procedures:

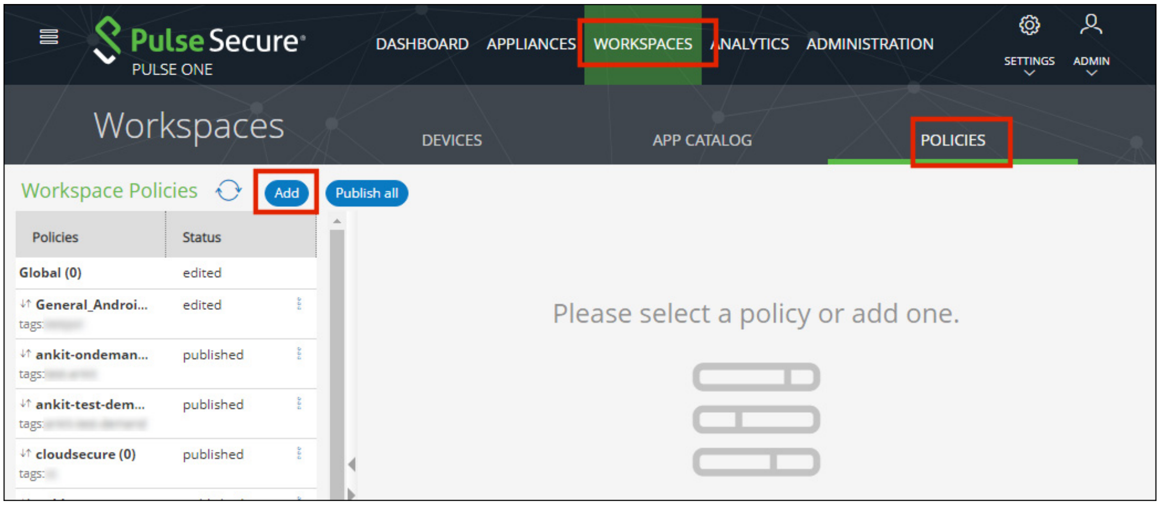
- "Adding an Android App to a Policy" on page 130.
- "Configuring Policy Properties" on page 134.
- "Setting a Password Policy" on page 136.

Adding an Android App to a Policy

To add an app to a policy:

1. Log in to Pulse One as an admin.
2. Select the **Workspaces** menu.
3. Select the **Policies** tab.
4. Click **Add** to add a new policy.

FIGURE 157 Add Policy

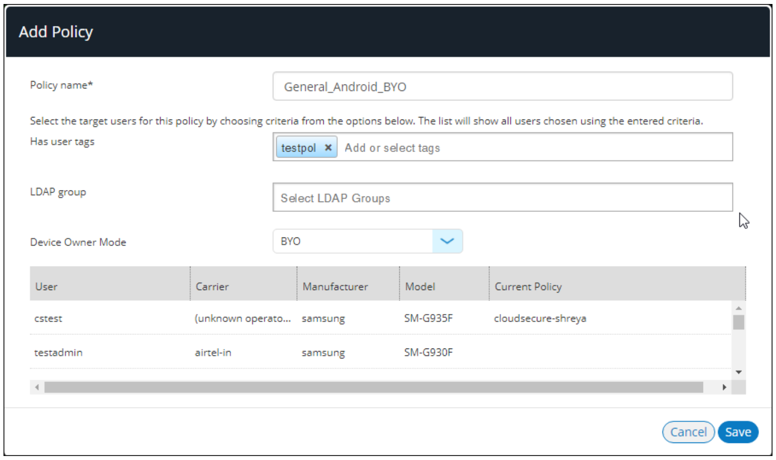


Policies	Status
Global (0)	edited
General_Androi... tags:	edited
ankit-ondeman... tags:	published
ankit-test-dem... tags:	published
cloudsecure (0) tags:	published

Please select a policy or add one.

5. Enter a **Policy Name**, complete the **Has user tags** property, and click **Save**. For example:

FIGURE 158 Add Policy Details



Add Policy

Policy name* General_Android_BYO

Select the target users for this policy by choosing criteria from the options below. The list will show all users chosen using the entered criteria.

Has user tags: testpol × Add or select tags

LDAP group: Select LDAP Groups

Device Owner Mode: BYO

User	Carrier	Manufacturer	Model	Current Policy
cstest	(unknown operato...	samsung	SM-G935F	cloudsecure-shreya
testadmin	airtel-in	samsung	SM-G930F	

The policy is added to the **Policies** list in the **Workspace Properties** page.

You must now add apps from the Google Play Store to this policy.

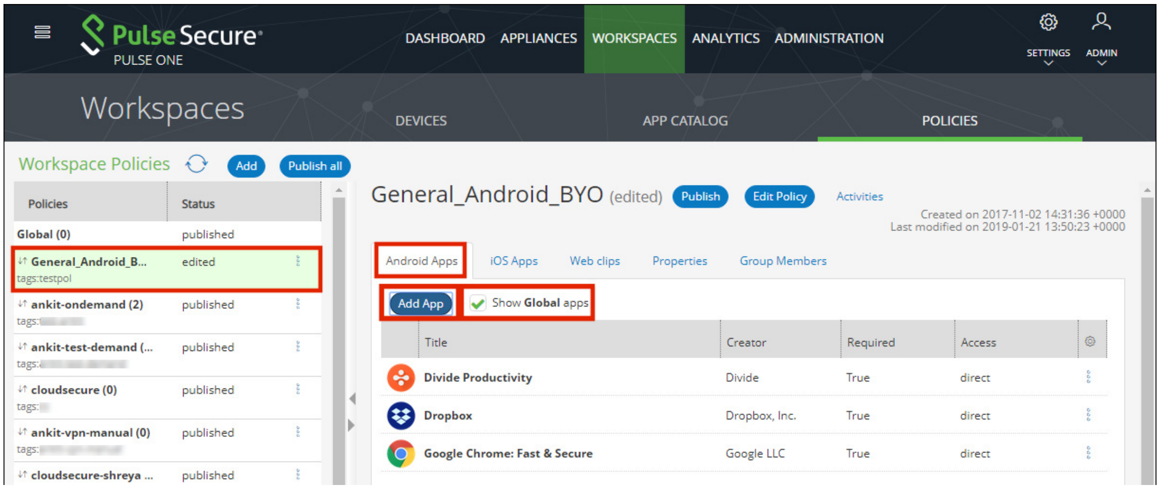
6. Click the **Android Apps** tab.

7. Enable the **Show Global apps** option.

A list of apps that are configured with global policy are displayed.

8. Click **Add App**.

FIGURE 159 Add App to Policy



Policies	Status
Global (0)	published
General_Android_B... tags:testpol	edited
ankit-ondemand (2) tags:[redacted]	published
ankit-test-demand (... tags:[redacted]	published
cloudsecure (0) tags:[redacted]	published
ankit-vpn-manual (0) tags:[redacted]	published
cloudsecure-shreya ...	published

General_Android_BYO (edited)

Created on 2017-11-02 14:31:36 +0000
Last modified on 2019-01-21 13:50:23 +0000

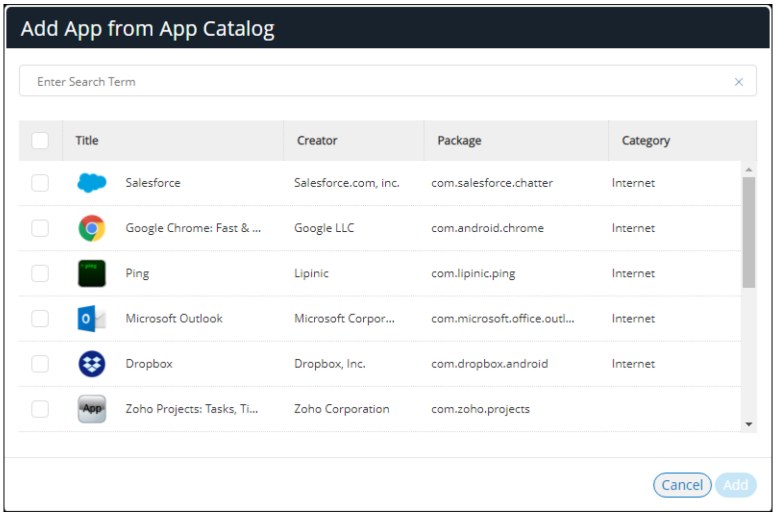
☑ Show **Global** apps

Title	Creator	Required	Access
Divide Productivity	Divide	True	direct
Dropbox	Dropbox, Inc.	True	direct
Google Chrome: Fast & Secure	Google LLC	True	direct

9. In the **Add App from App Catalog** dialog, enter the app name in the **Search** box and press **Enter**.

   A list of apps is displayed based on the search criteria. For example:

   FIGURE 160 Add App from App Catalog



Add App from App Catalog

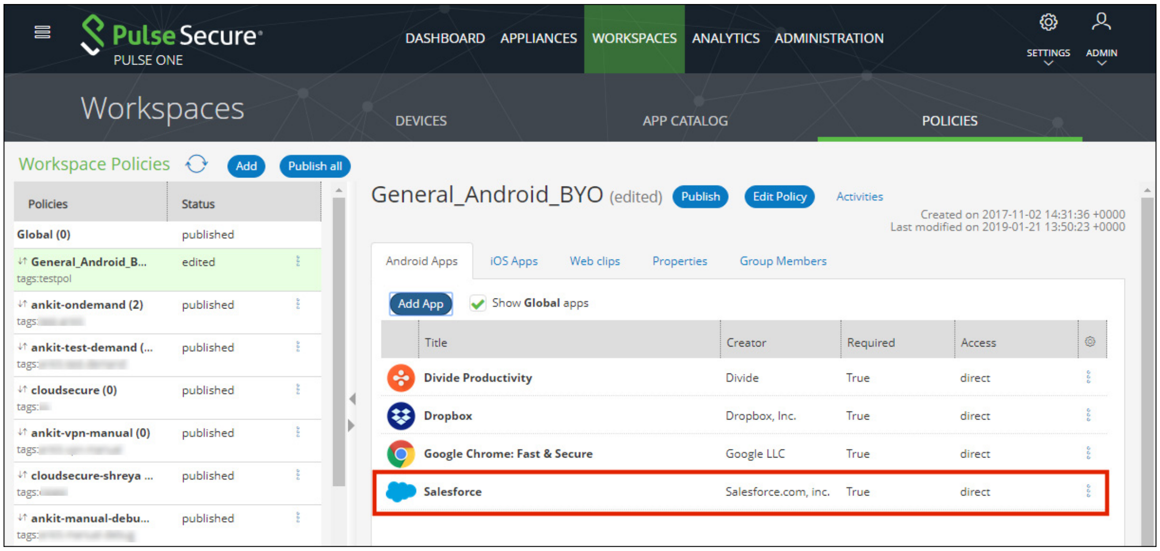
Enter Search Term

	Title	Creator	Package	Category
□	Salesforce	Salesforce.com, inc.	com.salesforce.chatter	Internet
□	Google Chrome: Fast & ...	Google LLC	com.android.chrome	Internet
□	Ping	Lipinic	com.lipinic.ping	Internet
□	Microsoft Outlook	Microsoft Corpor...	com.microsoft.office.outl...	Internet
□	Dropbox	Dropbox, Inc.	com.dropbox.android	Internet
□	Zoho Projects: Tasks, Ti...	Zoho Corporation	com.zoho.projects	

10. From the apps list, select the required app and click **Add**.

    The app is added to the policy. For example:

    FIGURE 161 Updated App List for Policy



Policies	Status
Global (0)	published
General_Android_B... tags:testpol	edited
ankit-ondemand (2) tags:[redacted]	published
ankit-test-demand (... tags:[redacted]	published
cloudsecure (0) tags:[redacted]	published
ankit-vpn-manual (0) tags:[redacted]	published
cloudsecure-shreya ... tags:[redacted]	published
ankit-manual-debu... tags:[redacted]	published

General_Android_BYO (edited)

Created on 2017-11-02 14:31:36 +0000
Last modified on 2019-01-21 13:50:23 +0000

☑ Show **Global** apps

Title	Creator	Required	Access
Divide Productivity	Divide	True	direct
Dropbox	Dropbox, Inc.	True	direct
Google Chrome: Fast & Secure	Google LLC	True	direct
Salesforce	Salesforce.com, inc.	True	direct

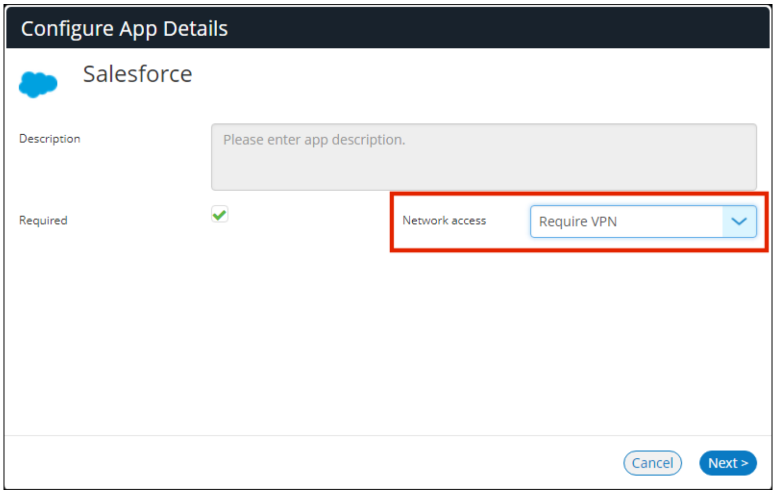
11. In the **Android Apps** list, select the **Actions** icon (⋮) for the app and click **Edit app rule**.

    The **Configure App Details** dialog appears.

12. Make the required configuration changes.

    For example, if you access the app through VPN only, then set **Network access** to *Require VPN*.

    FIGURE 162 Configure App Details

    Description: Please enter app description.

    Required: ☑

    Network access: Require VPN

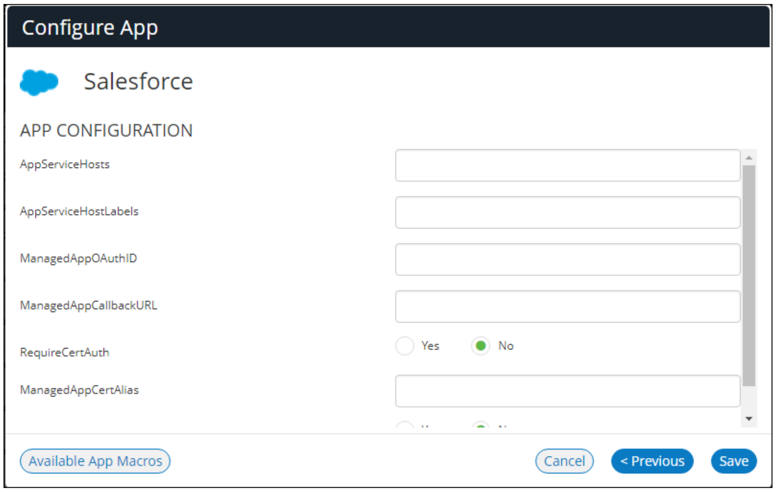
    Note: You cannot change the **Description**.

13. Click **Next**.

    The **Configure App** dialog appears.

14. Supply the required configuration and click **Save**. For example:

    FIGURE 163 Configure App

    APP CONFIGURATION

    AppServiceHosts:

    AppServiceHostLabels:

    ManagedAppOAuthID:

    ManagedAppCallbackURL:

    RequireCertAuth: ○ Yes ● No

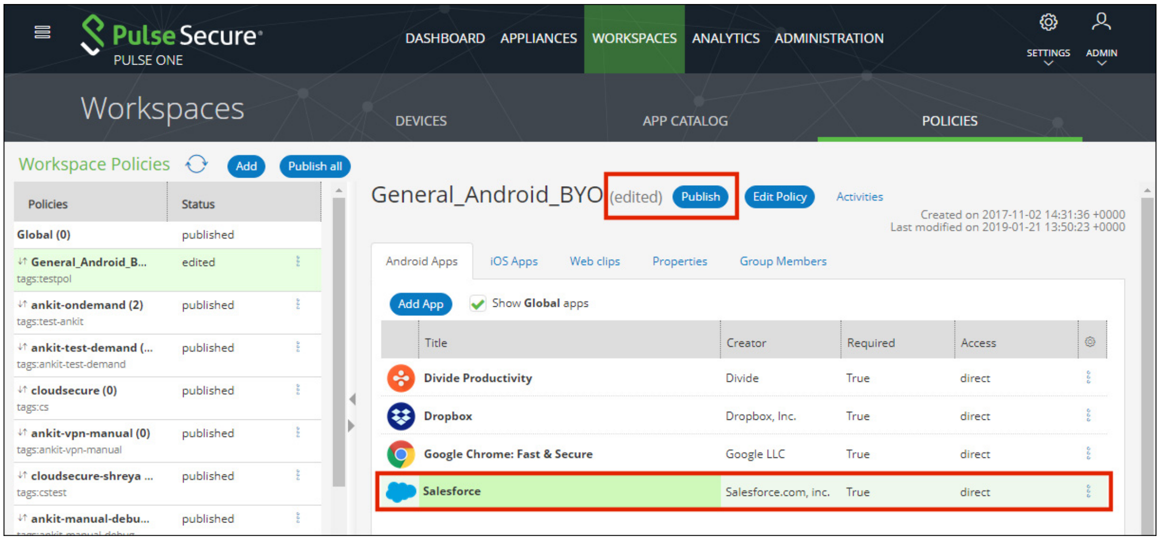
    ManagedAppCertAlias:

15. Some apps need permissions to access. For these apps, the **App Permissions** dialog appears. Select the required permissions for the app and click **Save**.

    For information about enabling app permission property and configuring default runtime permission, see **"Managing Pulse One Properties" on page 267**.

16. Select the app from the app list and click **Publish**.

FIGURE 164 Publish App



Created on 2017-11-02 14:31:36 +0000
Last modified on 2019-01-21 13:50:23 +0000

Policies	Status
Global (0)	published
General_Android_B... tags:testpol	edited
ankit-ondemand (2) tags:test-ankit	published
ankit-test-demand (... tags:ankit-test-demand	published
cloudsecure (0) tags:cs	published
ankit-vpn-manual (0) tags:ankit-vpn-manual	published
cloudsecure-shreya ... tags:cstest	published
ankit-manual-debu...	published

Title	Creator	Required	Access
Divide Productivity	Divide	True	direct
Dropbox	Dropbox, Inc.	True	direct
Google Chrome: Fast & Secure	Google LLC	True	direct
Salesforce	Salesforce.com, inc.	True	direct

The **Publish** confirmation dialog appears.

17. Click **Yes**. The app is published.

This completes adding an Android app to a policy.

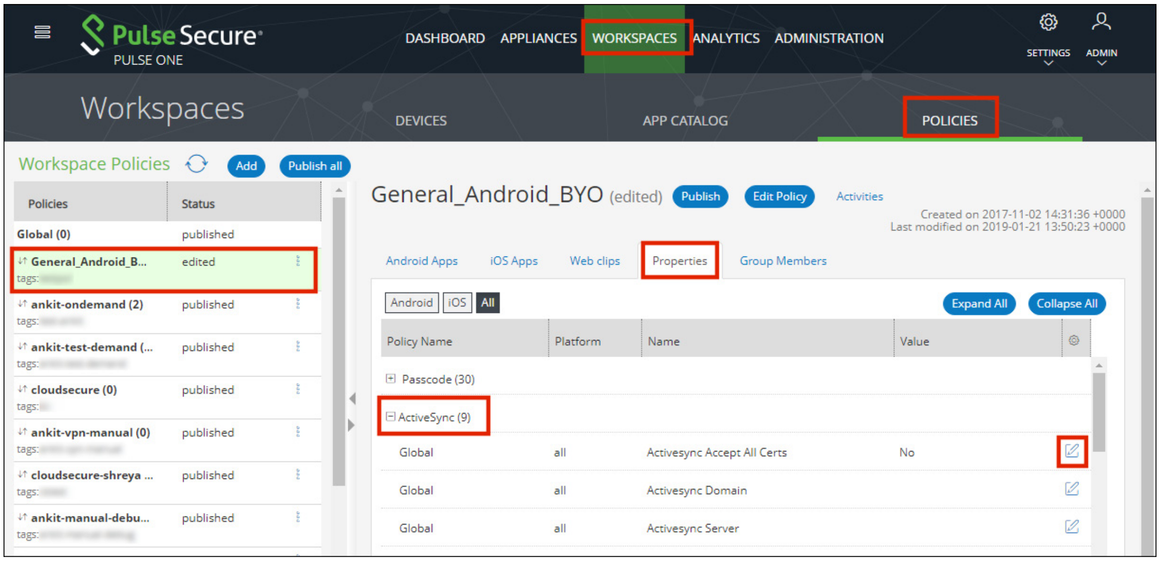
Configuring Policy Properties

To set the properties for a policy:

1. Select the **Workspace** tab.
2. Select the **Policies** tab.
3. Select the required policy.
4. Click the **Properties** tab for the policy.
5. Expand the required collection of policies. For example, *ActiveSync*.

6. Locate the required policy in the expanded list and click its **Edit** icon.

FIGURE 165 Edit Policy



General_Android_BYO (edited)

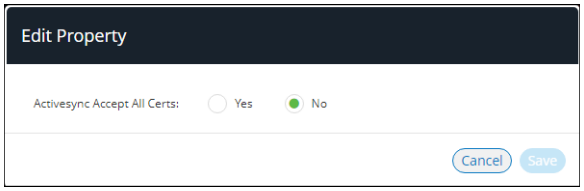
Created on 2017-11-02 14:31:36 +0000
Last modified on 2019-01-21 13:50:23 +0000

Policies	Status
Global (0)	published
General_Android_B... tags: [redacted]	edited
ankit-ondemand (2) tags: [redacted]	published
ankit-test-demand (... tags: [redacted]	published
cloudsecure (0) tags: [redacted]	published
ankit-vpn-manual (0) tags: [redacted]	published
cloudsecure-shreya ... tags: [redacted]	published
ankit-manual-debu... tags: [redacted]	published

Policy Name	Platform	Name	Value
⊞ Passcode (30)			
⊟ ActiveSync (9)			
Global	all	Activesync Accept All Certs	No
Global	all	Activesync Domain	
Global	all	Activesync Server	

7. Make the required changes and **Save** each. For example:

FIGURE 166 Edit Property



Activesync Accept All Certs: ○ Yes ● No

Setting a Password Policy

Android password settings are categorized into: *quality*, *expiration* and *complex*. For details of the password policy properties, see **"Understanding Policy Properties" on page 167**.

Password policies are configured in the admin console and deployed on Android devices.

- Devices running Android v6 (or earlier) support workspace management device passcodes only.
- Devices running Android v7 (or later) support both workspace management device passcodes and work profile passcodes. These can be used simultaneously.

To set a password:

1. Select the **Workspace** tab.
2. Select the **Policies** tab.
3. Select the required policy.
4. Click the **Properties** tab.
5. Expand the *Passcode* category.
6. Set the following properties for the *workspace management device passcode*:
    - **Expiration Days** – The number of days for which the passcode can remain unchanged.
    - **Lock Timeout** – The time in seconds where the Workspace will be locked if no Workspace app was in the foreground.
    - **Max Tries (iOS Factory Reset)** – The number of allowed failed attempts to enter the passcode at the device's lock screen.
    - **Numeric Only** – Boolean. If *True*, the user must to set a PIN.
    - **Passcode History** – When the user changes the passcode, it must be unique within the most recent specified number of entries in the history.
    - **Passcode Length** – The minimum overall length of the passcode.
    - **Require Special** – The minimum count of special characters in a passcode.

      Note: For Android, this is used for Workspace Managed Device Passcodes only.
    - **Require Letters** – The minimum count of letters in a Workspace Managed Device passcode.
    - **Require Lowercase** – The minimum count of lowercase letters in a Workspace Managed Device passcode.
    - **Require Non-Letters** – The minimum count of numbers and symbols in a Workspace Managed Device passcode.

- **Require Number** – The minimum count of numbers in a Workspace Managed Device passcode.
- **Require Uppercase** – The minimum count of uppercase letters in a Workspace Managed Device passcode.
- **Screenlock Password Quality** – The screen unlock mechanism. This can be set to *none*, *biometric*, *password*, *pattern*, *pin*, *pin_complex*, *alpha*, *alphanumeric* and *complex*.
    - If the device uses a different screen lock type to the one specified by the policy, the device is flagged as non-compliant.
    - If the screen unlock type is password, then **Passcode Length** and **Passcode History** policies are enforced.
    - If the screen unlock type is *pin* or *pin_complex*, then **Passcode History** policies are enforced.

7. For Android v7.0 (or later) you can also set the following properties for the *work profile passcode*:
    - **(Work Profile) Expiration Days** – The number of days for which the passcode can remain unchanged.
    - **(Work Profile) Lock Timeout** – The time in seconds where the Workspace will be locked if no Workspace app was in the foreground.
    - **(Work Profile) Max Tries** – The number of allowed failed attempts to enter the passcode at the device's lock screen.
    - **(Work Profile) Numeric Only** – Boolean. If *True*, the user is forced to set a PIN.
    - **(Work Profile) Passcode History** – When the user changes the passcode, it must be unique within the most recent specified number of entries in the history.
    - **(Work Profile) Passcode Length** – The minimum overall length of the passcode.
    - **(Work Profile) Require Letters** – The minimum count of letters in a passcode.
    - **(Work Profile) Require Lowercase** – The minimum count of lowercase letters in a passcode.
    - **(Work Profile) Require Non-Letters** – The minimum count of numbers and symbols in a passcode.
    - **(Work Profile) Require Number** – The minimum count of numbers in a passcode.
    - **(Work Profile) Require Special** – The minimum count of special characters in a passcode.
    - **(Work Profile) Require Uppercase** – The minimum count of uppercase letters in a passcode.

- **(Work Profile) Screenlock Password Quality** – The screen unlock mechanism. This can be set to *none*, *biometric*, *password*, *pattern*, *pin*, *pin_complex*, *alpha*, *alphanumeric* and *complex*.
    - If the device uses a different screen lock type to the one specified by the console, the device is flagged as non-compliant.
    - If the screen unlock type is password, then **Passcode Length** and **Passcode History** policies are enforced.
    - If the screen unlock type is *pin* or *pin_complex*, then **Passcode History** policies are enforced.

8. After the password policy is complete, **Publish** the policy to all devices that use it.

Note: If a user has not defined a screen lock in his device, then the password policy defined by the admin will be forced to the user's device.

Workspace Management

Managing Users

Pulse One users with a Workspace license entitlement can manage Workspaces from the **Workspaces** menu.

- "Adding a User" on page 139.
- "Deleting a User" on page 141.
- "Verifying an LDAP Group" on page 142.
- "Adding a Policy Tag to a Workspace User Account" on page 143.
- "Performing Workspace Actions" on page 143.
- "Understanding the Workspace Details Window" on page 146.

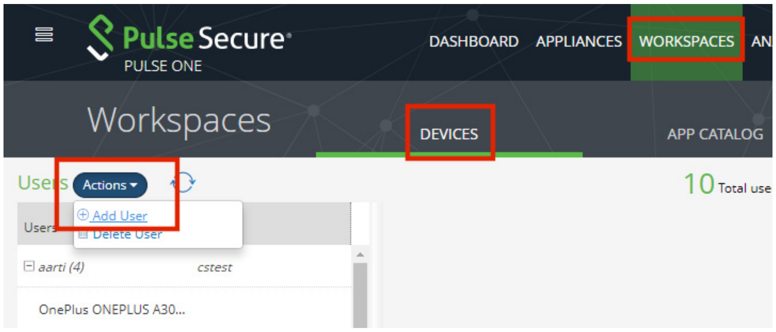
Adding a User

This section details the steps to add a new user (workspace) to your domain.

1. Select the **Workspaces** menu.
2. Select the **Devices** tab. A list of **Users** appears.

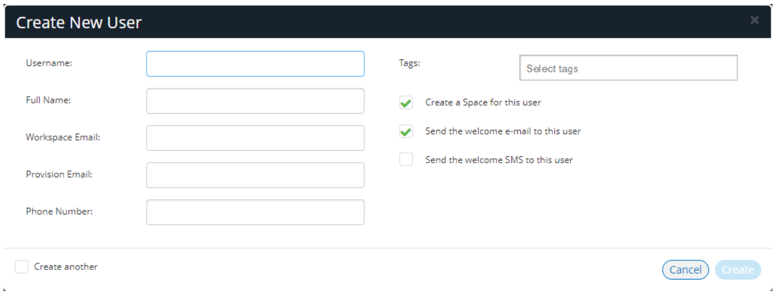
3. Click the **Actions** drop-down menu, and click **Add User**.

FIGURE 167 Add User



The **Create New User** dialog appears.

FIGURE 168 Create New User


Create New User

Username:

Full Name:

Workspace Email:

Provision Email:

Phone Number:

Tags: Select tags

☑ Create a Space for this user

☑ Send the welcome e-mail to this user

☐ Send the welcome SMS to this user

☐ Create another

4. Complete the **required fields:**

   - **Username** – The user name. This must be unique. This property can be used to configure the email client inside the workspace during the provisioning process.
   - **Full Name** – User's full name.
   - **Workspace Email** – Email account to which workspace notifications are sent. This account can also be used to configure the email client inside the workspace during the provisioning process.
   - **Provision Email** – Email account to which the welcome email is sent

5. (Optional) Complete the following fields:

   - **Phone Number** – Phone number to which the welcome SMS is sent.
   - **Tags** – Tags assigned to this user, used for policy assignment.

6. (Optional) Select the required state for the following options:

   - **Create a Space for this user**
   - **Send the welcome email to this user**
   - **Send the welcome SMS to this user**

7. Click **Create** to complete the process.

   The new user is added to the **Users** list.

Deleting a User

This section details the steps to delete a user from your domain.

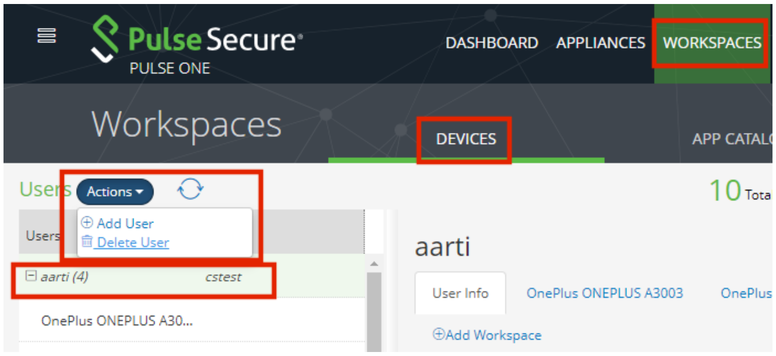
Note: You must delete all workspaces/devices from a user before you can delete the user.

1. Select the **Workspaces** menu.
2. Select the **Devices** tab.

   A list of **Users** appears.
3. Locate the required user, or (optionally) click the **Search** button and use the search box.
4. Expand the user you want to delete.

   A list of the workspaces/devices registered to that user appears.
5. Delete each individual workspace/device from the user by using **Actions > Delete Workspace**.
6. After all workspaces/devices are deleted, select the user you want to delete.
7. Click the **Actions** drop-down menu, and click **Delete User**.

   FIGURE 169 Delete User



   A confirmation dialog appears.
8. Click **Yes** to confirm the user deletion.

   The selected user is removed from the **Users** list.

Verifying an LDAP Group

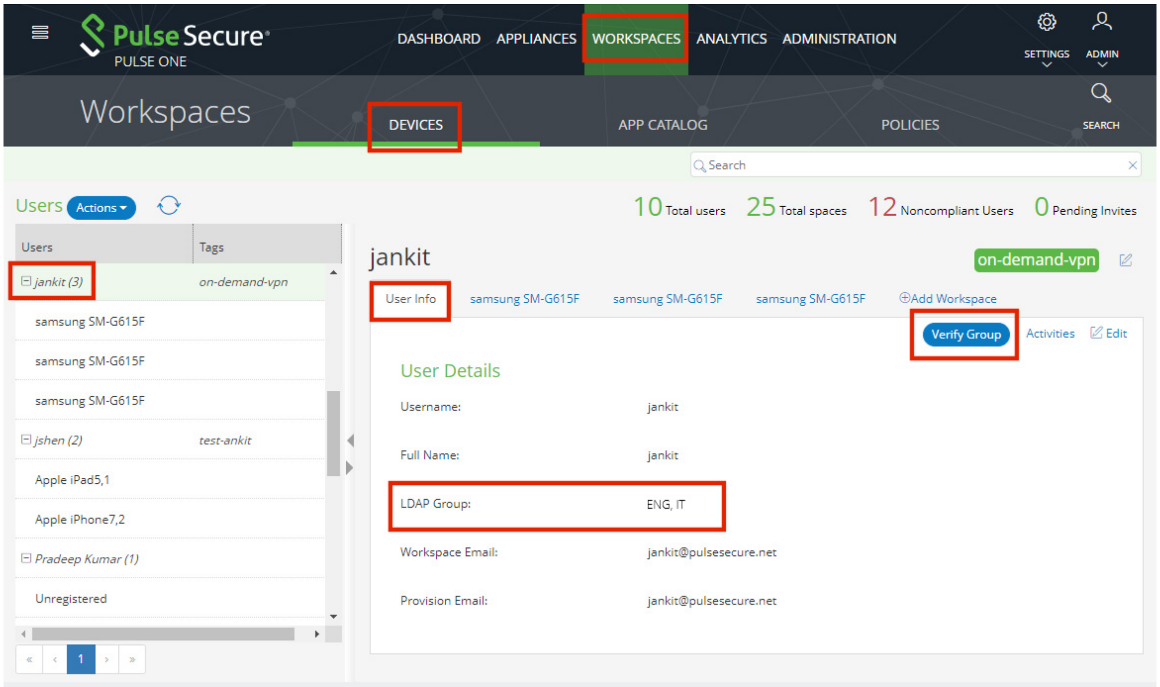
When a user group is changed in the back-end Active Directory server, the change is not immediately reflected in the User Info page. The **Verify Group** button is provided to re-verify the user's LDAP group and recalculate the policy for the user.

To verify an LDAP group for a user:

1. Select the **Workspaces** menu.
2. Select the **Devices** tab. A list of **Users** appears.
3. Locate the required user in the list, or (optionally) click the **Search** button and use the search box.
4. Select the **User Info** tab in the right-hand panel.
5. Click the **Verify Group** button.

   The LDAP group updates and the corresponding policy is reapplied to the user. For example:

FIGURE 170 Verify Group



10 Total users 25 Total spaces 12 Noncompliant Users 0 Pending Invites

Users	Tags
jankit (3)	on-demand-vpn
samsung SM-G615F	
samsung SM-G615F	
samsung SM-G615F	
jshen (2)	test-ankit
Apple iPad5,1	
Apple iPhone7,2	
Pradeep Kumar (1)	
Unregistered	

jankit

User Details

Username:	jankit
Full Name:	jankit
LDAP Group:	ENG, IT
Workspace Email:	jankit@pulsesecure.net
Provision Email:	jankit@pulsesecure.net

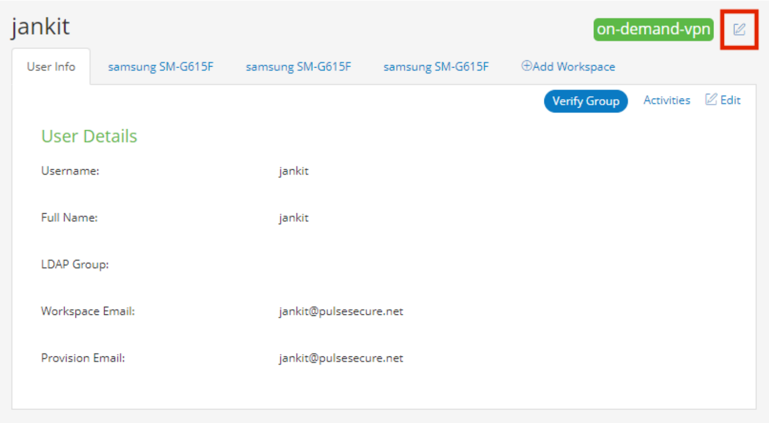
Adding a Policy Tag to a Workspace User Account

Tags are used to apply policies to users' accounts. After a policy is tagged, just add the same tag to the user to apply the policy to that user's device.

This section describes the steps to apply a policy tag to a Workspace User Space.

1. Select the **Workspaces** menu.
2. Select the **Devices** tab. A list of **Users** appears.
3. Locate the required user in the list, or (optionally) click the **Search** button and use the search box.
4. Click the **Tags** icon located at the corner of the user details panel. For example:

FIGURE 171 Tags Icon



Username: jankit

Full Name: jankit

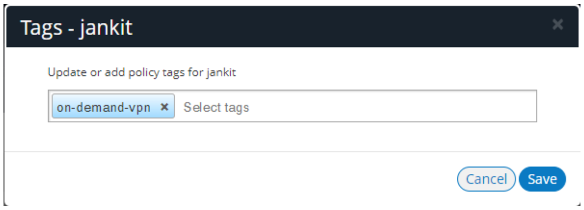
LDAP Group:

Workspace Email: jankit@pulsesecure.net

Provision Email: jankit@pulsesecure.net

The **Tags** dialog appears. For example:

FIGURE 172 Add Tags



Update or add policy tags for jankit

on-demand-vpn × Select tags

5. Update or add policy tags to the user and click **Save**.

Performing Workspace Actions

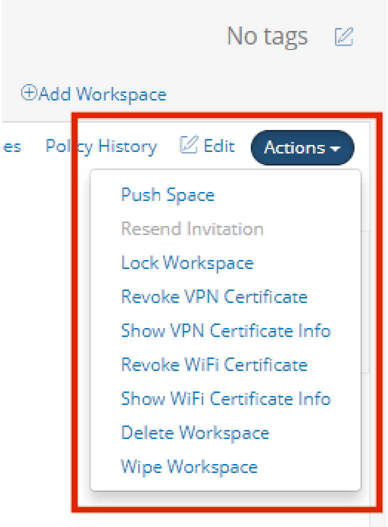
This section details the steps to perform administrative actions on a workspace.

1. Select the **Workspaces** menu.
2. Select the **Devices** tab. A list of **Users** appears.
3. Locate the required user in the list, or (optionally) click the **Search** button and use the search box.

4. Expand the required user, and select the required workspace.

5. Select **Actions** from the Workspace panel. For example:

FIGURE 173 Select the User and Workspace



6. Select the action you want to perform:

   Note: All possible actions are listed below. However, all actions cannot be seen simultaneously.

   - **Push Space** – sends the latest policy to the user's device and forces a check-in.
   - **Resend Invitation** – resends the Workspace Welcome email or SMS with a new registration token.

     Note: This action is only available before the Workspace has been provisioned.
   - **Reset Passcode** – resets the Workspace passcode (supported in iOS devices only).
   - **Lock Workspace** – (Android only) Locks the device.
   - **Lock Device** – (iOS only) Locks the device.
   - **Show VPN Certificate Info** – shows if the VPN certificate is valid. This action is not active when **Force Update VPN Cert** is present.
   - **Revoke VPN Certificate** – prompts to revoke the VPN certificate. This action is not active when **Force Update VPN Cert** is present.
   - **Unrevoke VPN Certificate** – prompts to reverse a revoke request on the VPN certificate.
   - **Force Update VPN Cert** – where an external PKI server is configured, this forces a fetch of a new VPN certificate from the external PKI Server using SCEP. This action is not active when either **Revoke VPN Certificate** or **Show VPN Certificate Info** are present. See the required settings in **"Enterprise PKI Integration" on page 183**.

- **Show Wifi Certificate Info** – shows if the WiFi certificate is valid. This action is not active when **Force Update Wifi Cert** is present.
- **Revoke Wifi Certificate** – prompts to revoke WiFi certificate. This action is not active when **Force Update Wifi Cert** is present.
- **Unrevoke Wifi Certificate** – prompts to reverse a revoke request on the WiFi certificate.
- **Force Update WiFi Cert** – where an external PKI server is configured, this forces a fetch of a new WiFi certificate from the external PKI Server using SCEP. This action is not active when either **Revoke Wifi Certificate** or **Show Wifi Certificate Info** are present. See the required settings in **"Enterprise PKI Integration" on page 183**.
- **Update Location** – updates the location of the device (iOS only), see **"Locating a Device" on page 249**.
- **Lost Mode** – indicates that the device is lost, see **"Working with Lost Mode for a Device" on page 250**.
- **Request Lost Mode Location** – requests a location update for a lost device (iOS only), see **"Working with Lost Mode for a Device" on page 250**. This command is only active when a device is in Lost Mode.
- **Play Lost Mode Sound** – requests that a continuous loud tone is played on a lost device (iOS only), see **"Working with Lost Mode for a Device" on page 250**. This command is only active when a device is in Lost Mode.
- **Disable Lost Mode** – cancels lost mode for a device (iOS only) after it is returned to its user, see **"Working with Lost Mode for a Device" on page 250**. This command is only active when a device is in Lost Mode.
- **Delete Workspace** – deletes the Workspace record from the Management server.

  Note: When a Workspace is deleted, no further administrative actions can be performed on the Workspace, including wiping the Workspace.
- **Wipe Workspace** – wipes all enterprise data from the device. A confirmation appears.

  Note: This action will un-enroll the device and permanently delete enterprise data, apps, and configuration. All personal information on the device remains intact.

  Note: This action does not appear for corporate owned devices, as it would perform the same action as a **Full Device Wipe** (see below).
- **Full Device Wipe** – wipes the entire device back to its factory defaults. A confirmation appears.

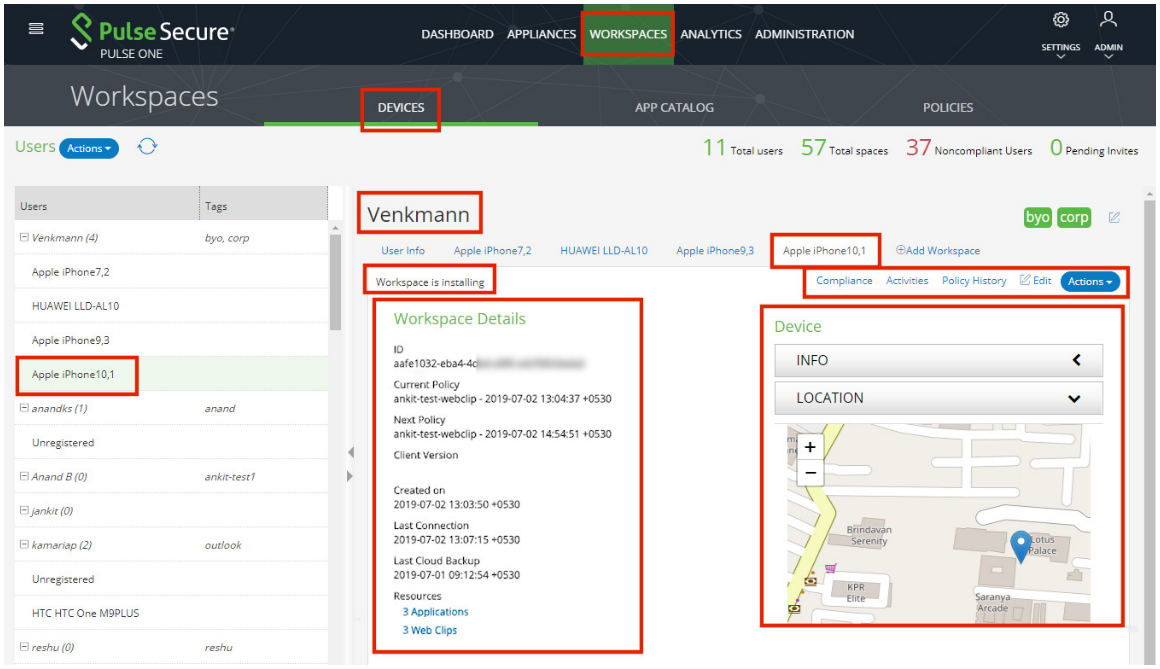
  Note: This action requires that the **Allow the ability to perform full device wipes?** workspace property is enabled for the policy, see **"Workspaces" on page 182**.

Understanding the Workspace Details Window

The **Devices** panel allows you to view the overall status of the workspace.

- **Device Manufacturer/Model** – used to identify the workspace.
- **Workspace State** – the status of the workspace.
- **Workspace Apps** – the apps installed in the workspace.
- **Workspace Details** – the workspace details. This includes **Resources**, which lists:
  - The number of apps on this policy, and hyperlink to the app(s).
  - (iOS only) The number of web clips on this policy, and hyperlink to the web clip(s).
- **Device Info** – information gathered from the device.
- **Device Location** – physical device location gathered from the device (iOS only) and displayed on a map, see **"Working with Device Location" on page 235**.

FIGURE 174 Workspace panel



11 Total users 57 Total spaces 37 Noncompliant Users 0 Pending Invites

Users	Tags
Venkmann (4)	byo, corp
Apple iPhone7,2	
HUAWEI LLD-AL10	
Apple iPhone9,3	
Apple iPhone10,1	
anandks (1)	anand
Unregistered	
Anand B (0)	ankit-test1
jankit (0)	
kamariap (2)	outlook
Unregistered	
HTC HTC One M9PLUS	
reshu (0)	reshu

Venkmann

Workspace is installing

Workspace Details

ID
aafe1032-eba4-4c[redacted]

Current Policy
ankit-test-webclip - 2019-07-02 13:04:37 +0530

Next Policy
ankit-test-webclip - 2019-07-02 14:54:51 +0530

Client Version

Created on
2019-07-02 13:03:50 +0530

Last Connection
2019-07-02 13:07:15 +0530

Last Cloud Backup
2019-07-01 09:12:54 +0530

Resources
3 Applications
3 Web Clips

The **Compliance** tab displays the status of device properties and whether they are compliant with the Workspace security policy.

Android devices support the following properties, and indicates if the current value is compliant:

- **Compliance Rooted Detection** – Indicates whether the device is Rooted or Non-Rooted.
- **Policy Expired** – Indicates if the policy is expired (Yes / No).
- **Compliance USB debugging** – Indicates whether debugging is USB Enabled or USB Disabled.

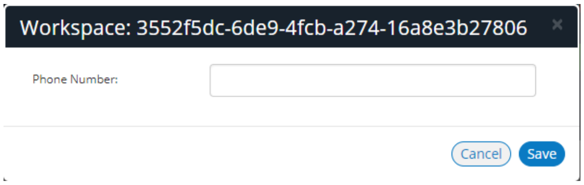
- **Profile password complexity** – Indicates the profile password type. That is: none, biometric, password, pattern, pin, pin_complex, alpha, alphanumeric or complex.
- **Device password complexity** – Indicates the device password type. That is: none, biometric, password, pattern, pin, pin_complex, alpha, alphanumeric or complex.

iOS devices support the following properties, and indicates if the current value is compliant:

- **Jailbreak Detection** – Indicates whether jailbreak detection is enabled (Yes / No).
- **Policy Expired** – Indicates if the policy is expired (Yes / No).
- **iOS Minimum OS version** – Indicates the policy's minimum OS version.
- **iOS Pulse Client Denied To Use Location Service** – Indicates whether the device can use the location service, see **"Working with Device Location" on page 235**.
- **iOS Minimum Pulse Client version** – Indicates the policy's minimum Pulse Client version.

The **Edit** window allows you to view and edit the phone number to which the welcome SMS is sent. For example:

FIGURE 175 Workspace Details

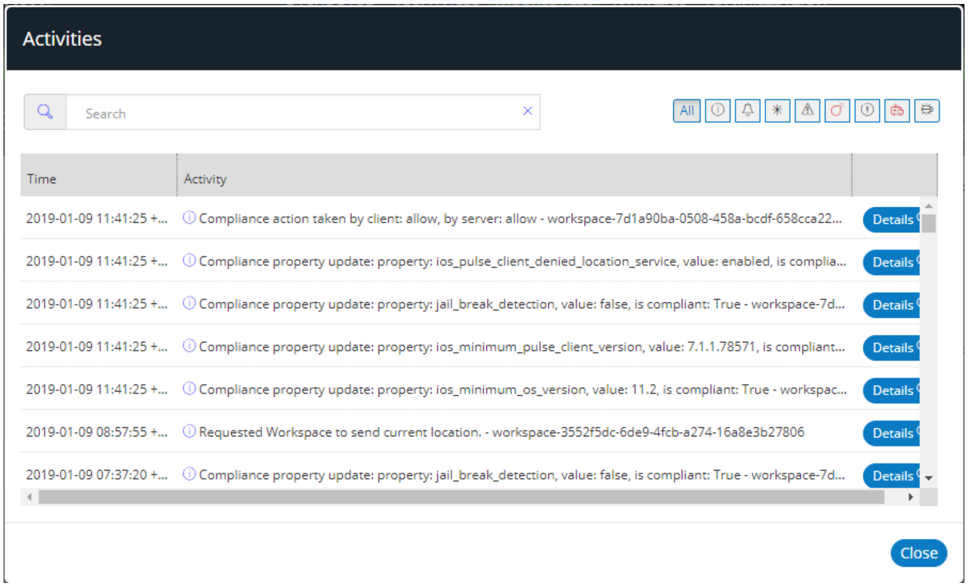


Workspace: 3552f5dc-6de9-4fcb-a274-16a8e3b27806

Phone Number:

The **Activities** window displays the log of Workspace activity. Double click an activity to see the detailed view.

FIGURE 176 Activities



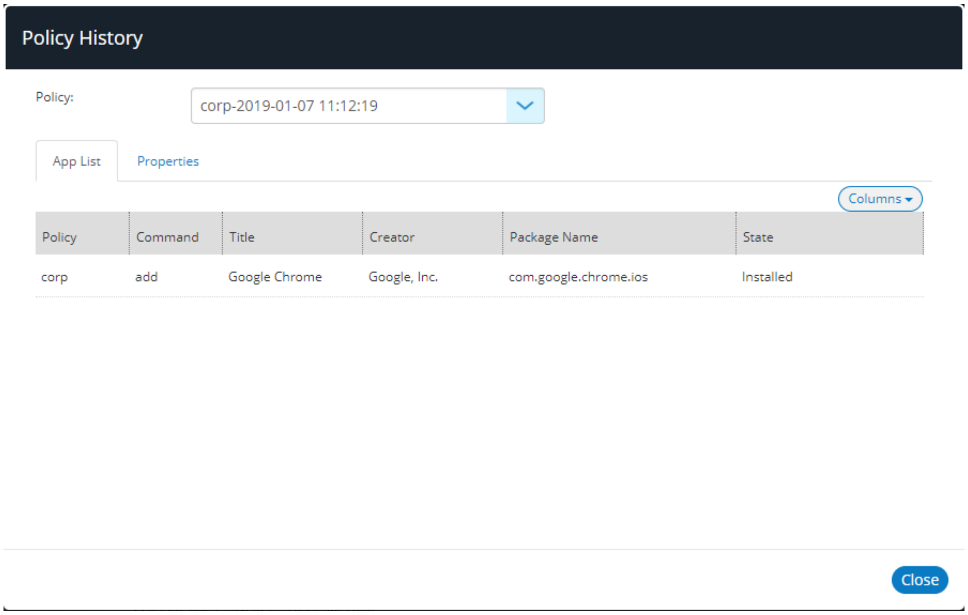
Activities

Search

Time	Activity	
2019-01-09 11:41:25 +...	ⓘ Compliance action taken by client: allow, by server: allow - workspace-7d1a90ba-0508-458a-bcdf-658cca22...	Details
2019-01-09 11:41:25 +...	ⓘ Compliance property update: property: ios_pulse_client_denied_location_service, value: enabled, is complia...	Details
2019-01-09 11:41:25 +...	ⓘ Compliance property update: property: jail_break_detection, value: false, is compliant: True - workspace-7d...	Details
2019-01-09 11:41:25 +...	ⓘ Compliance property update: property: ios_minimum_pulse_client_version, value: 7.1.1.78571, is compliant...	Details
2019-01-09 11:41:25 +...	ⓘ Compliance property update: property: ios_minimum_os_version, value: 11.2, is compliant: True - workspac...	Details
2019-01-09 08:57:55 +...	ⓘ Requested Workspace to send current location. - workspace-3552f5dc-6de9-4fcb-a274-16a8e3b27806	Details
2019-01-09 07:37:20 +...	ⓘ Compliance property update: property: jail_break_detection, value: false, is compliant: True - workspace-7d...	Details

The **Policy History** window displays the current and previous policies applied to a Workspace.

FIGURE 177 Policy History



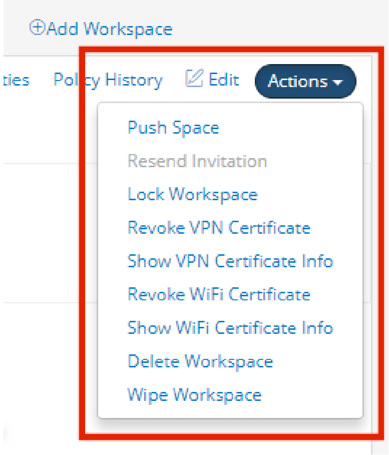
Policy History

Policy: corp-2019-01-07 11:12:19

Policy	Command	Title	Creator	Package Name	State
corp	add	Google Chrome	Google, Inc.	com.google.chrome.ios	Installed

The **Actions** menu displays the list of actions available for the Workspace.

FIGURE 178 Workspace Actions



Working with the App Catalog

You can add iOS and Android apps to the App Catalog. From there, you can add them to a policy.

This section describes:

- **"Working with the Apple Volume Purchase Program" on page 149**.
- **"Adding iOS Apps to the App Catalog" on page 152**.

  Note: The addition of Android apps to the App Catalog is described in **"Adding an Android App to the App Catalog" on page 113**.
- **"Adding iOS Apps to a Policy from the App Catalog" on page 157**.

  Note: The addition of Android apps to a Policy from the App Catalog is described in **"Configuring Policy Settings" on page 130**.

Working with the Apple Volume Purchase Program

The Apple Volume Purchase Program (VPP) enables customers to buy bulk licenses for iOS apps.

Note: Pulse Workspace supports Apple VPP for device-based licensing only. Device-based licensing uniquely identifies a device using serial numbers. Every user does not require an Apple ID. Rather, the administrator assigns apps directly to devices using Pulse Workspace.

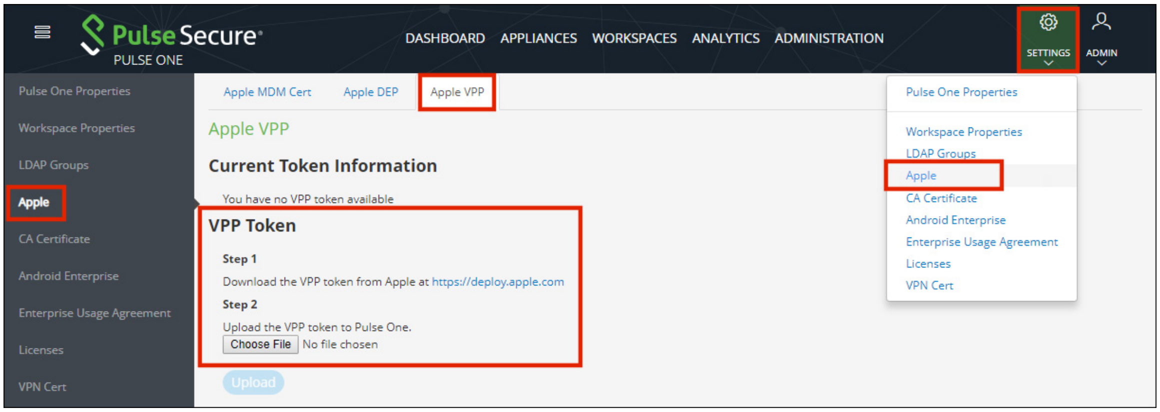
You can assign VPP-licensed apps to policies, and then apply those policies to iOS devices.

To use VPP on Pulse Workspace:

1. Click the **Settings** icon on top-right-corner of the page and select **Apple**.
2. Select the **Apple VPP** tab.

   The **Apple VPP** management page appears.

   FIGURE 179 Apple VPP page



Apple VPP

Current Token Information

You have no VPP token available

VPP Token

Step 1

Download the VPP token from Apple at https://deploy.apple.com

Step 2

Upload the VPP token to Pulse One.

No file chosen

3. Under **VPP Token**, click the link to access the Apple Deployment Program (ADP) portal.

4. On the ADP portal, enroll your business.

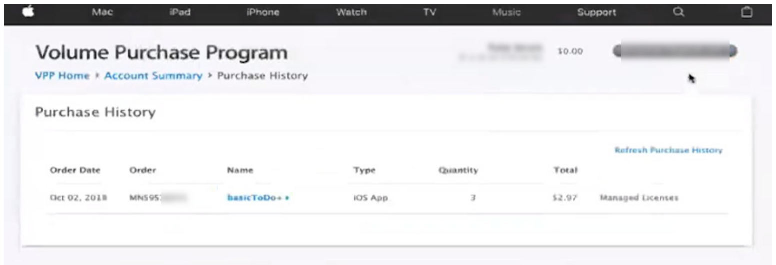
   Note: You require the Data Universal Numbering System (D-U-N-S) number for your business.

   Note: If you have previously registered your business on ADP to use Apple web page, the same ADP account can be used for Apple VPP.

5. Verify your account using the two-step email verification process.

6. On the Apple VPP portal, purchase iOS apps in the required quantities. For example:

   FIGURE 180 VPP purchases



Volume Purchase Program

[redacted] $0.00 [redacted]

VPP Home › Account Summary › Purchase History

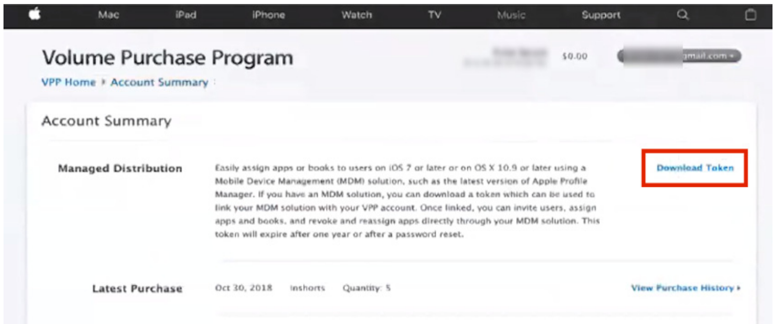
Purchase History

Refresh Purchase History

Order Date	Order	Name	Type	Quantity	Total	
Oct 02, 2018	MN595[redacted]	basicToDo+ ▸	iOS App	3	$2.97	Managed Licenses

7. On the Apple VPP **Account Summary** page, click **Download Token** and save the file locally.

   FIGURE 181 Download VPP Token



Volume Purchase Program

[redacted] $0.00 [redacted]gmail.com ▾

VPP Home › Account Summary

Account Summary

Managed Distribution Easily assign apps or books to users on iOS 7 or later or on OS X 10.9 or later using a Mobile Device Management (MDM) solution, such as the latest version of Apple Profile Manager. If you have an MDM solution, you can download a token which can be used to link your MDM solution with your VPP account. Once linked, you can invite users, assign apps and books, and revoke and reassign apps directly through your MDM solution. This token will expire after one year or after a password reset.

Download Token

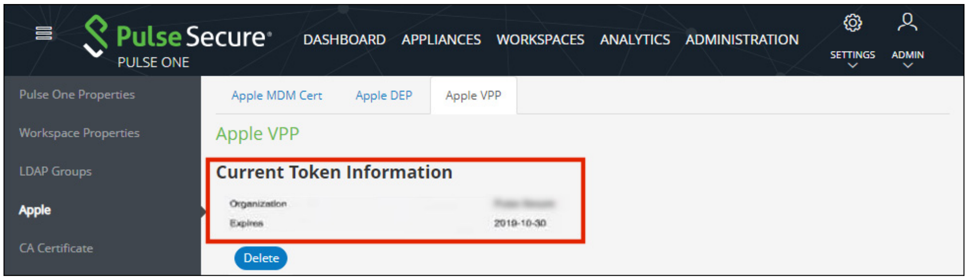
Latest Purchase Oct 30, 2018 inshorts Quantity: 5 View Purchase History ›

8. On Pulse One, under **VPP Token**, click **Choose File** and select the VPP token file.

9. Click **Upload**.

   The **Current Token Information** updates.

   FIGURE 182 Current Token Information



Apple VPP

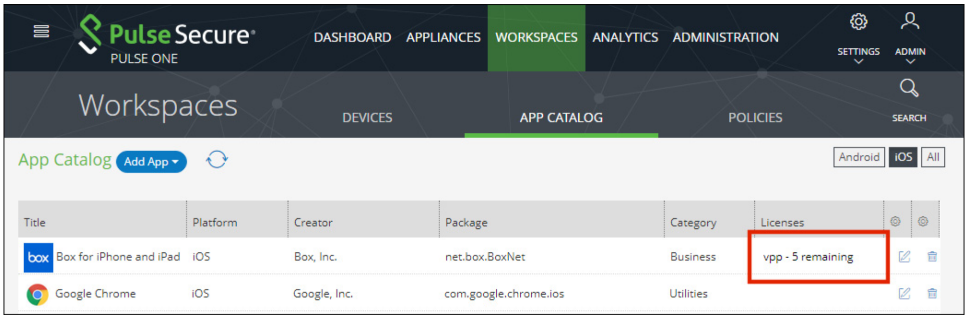
Current Token Information

Organization	[redacted]
Expires	2019-10-30

10. Click the **Workspaces** menu and then the **App Catalog** tab.

    The App Catalog automatically syncs to show all VPP-purchased apps and the remaining license count for each. For example:

    FIGURE 183 App Catalog With VPP Licenses



Title	Platform	Creator	Package	Category	Licenses
Box for iPhone and iPad	iOS	Box, Inc.	net.box.BoxNet	Business	vpp - 5 remaining
Google Chrome	iOS	Google, Inc.	com.google.chrome.ios	Utilities	

11. Add VPP-licensed apps to new or existing policies.

12. (Optional) If the policies are in use, publish the policies.

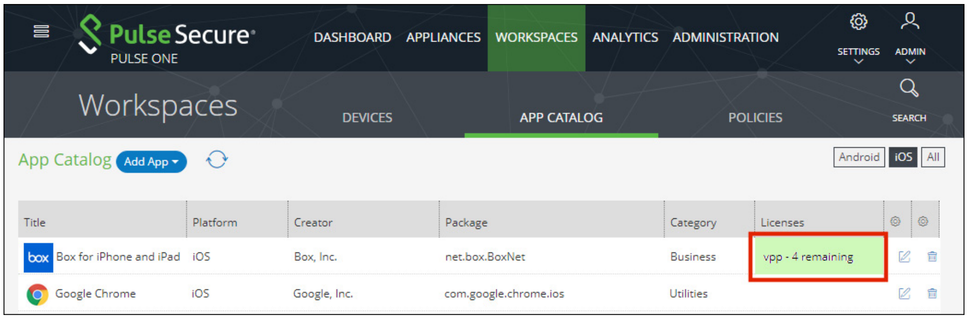
    The VPP-licensed apps are installed on all devices that use the policy, subject to license availability.

13. (Optional) Create new devices to install the VPP-licensed apps

    The VPP-licensed apps are installed on all devices that use the policy, subject to license availability.

    As licenses are consumed, the **Licensing** column of the App Catalog updates.

    FIGURE 184 Updated License Counts



Title	Platform	Creator	Package	Category	Licenses
Box for iPhone and iPad	iOS	Box, Inc.	net.box.BoxNet	Business	vpp - 4 remaining
Google Chrome	iOS	Google, Inc.	com.google.chrome.ios	Utilities	

Adding iOS Apps to the App Catalog

You can add iOS apps to the **App Catalog** in two ways:

- From the App Store, see **"Adding an iOS App From the App Store to the App Catalog" on page 152**.
- Manually, from a third-party source, see **"Adding an iOS App to the App Catalog Manually" on page 154**.

Adding an iOS App From the App Store to the App Catalog

To add an iOS App from the App Store to the App Catalog:

Note: If the iOS app requires an app config schema, then request this from the application vendor.

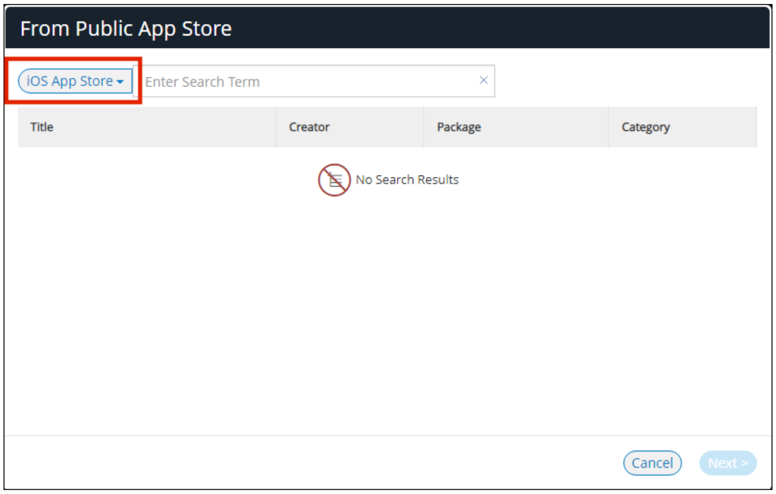
1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab.

   The **App Catalog** page appears.

   Note: Ensure the app you are going to add is not listed.
3. In the **App Catalog** page, click **Add App** and then select **Add App From Store**.

   The **From Public App Store** dialog appears.
4. In the **From Public App Store** dialog, select iOS App Store.

   FIGURE 185 Add iOS App From Store

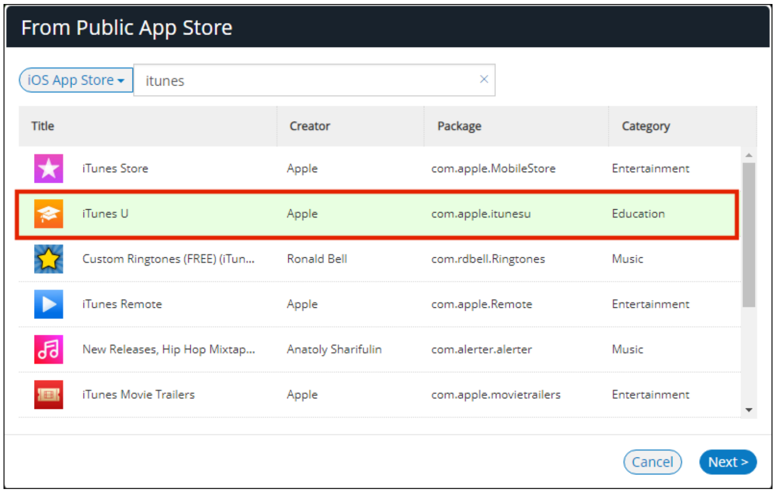
   

5. Type the name of the app in the **Search** box and press Enter.

   A list of apps is displayed based on the search criteria.

6. Select the required app from the apps list and click **Next**.

FIGURE 186 Select iOS App from Search Result



From Public App Store

iOS App Store ▾ | itunes ×

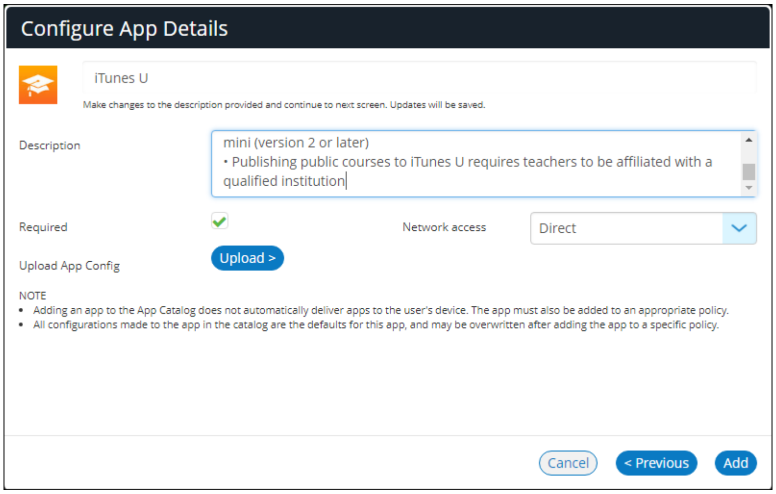
Title	Creator	Package	Category
iTunes Store	Apple	com.apple.MobileStore	Entertainment
iTunes U	Apple	com.apple.itunesu	Education
Custom Ringtones (FREE) (iTun...	Ronald Bell	com.rdbell.Ringtones	Music
iTunes Remote	Apple	com.apple.Remote	Entertainment
New Releases, Hip Hop Mixtap...	Anatoly Sharifulin	com.alerter.alerter	Music
iTunes Movie Trailers	Apple	com.apple.movietrailers	Entertainment

The **Configure App Details** dialog appears.

7. In the **Configure App Details** dialog:

   - Change the **Description** if required.
   - Select the **Required** check box if the app should be pushed automatically upon enrollment.
   - If you access the app through VPN, then then set **Network access** to *Per app VPN*.

FIGURE 187 Configure iOS App Details



Configure App Details

iTunes U

Make changes to the description provided and continue to next screen. Updates will be saved.

Description: mini (version 2 or later)
• Publishing public courses to iTunes U requires teachers to be affiliated with a qualified institution

Required: ✓

Network access: Direct

Upload App Config: Upload >

NOTE
- Adding an app to the App Catalog does not automatically deliver apps to the user's device. The app must also be added to an appropriate policy.
- All configurations made to the app in the catalog are the defaults for this app, and may be overwritten after adding the app to a specific policy.

- If you have an app config schema from the app vendor, click **Upload** and select the schema file.
- Click **Add**.

The iOS app is added to the **App Catalog**.

Note: Adding an app to the **App Catalog** does not automatically deliver apps to the user's device. The app must also be added to an appropriate policy.

Note: All configuration changes made to the app in the **App Catalog** are the defaults for the app. However, you can overwrite these after adding the app to a specific policy.

The next step is to add the app to a specific policy. For details, see **"Adding iOS Apps to a Policy from the App Catalog" on page 157**.

Adding an iOS App to the App Catalog Manually

Before proceeding with manual adding of iOS app, ensure you have the following details:

- The application package name. For example: *com.microsoft.office.word*
- The application title. For example: *Microsoft Word*
- The application creator. That is, the provider of the app. For example: *Microsoft*

Two manual methods are available:

- You can source the app from a third-party URL. In this case, you will also need the location of the manifest.plist file that was created by the app distributor.
- You can upload the app from a local copy of the iOS app in .ipa format.

To add an iOS app to the **App Catalog** using either manual method:

1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab.

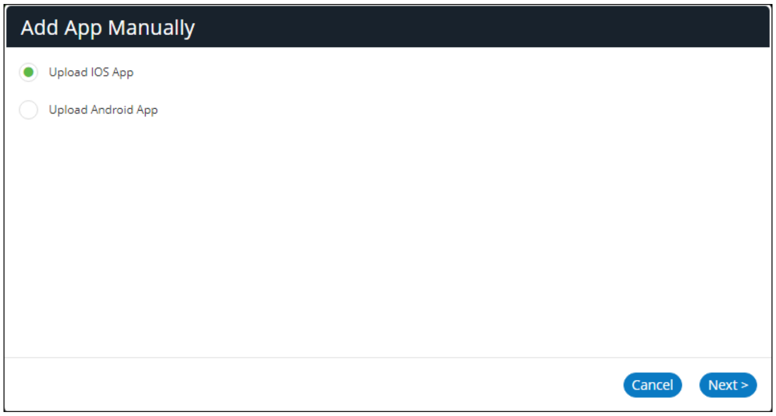
   The **App Catalog** page appears.

   Note: Ensure the app you are going to add is not listed.

3. In the **App Catalog** page, click **Add App** and then select **Add App Manually**.

   The **Add App Manually** dialog appears.

   FIGURE 188 Add App Manually

   Add App Manually

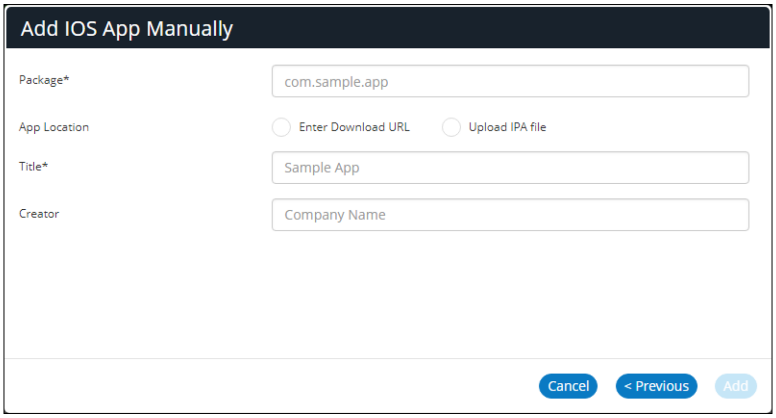
   ● Upload IOS App

   ○ Upload Android App

4. In the **Add App Manually** window, select **Upload iOS App** and click **Next**.

   The **Add iOS App Manually** dialog appears:

   FIGURE 189 Add iOS App Manually

   Add IOS App Manually

   Package* com.sample.app

   App Location ○ Enter Download URL ○ Upload IPA file

   Title* Sample App

   Creator Company Name

5. Specify the app **Package**. For example: com.demo.word.

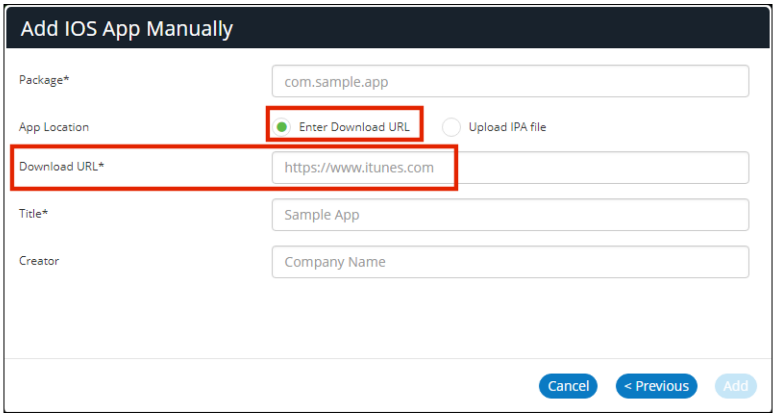
6. Specify the app **Title**. This will be the name of the app in the **App Catalog**.

7. Specify the app **Creator**. That is, the provider of the app.

8. (Optional) If you want to source the app from a third-party URL:

   - Select **Enter Download URL**. The dialog updates to include a **Download URL** property:

     FIGURE 190 Source an iOS App from a URL

     Add IOS App Manually

     Package* com.sample.app

     App Location ● Enter Download URL ○ Upload IPA file

     Download URL* https://www.itunes.com

     Title* Sample App

     Creator Company Name

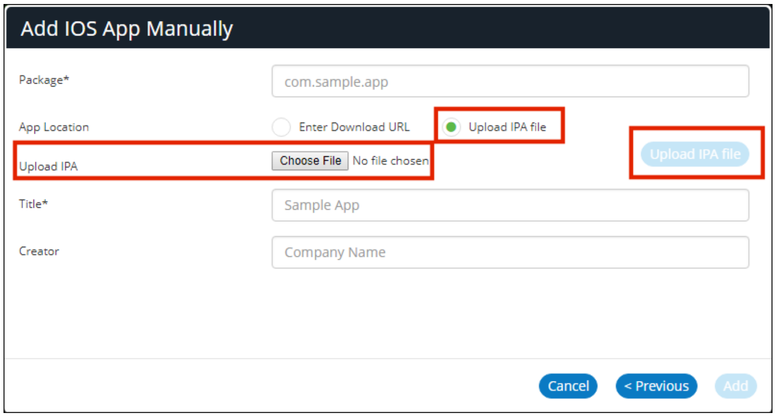
   - Specify the **Download URL**.

   Note: This URL must be accessible by the end user's devices.

9. (Optional) If you want to upload the app from a local copy:

   - Select **Upload IPA File**. The dialog updates to include an **App Location** property:

     FIGURE 191 Source an iOS App from a Local Copy

     Add IOS App Manually

     Package* com.sample.app

     App Location ○ Enter Download URL ● Upload IPA file

     Upload IPA Choose File No file chosen

     Title* Sample App

     Creator Company Name

   - Click **Choose File** and locate the file.

   - Click **Upload IP File**.

10. Click **Add**.

    The app is added to the **App Catalog**.

The next step is to add the app to a specific policy. For details, see **"Adding iOS Apps to a Policy from the App Catalog" on page 157**.

Adding iOS Apps to a Policy from the App Catalog

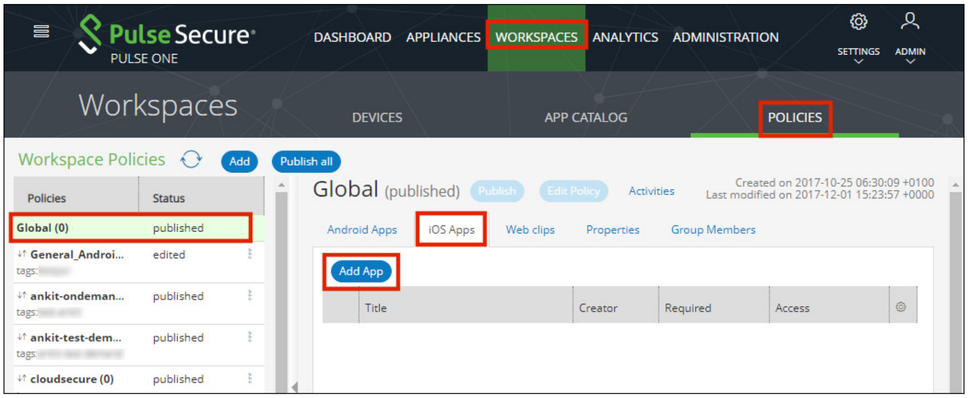
To add the app to a policy:

1. Select the **Workspaces** menu.
2. Select the **Policies** tab.

   A list of policies is displayed.

3. Select a policy from the list, select the **iOS Apps** tab, and click **Add App**.

   FIGURE 192 Add iOS App



Global (published)

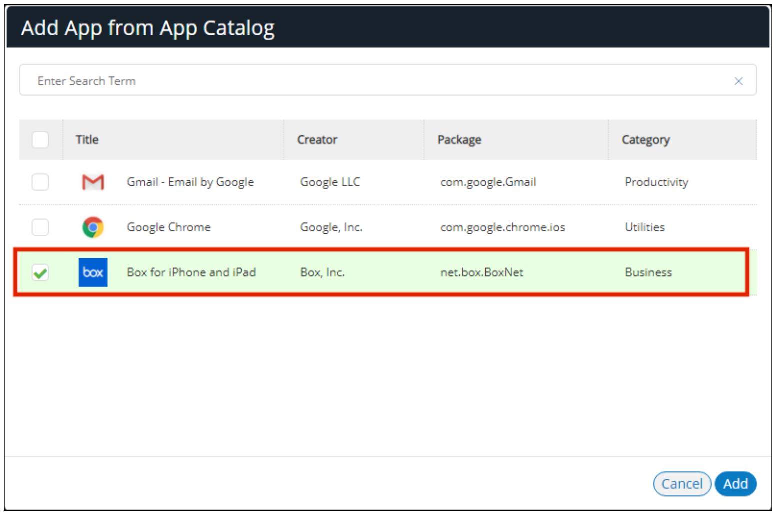
Created on 2017-10-25 06:30:09 +0100
Last modified on 2017-12-01 15:23:57 +0000

Policies	Status
Global (0)	published
General_Androi... tags: [redacted]	edited
ankit-ondeman... tags: [redacted]	published
ankit-test-dem... tags: [redacted]	published
cloudsecure (0)	published

   The **Add App from App Catalog** dialog appears.

4. Select the app from the app catalog list and click **Add**.

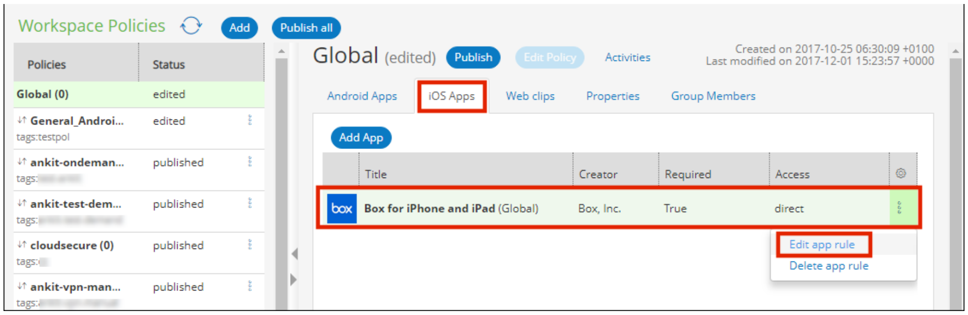
   FIGURE 193 Add App from App Catalog



	Title	Creator	Package	Category
□	Gmail - Email by Google	Google LLC	com.google.Gmail	Productivity
□	Google Chrome	Google, Inc.	com.google.chrome.ios	Utilities
☑	Box for iPhone and iPad	Box, Inc.	net.box.BoxNet	Business

5. In the **iOS Apps** tab, select the app and click **Edit app rule**.

FIGURE 194 Edit App Rule



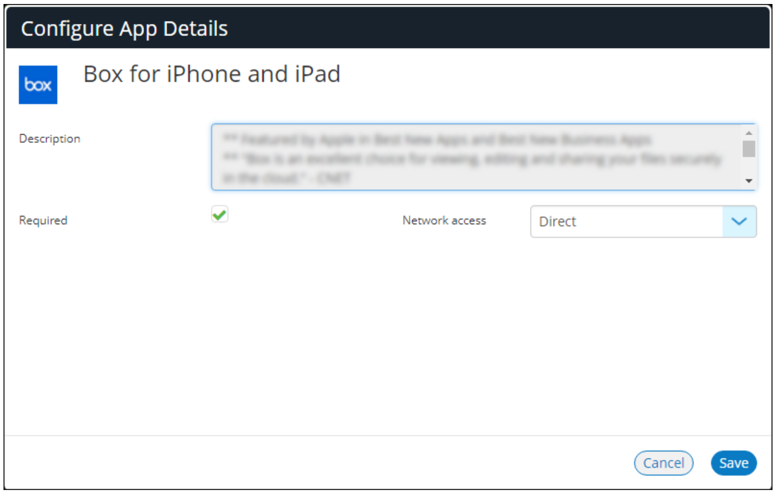
Policies	Status
Global (0)	edited
General_Androi... tags:testpol	edited
ankit-ondeman... tags:[redacted]	published
ankit-test-dem... tags:[redacted]	published
cloudsecure (0) tags:[redacted]	published
ankit-vpn-man... tags:[redacted]	published

Title	Creator	Required	Access
Box for iPhone and iPad (Global)	Box, Inc.	True	direct

The **Configure App Details** dialog appears.

6. In the **Configure App Details** dialog, make appropriate changes and click **Save**.

FIGURE 195 Configure App Details



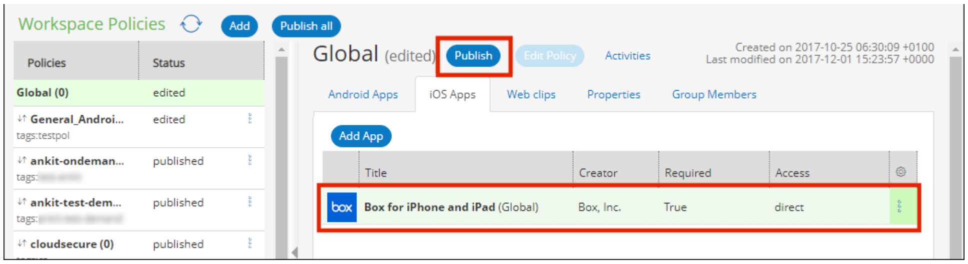
Description: [redacted]

Required: ✓

Network access: Direct

7. Select the app and click **Publish**.

FIGURE 196 Publish App



Policies	Status
Global (0)	edited
General_Androi... tags:testpol	edited
ankit-ondeman... tags:[redacted]	published
ankit-test-dem... tags:[redacted]	published
cloudsecure (0)	published

Title	Creator	Required	Access
Box for iPhone and iPad (Global)	Box, Inc.	True	direct

A confirmation prompt appears.

8. Click **Yes** to confirm the publication.

This completes the process.

Working with Web Clips

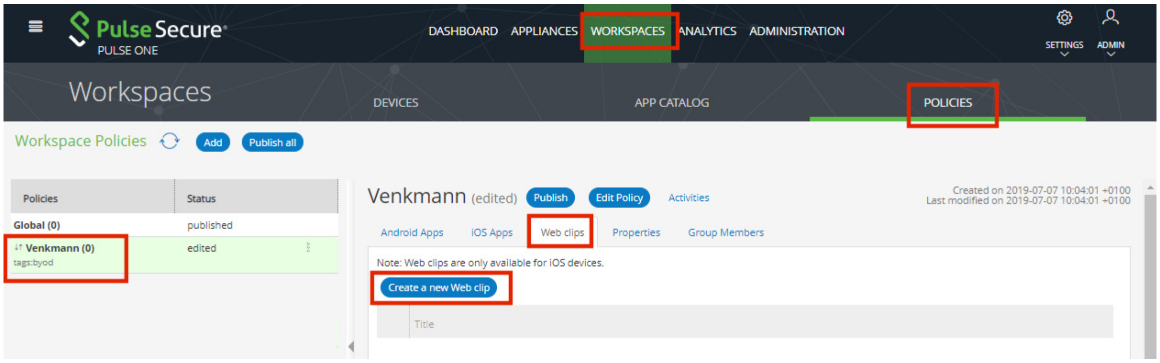
A web clip is a URL-based bookmark associated with a policy. When the policy is applied to a mobile device, the web clip bookmark is created automatically on the device.

Note: Web clips are currently supported on iOS devices only.

To create a webclip:

1. Select the **Workspaces** menu.
2. Select the **Policies** tab.
3. Select a policy from the list.
4. Select the **Web clips** tab. For example:

FIGURE 197 Add Web Clip



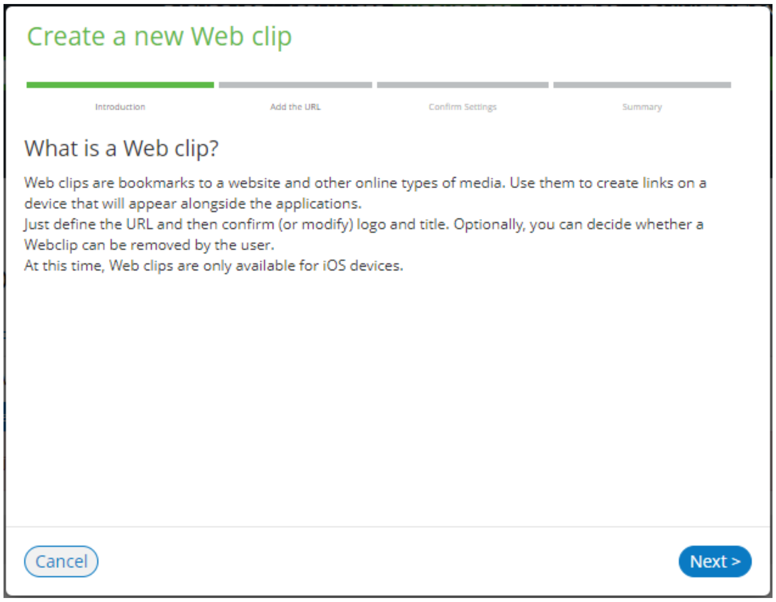
Policies	Status
Global (0)	published
Venkmann (0) tags:byod	edited

Created on 2019-07-07 10:04:01 +0100
Last modified on 2019-07-07 10:04:01 +0100

Note: Web clips are only available for iOS devices.

5. Click **Create a new Web clip**.
6. The **Create a new Web clip** wizard appears:

FIGURE 198 Web Clip Wizard: Introduction

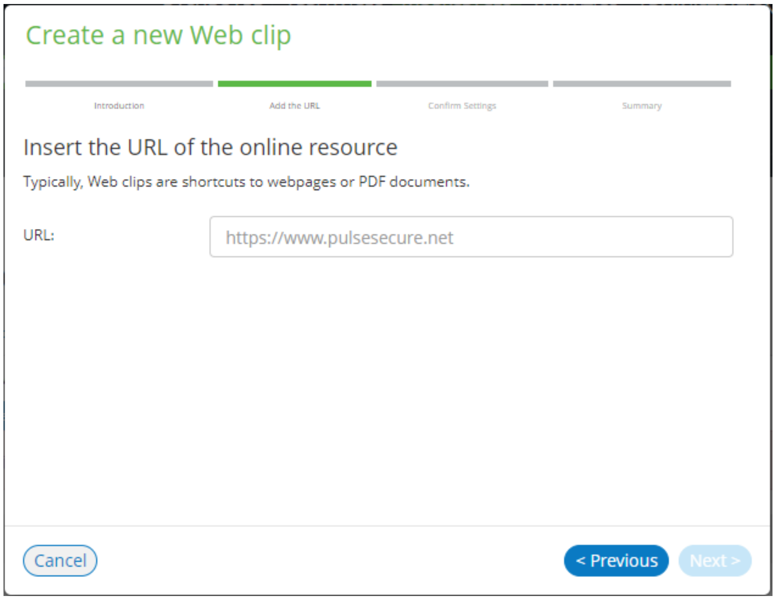


What is a Web clip?

Web clips are bookmarks to a website and other online types of media. Use them to create links on a device that will appear alongside the applications.
Just define the URL and then confirm (or modify) logo and title. Optionally, you can decide whether a Webclip can be removed by the user.
At this time, Web clips are only available for iOS devices.

7. Click **Next**. The next panel of the wizard appears.

FIGURE 199 Web Clip Wizard: Add the URL



Insert the URL of the online resource

Typically, Web clips are shortcuts to webpages or PDF documents.

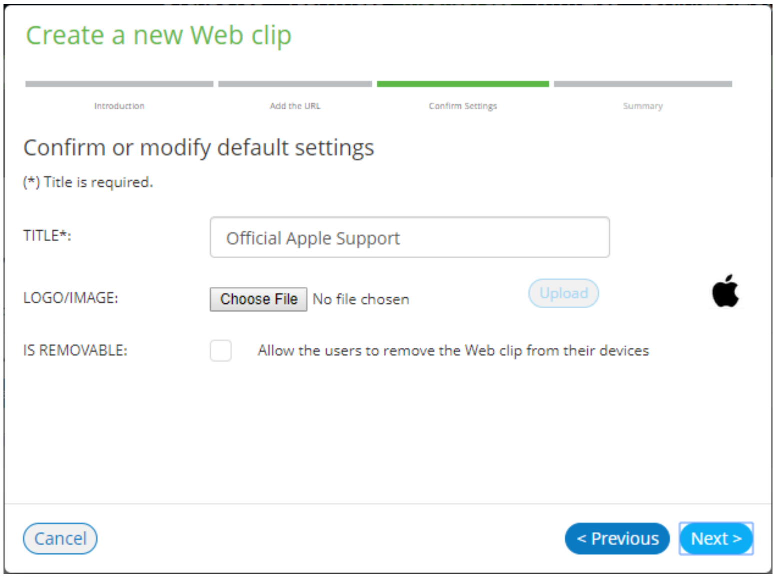
URL: https://www.pulsesecure.net

8. Enter the full **URL** for the web clip bookmark.

   Click **Next**. The next panel of the wizard appears.

   Where supported, the title of the web page and an icon is retrieved automatically. For example:

FIGURE 200 Web Clip Wizard: Confirm Settings



Confirm or modify default settings

(*) Title is required.

TITLE*: Official Apple Support

LOGO/IMAGE: No file chosen

IS REMOVABLE: □ Allow the users to remove the Web clip from their devices

9. If no title for the URL was retrieved, you must specify a **Title**.

10. (Optional) Upload a **Logo/Image** for the web clip bookmark.

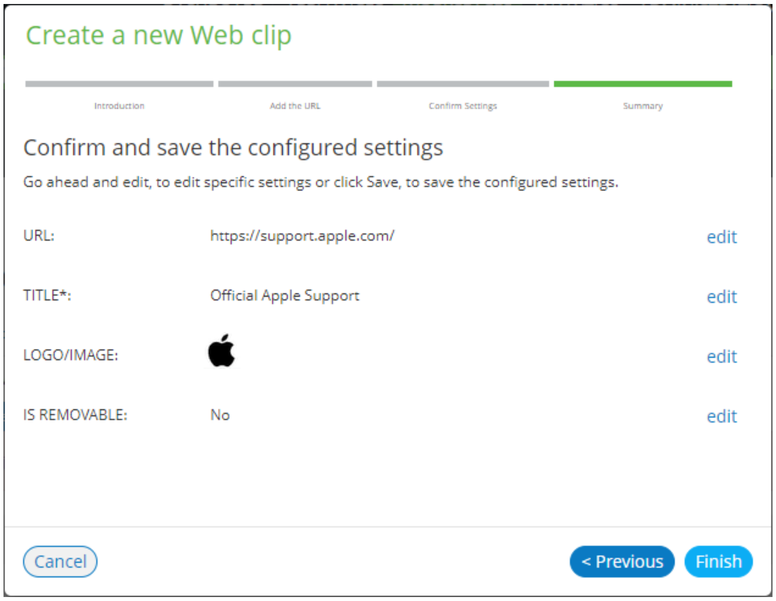
    Note: This image file must be .PNG format, and no larger than 512Kb.

    Note: If no logo is specified, a plain white icon will be used for the web clip bookmark on the mobile device.

11. If you want the user to be able to remove the web clip bookmark from their device, enable the **Is Removable** check box.

12. Click **Next**. The final panel of the wizard appears.

FIGURE 201 Web Clip Wizard: Summary



Confirm and save the configured settings

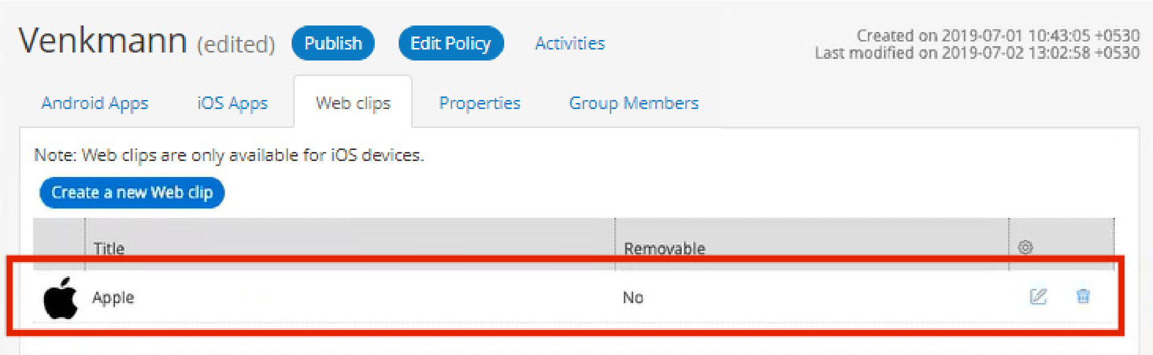
Go ahead and edit, to edit specific settings or click Save, to save the configured settings.

URL:	https://support.apple.com/
TITLE*:	Official Apple Support
LOGO/IMAGE:	
IS REMOVABLE:	No

13. Click **Finish** to close the wizard and create the web clip bookmark.

    The **Web clips** tab for the policy updates to include the new web clip bookmark. For example:

FIGURE 202 New Web Clip Added to Policy



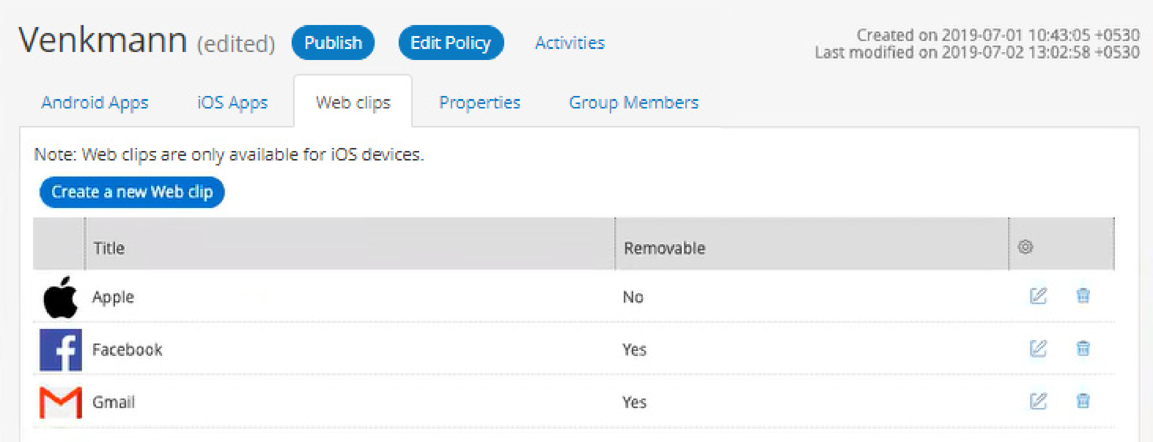
Created on 2019-07-01 10:43:05 +0530
Last modified on 2019-07-02 13:02:58 +0530

Note: Web clips are only available for iOS devices.

Title	Removable
Apple	No

14. (Optional) Repeat steps 5 to 12 to add each required bookmark. For example:

FIGURE 203 Additional Web Clips Added to Policy



Venkmann (edited) Publish Edit Policy Activities

Created on 2019-07-01 10:43:05 +0530
Last modified on 2019-07-02 13:02:58 +0530

Android Apps | iOS Apps | Web clips | Properties | Group Members

Note: Web clips are only available for iOS devices.

Create a new Web clip

Title	Removable
Apple	No
Facebook	Yes
Gmail	Yes

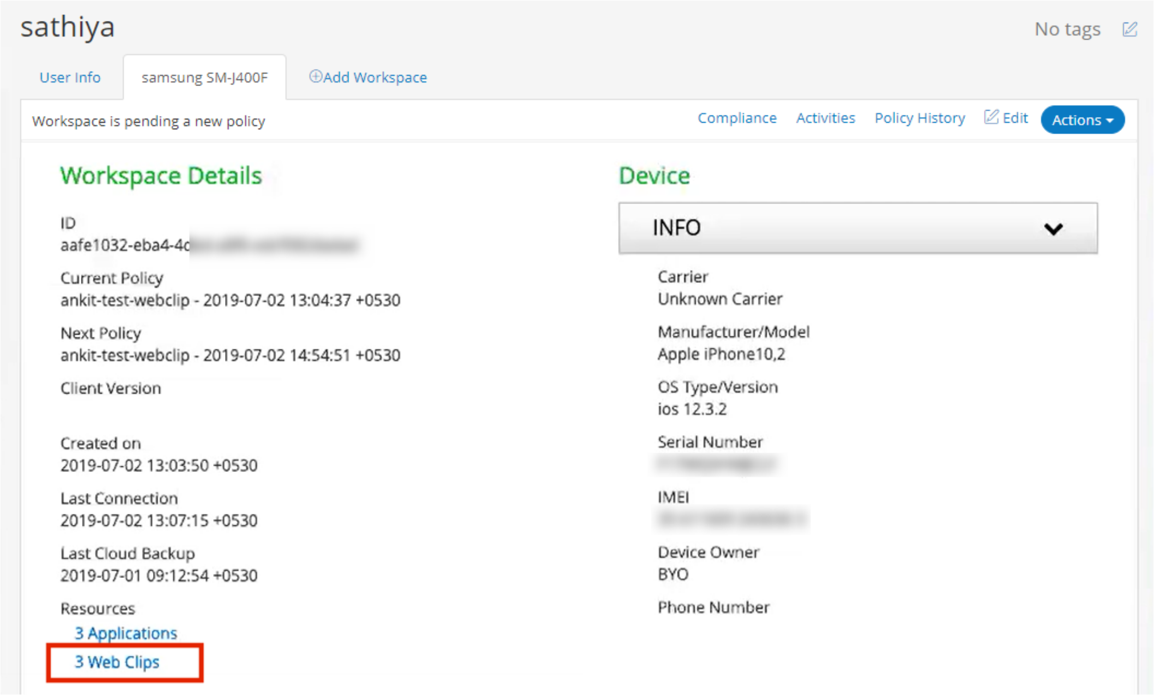
15. (Optional) To delete a web clip bookmark from a policy, click its **Delete** (🗑) icon.

16. (Optional) To edit a web clip bookmark for a policy, click its **Edit** (✎) icon and update its details in the wizard.

17. (Optional) Confirm the addition of web clips:

- Navigate to **Workspaces > Devices** and select the required workspace.
- Examine the details for the registered workspace. For example:

FIGURE 204 Web Clip Bookmarks on Workspace Details Page



sathiya

No tags

User Info | samsung SM-J400F | ⊕Add Workspace

Workspace is pending a new policy

Compliance Activities Policy History Edit Actions ▾

Workspace Details

ID
aafe1032-eba4-4c[redacted]

Current Policy
ankit-test-webclip - 2019-07-02 13:04:37 +0530

Next Policy
ankit-test-webclip - 2019-07-02 14:54:51 +0530

Client Version

Created on
2019-07-02 13:03:50 +0530

Last Connection
2019-07-02 13:07:15 +0530

Last Cloud Backup
2019-07-01 09:12:54 +0530

Resources
3 Applications
3 Web Clips

Device

INFO

Carrier
Unknown Carrier

Manufacturer/Model
Apple iPhone10,2

OS Type/Version
ios 12.3.2

Serial Number
[redacted]

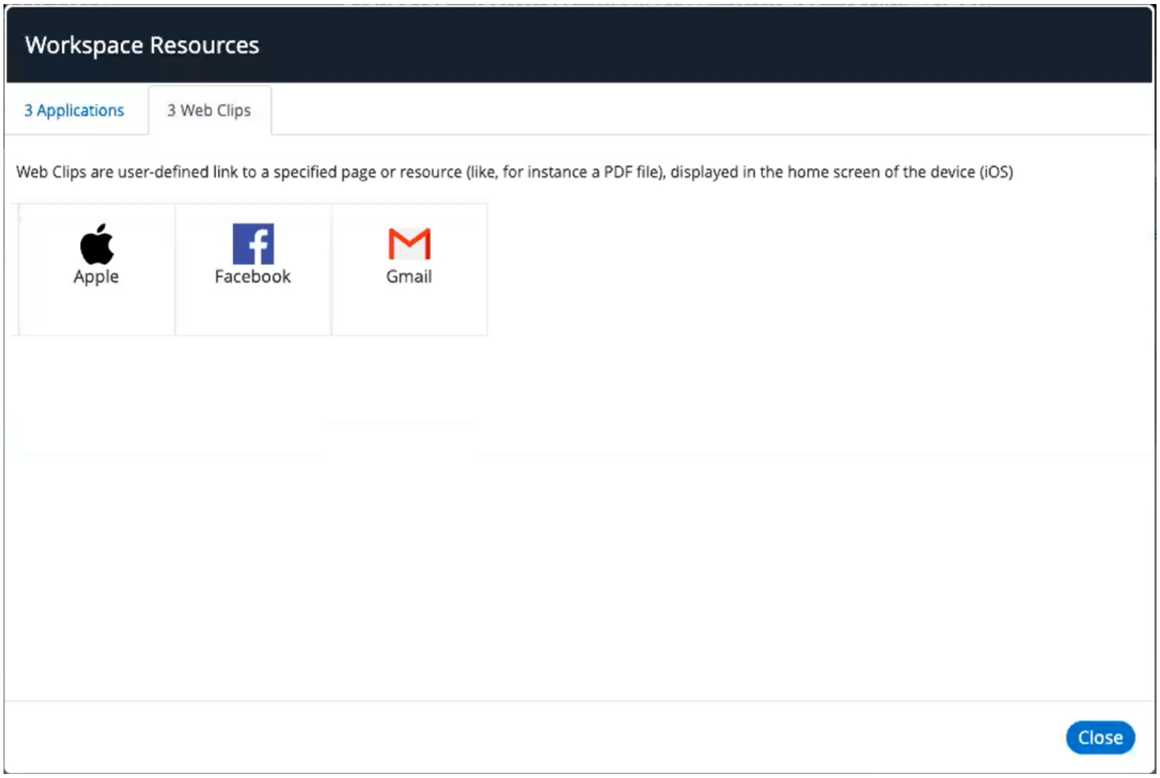
IMEI
[redacted]

Device Owner
BYO

Phone Number

- Click the **Web Clips** hyperlink. The **Workspace Resources** page appears. For example:

FIGURE 205 Web Clip Bookmarks

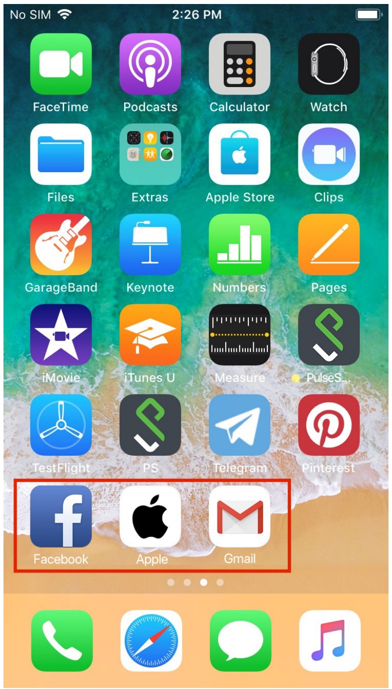


Workspace Resources

Web Clips are user-defined link to a specified page or resource (like, for instance a PDF file), displayed in the home screen of the device (iOS)

18. **Publish** the policy to add the web clip bookmarks to all devices that use the policy. For example:

FIGURE 206 Web Clip Bookmarks on Mobile Device



Working with Policies

This section describes the following tasks:

- "Creating a Policy" on page 164.
- "Understanding Policy Properties" on page 167.

Creating a Policy

When you create a policy, you define specific users and device types to which the policy applies:

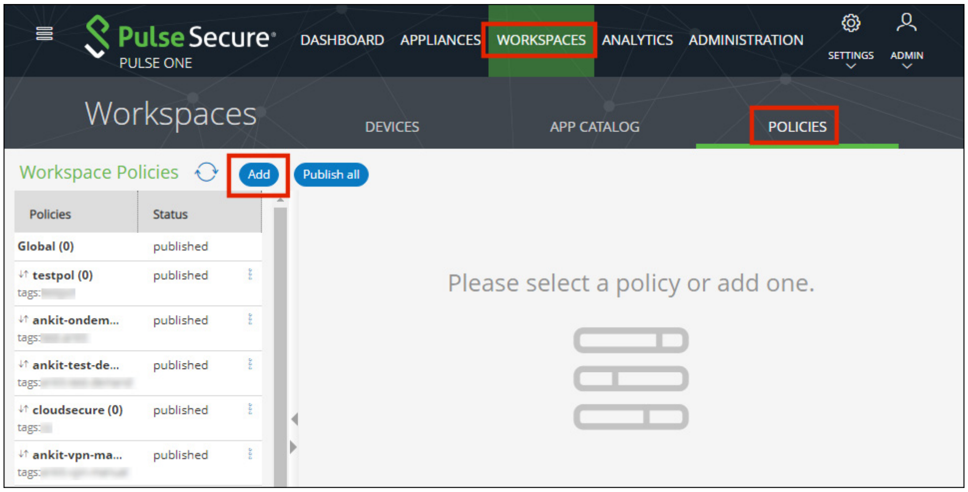
- Each policy applies to users listed as its **User tags**.
- Each policy can have one of three **Device User Mode** settings:
  - BYO: The policy is applied to a user's BYO devices only.
  - Corporate Owned: The policy is applied to a user's corporate owned devices only.
  - Both (BYO and Corporate Owned): The policy is applied to all of a user's devices.

  This enables a user to have different policies for different device types.

This section details the steps to create a new policy:

1. Select the **Workspaces** menu.
2. Select the **Policies** tab.
3. Click **Add** to add a new policy.

   FIGURE 207 Workspace Policies



Policies	Status
Global (0)	published
testpol (0) tags:[redacted]	published
ankit-ondem... tags:[redacted]	published
ankit-test-de... tags:[redacted]	published
cloudsecure (0) tags:[redacted]	published
ankit-vpn-ma... tags:[redacted]	published

Please select a policy or add one.

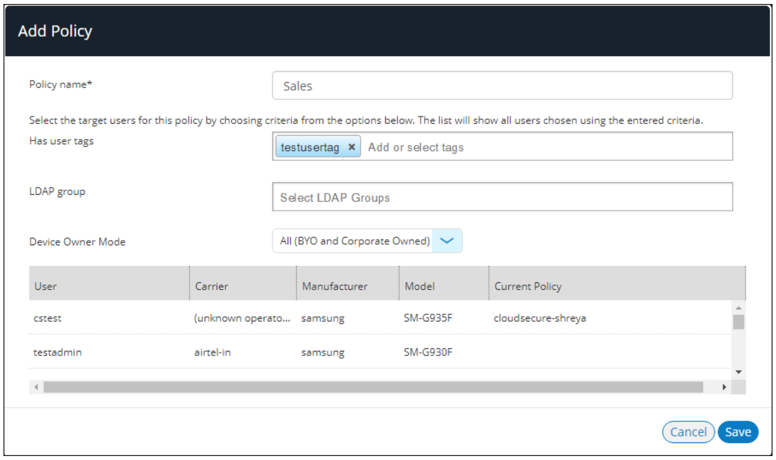
The **Add Policy** dialog appears.

4. Specify the **Policy Name**.

   Note: Policy names are not unique. Policies are unique based on their search criteria.

5. Specify the **User tags** and **LDAP Group** for the policy. For example:

   FIGURE 208 Add Policy



Add Policy

Policy name* Sales

Select the target users for this policy by choosing criteria from the options below. The list will show all users chosen using the entered criteria.

Has user tags: testusertag × Add or select tags

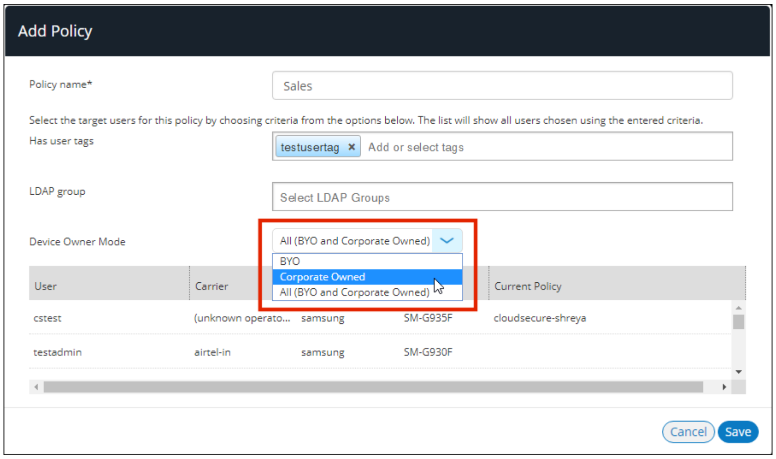
LDAP group: Select LDAP Groups

Device Owner Mode: All (BYO and Corporate Owned)

User	Carrier	Manufacturer	Model	Current Policy
cstest	(unknown operato...	samsung	SM-G935F	cloudsecure-shreya
testadmin	airtel-in	samsung	SM-G930F	

6. Select the required **Device Owner Mode**. This property determines whether this policy is applied to a user's devices that are BYO, corporate owned, or both. For example:

   FIGURE 209 Add Device Owner Mode to Policy



Add Policy

Policy name* Sales

Select the target users for this policy by choosing criteria from the options below. The list will show all users chosen using the entered criteria.

Has user tags: testusertag × Add or select tags

LDAP group: Select LDAP Groups

Device Owner Mode: All (BYO and Corporate Owned)

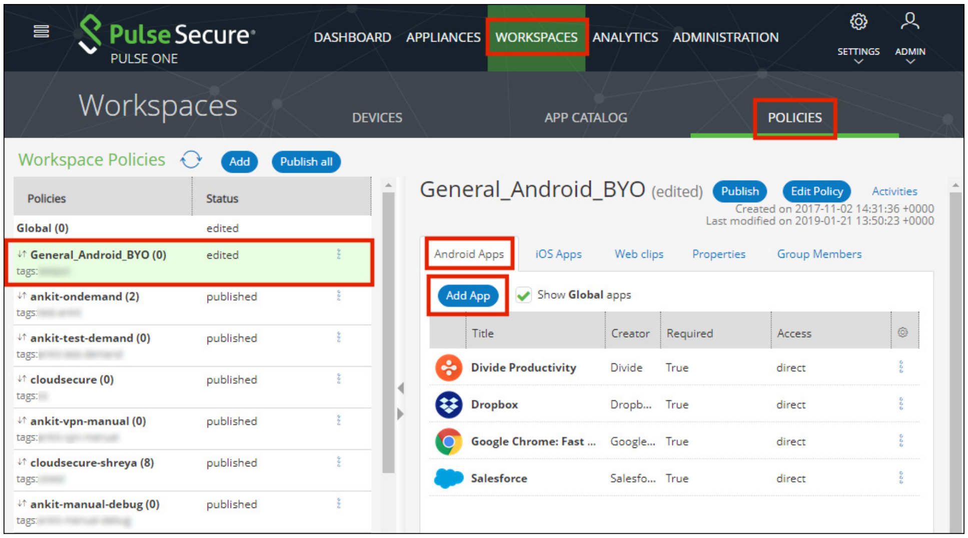
User	Carrier	Manufacturer	Model	Current Policy
cstest	(unknown operato...	samsung	SM-G935F	cloudsecure-shreya
testadmin	airtel-in	samsung	SM-G930F	

7. Click **Save**.

   The policy is created with an edited state.

8. You can now add applications and properties to the policy before applying the policy to mobile devices. For example:

FIGURE 210 Add Apps and Properties



General_Android_BYO (edited)
Created on 2017-11-02 14:31:36 +0000
Last modified on 2019-01-21 13:50:23 +0000

☑ Show **Global** apps

Policies	Status
Global (0)	edited
General_Android_BYO (0) tags: [redacted]	edited
ankit-ondemand (2) tags: [redacted]	published
ankit-test-demand (0) tags: [redacted]	published
cloudsecure (0) tags: [redacted]	published
ankit-vpn-manual (0) tags: [redacted]	published
cloudsecure-shreya (8) tags: [redacted]	published
ankit-manual-debug (0) tags: [redacted]	published

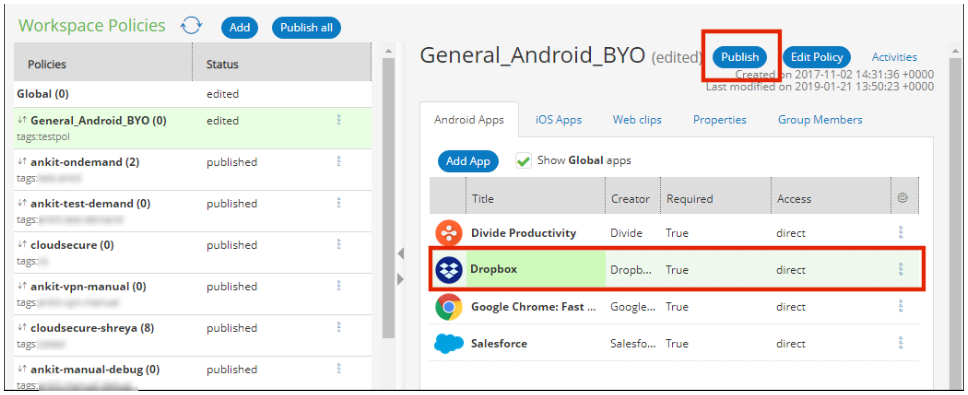
Title	Creator	Required	Access
Divide Productivity	Divide	True	direct
Dropbox	Dropb...	True	direct
Google Chrome: Fast ...	Google...	True	direct
Salesforce	Salesfo...	True	direct

9. After you have completed editing the policy, click **Publish**.

The policy's state changes from *edited* to *publishing* and then *published*.

This applies the policy to all mobile devices that use the policy.

FIGURE 211 Publish the Policy



General_Android_BYO (edited)
Created on 2017-11-02 14:31:36 +0000
Last modified on 2019-01-21 13:50:23 +0000

☑ Show **Global** apps

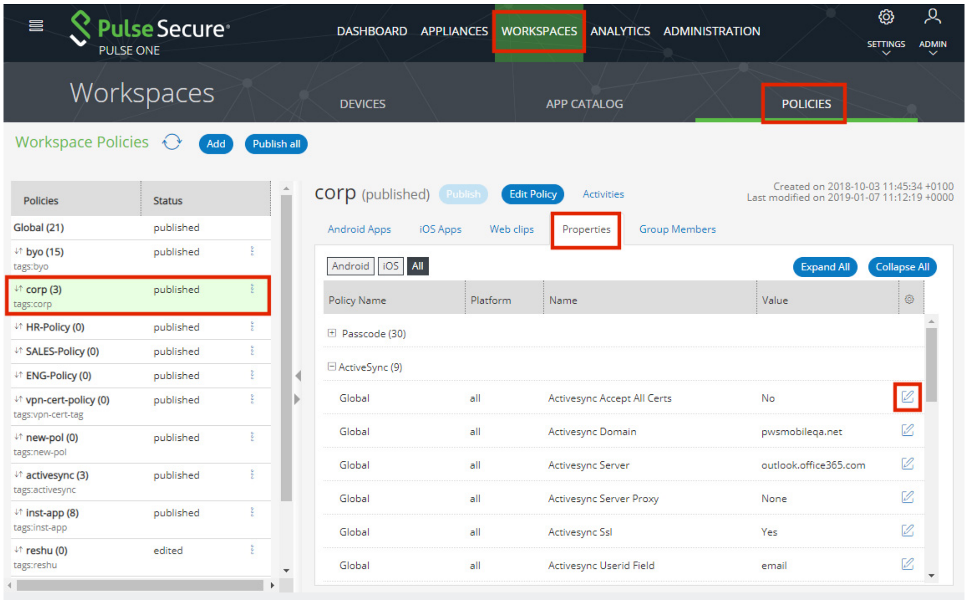
Policies	Status
Global (0)	edited
General_Android_BYO (0) tags:testpol	edited
ankit-ondemand (2) tags: [redacted]	published
ankit-test-demand (0) tags: [redacted]	published
cloudsecure (0) tags: [redacted]	published
ankit-vpn-manual (0) tags: [redacted]	published
cloudsecure-shreya (8) tags: [redacted]	published
ankit-manual-debug (0) tags: [redacted]	published

Title	Creator	Required	Access
Divide Productivity	Divide	True	direct
Dropbox	Dropb...	True	direct
Google Chrome: Fast ...	Google...	True	direct
Salesforce	Salesfo...	True	direct

Understanding Policy Properties

This section describes all supported policy properties for a workspace.

FIGURE 212 Policy Properties



Policies	Status
Global (21)	published
byo (15) tags:byo	published
corp (3) tags:corp	published
HR-Policy (0)	published
SALES-Policy (0)	published
ENG-Policy (0)	published
vpn-cert-policy (0) tags:vpn-cert-tag	published
new-pol (0) tags:new-pol	published
activesync (3) tags:activesync	published
inst-app (8) tags:inst-app	published
reshu (0) tags:reshu	edited

corp (published)

Created on 2018-10-03 11:45:34 +0100
Last modified on 2019-01-07 11:12:19 +0000

Policy Name	Platform	Name	Value
⊞ Passcode (30)			
⊟ ActiveSync (9)			
Global	all	Activesync Accept All Certs	No
Global	all	Activesync Domain	pwsmobileqa.net
Global	all	Activesync Server	outlook.office365.com
Global	all	Activesync Server Proxy	None
Global	all	Activesync Ssl	Yes
Global	all	Activesync Userid Field	email

Passcode

Different **Passcode** properties are used for iOS and Android.

Android for Work supports two levels of passcode challenge to protect the data in the device and the Workspace:

- *Workspace Managed Device Passcode* - This applies passcode policies only to Workspace managed devices enrolled with a Work Profile. This passcode will need to be entered each time the device is unlocked and can be applied in addition to the Work Profile Passcode.
- *Work Profile Passcode* - This applies passcode policies only to Workspace apps, so users do not have to enter complex passwords each time they unlock their device when enrolled with a Work Profile. The Work Profile passcode ensures that the end users can access their private apps while keeping corporate app data protected without the use of wrapping technologies. The Work Profile Passcode is supported on Android 7.0 and above.

The following properties are supported by both Android and iOS:

- **Expiration Days** – The number of days for which the passcode can remain unchanged.
- **Lock Timeout** – The time in seconds where the Workspace will be locked if no Workspace app was in foreground.
- **Max Tries (iOS Factory Reset)** – The number of allowed failed attempts to enter the passcode at the device's lock screen.
- **Numeric Only** – Boolean. If *True*, the user must to set a PIN.

- **Passcode History** – When the user changes the passcode, it must be unique within the most recent specified number of entries in the history.
- **Passcode Length** – The minimum overall length of the passcode.
- **Require Special** – The minimum count of special characters in a passcode.

  Note: For Android, this is used for Workspace Managed Device Passcodes only.

The following properties are supported by Android only:

- **(Work Profile) Expiration Days** – The number of days for which the passcode can remain unchanged.
- **(Work Profile) Lock Timeout** – The time in seconds where the Workspace will be locked if no Workspace app was in the foreground.
- **(Work Profile) Max Tries** – The number of allowed failed attempts to enter the passcode at the device's lock screen.
- **(Work Profile) Numeric Only** – Boolean. If *True*, the user is forced to set a PIN.
- **(Work Profile) Passcode History** – When the user changes the passcode, it must be unique within the most recent specified number of entries in the history.
- **(Work Profile) Passcode Length** – The minimum overall length of the passcode.
- **(Work Profile) Require Letters** – The minimum count of letters in a passcode.
- **(Work Profile) Require Lowercase** – The minimum count of lowercase letters in a passcode.
- **(Work Profile) Require Non-Letters** – The minimum count of numbers and symbols in a passcode.
- **(Work Profile) Require Number** – The minimum count of numbers in a passcode.
- **(Work Profile) Require Special** – The minimum count of special characters in a passcode.
- **(Work Profile) Require Uppercase** – The minimum count of uppercase letters in a passcode.
- **(Work Profile) Screenlock Password Quality** – The screen unlock mechanism. This can be set to *none*, *biometric*, *password*, *pattern*, *pin*, *pin_complex*, *alpha*, *alphanumeric* and *complex*.
  - If the device uses a different screen lock type to the one specified by the console, the device is flagged as non-compliant.
  - If the screen unlock type is *password*, then **Passcode Length** and **Passcode History** policies are enforced.
  - If the screen unlock type is *pin* or *pin_complex*, then **Passcode History** policies are enforced.
- **Require Letters** – The minimum count of letters in a Workspace Managed Device passcode.

- **Require Lowercase** – The minimum count of lowercase letters in a Workspace Managed Device passcode.
- **Require Non-Letters** – The minimum count of numbers and symbols in a Workspace Managed Device passcode.
- **Require Number** – The minimum count of numbers in a Workspace Managed Device passcode.
- **Require Uppercase** – The minimum count of uppercase letters in a Workspace Managed Device passcode.
- **Screenlock Password Quality** – The screen unlock mechanism. This can be set to none, biometric, password, pattern, pin, pin_complex, alpha, alphanumeric and complex.
    - If the device uses a different screen lock type to the one specified by the policy, the device is flagged as non-compliant.
    - If the screen unlock type is password, then **Passcode Length** and **Passcode History** policies are enforced.
    - If the screen unlock type is pin or pin_complex, then **Passcode History** policies are enforced.

The following properties are supported by iOS only:

- **iOS Allow Simple** – Boolean. If *True*, a simple passcode is allowed. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters. For example: 123 or CBA.
- **iOS Force Pin** – Boolean. If *True*, the user is forced to set a PIN. Simply setting this value (and not others) forces the user to enter a passcode.
- **iOS Max Grace Period** – The maximum grace period, in minutes, to unlock the phone without entering a passcode.
- **iOS Max Inactivity** – The number of minutes for which the device can be idle (without being unlocked by the user) before it gets locked by the system.

Single Sign On

These properties support single sign-on using Kerberos authentication from iOS devices at iOS v7 or above.

For full details of this functionality, see **"Configuring Kerberos-Based Authentication" on page 232**.

The following properties are supported by iOS only:

- **Account Name** – The name for the account.
- **Authentication Realm** – The Kerberos realm name. This value is case sensitive.
- **Enabled** – Boolean. If *True*, Kerberos authentication is enabled.
- **Package names allowed to use Kerberos Auth** – (Optional) A newline-separated list of applications identifiers that are allowed to use this login. Each line of this property represents an application. For example:

  com.microsoft.outlook
  com.google.mail.

  Note: If this field not specified, all app identifiers match automatically for this login.
- **Principal Name** – The Kerberos principal name. It is best practice to set to the macro string value *<USER_USERNAME>*. This macro value is automatically replaced with the user's name when connecting to a device.
- **URL Prefix Matches to use Kerberos Auth** – A newline-separated list of URLs prefixes that must be matched to use this account for Kerberos authentication over HTTP. Each line of this property represents a URL, and must begin with either *http://* or *https://*. For example:

  http://demo.pwskerb.example1
  http://demo.pwskerb.example2

  Note: Kerberos authentication for the user will be performed manually once, on the first match of any of the listed URLs. For all subsequent uses of *any* URL, Kerberos authentication will be performed automatically.

ActiveSync

All **ActiveSync** properties are supported by both Android and iOS. See also **"iOS ActiveSync" on page 176**.

- **Activesync Accept All Certs** – Boolean. If *True*, the Workspace email client will accept an untrusted server certificate.
- **Activesync Allow Authentication via Certificate**. Boolean. If *True*, the use of the following workspace properties is enabled. See **"Enterprise PKI Integration" on page 183** for full details.
    - **Use SCEP to request certificate for Android ActiveSync from external PKI server**.
    - **Use SCEP to request certificate for iOS ActiveSync from external PKI server**.
    - **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices**.
- **Activesync Domain** – The domain set for the Workspace ActiveSync connection. The ActiveSync domain must be the Enterprise domain, which should be the same as the Exchange Server domain.
- **Activesync Server** – If the proxy uses PCS, this property should be set to ActiveSync Server Proxy address of the Pulse Connect Secure (PCS). Otherwise, this can be left blank.
- **Activesync Server Proxy** – This must be set to *Security Appliance* if PCS is used. Otherwise, it should be set to *None*.
- **Activesync Ssl** – If the Workspace client will connect to the ActiveSync server using an SSL connection, this should be set to *True*.
- **Activesync Userid Field** – If the **ActiveSync Server Proxy** uses PCS, this must be set to *username*. Otherwise, it should be set to *email*.
- **UPN Domain Name** – The domain set for constructed UPN method of login authentication.
- **Use Constructed UPN for Workspace Email** – Boolean. If *True*, the constructed UPN is used for ActiveSync email, and Office365 users will be able to use UPN as the login username instead of using their email addresses.
- **Use Pulse One for authentication (Override Active Sync Server)** – The following values are supported:
    - *True* – Pulse One will be used as authentication server for ActiveSync connections, and it will override the configured ActiveSync server settings.
    - *False* – existing ActiveSync server settings will be used for ActiveSync connections.

App Visibility

All **App Visibility** properties are supported by both Android and iOS:

- **Aggregate Duration Hours** – The aggregation window (in hours) for collecting app visibility metrics on the mobile device. The default is 1, the maximum is 72. At the end of this window, a new set of metrics is started. Metric sets are retained by the mobile device and sent to the server on a schedule defined by **Report Frequency Hours**.

  Note: **Aggregate Duration Hours** should not be greater than **Report Frequency Hours**.

- **Enable App Visibility Supporting** –Boolean. If True, app visibility reporting is performed by the mobile device, and reported to the server.
- **Network Access** – This defines when metrics can be sent by the mobile device to the server. This allows the IT Admin to limit usage of mobile data. Supported settings are *Wifi Only* and *Wifi And Cellular*.
- **Report Frequency Hours** – The frequency (in hours) at which the mobile device sends collected metrics to the server. The default is 1, the maximum is 72. IT Admin can increase this value to decrease how often metrics are sent to the server. Metrics are collected by the mobile device on a schedule defined by **Aggregate Duration Hours**.

  Note: **Report Frequency Hours** should not be less than **Aggregate Duration Hours**.

Space

All **Space** properties are supported by Android only:

- **Allow Art** – Boolean. If *True*, Android devices that run ART can be provisioned.
- **Android Email Auto Config Enabled** – Boolean. If *True*, the Workspace ActiveSync account will be configured on Android devices.
- **Android Email Manual Config Allowed** – Boolean. If *True*, the user can change the ActiveSync account settings in the Workspace.
- **Crash Count** – The number of times an app can crash in the **Crash Period Sec** time frame before the application is disabled.
- **Crash Grace Time Sec** – The number of seconds the Workspace will wait before allowing the app to restart.
- **Crash Period Sec** – The time frame for watching for repeated app crashes.
- **Debug** – Policy update explicitly uses the **Debug** policy in the console to "refresh_sec=10". The normal policy property for policy refresh has a resolution of 1 hour. This can be set to smaller periods of time.
- **Error Reporting Level** – The detail of the logging information sent to the server when the user sends a debug log. The can be set to *1*, *2* or *3*.
- **Heartbeat Time Sec** – The number of seconds between connection heartbeats.

- **Policy Expiration days** – The number of days after which a Workspace is considered to be out of compliance. The Workspace is blocked for not contacting the server. The blocked user can contact the Workspace administrator to extend the policy expiration days.

Android Restrictions

All **Android Restrictions** properties are supported by Android only:

- **Allow Screenshot** – Boolean. If *True*, the use of the screenshot function is supported.

  Note: This property is used by corporate devices only.

- **Allow to use Camera** – Boolean. If *True*, the use of the camera is supported.

  Note: This property is used by corporate devices only.

- **Block Unknown Sources** – Boolean. If *True*, users cannot install apps from unknown sources such as third-party app stores, file-sharing utilities, web browsers, and email attachments.
- **Default Runtime Permission** – Sets the chosen value as default for all permissions for all apps on a policy. The supported values are *prompt*, *grant* and *deny*.

  Note: If the administrator modifies the runtime permission from *grant* to *deny* and enforces the policy on an existing provisioned device, the user must clear the cache on all managed apps.

- **Disallow Cross Profile Copy Paste** – Boolean. If *True*, users cannot copy the contents of this work profile and paste into other profiles. Users can still copy the contents of other profiles and paste into this work profile.

iOS Restrictions

All **iOS Restrictions** properties are supported by iOS only:

- **Blacklist Package Names** – Users cannot use the apps listed in this policy on their iOS device.

  Note: This policy is applicable only to Supervised iOS devices with iOS version of 10.0 or later.

- **iOS Allow Air Drop – Boolean. If** *True*, **Air Drop is enabled.**

  Note: This policy is applicable only to Supervised iOS devices with iOS version of 10.0 or later.

- **iOS Allow Camera** – Boolean. If *True*, the camera is enabled.

  Note: This property is used by corporate devices only.

- **iOS Allow Cloud Backup** – Boolean. If *True*, iCloud backup is enabled.
- **iOS Allow Cloud Keychain Sync** – Boolean. If *True*, iCloud keychain sync is enabled.
- **iOS Allow Enterprise Book Backup** – Boolean. If *True*, the backup of enterprise books is enabled.
- **iOS Allow Enterprise Book Metadata Sync** – Boolean. If *True*, the synchronization of enterprise book metadata is enabled.

- **iOS Allow Handoff** – Boolean. If *True*, the continuity feature is enabled.
- **iOS Allow Managed App Cloud Sync** – Boolean. If *True*, the management app can use cloud sync.
- **iOS Allow Modifying Bluetooth Settings -** Boolean. If *True*, Bluetooth settings can be changed.

  Note: This policy is applicable only to Supervised iOS devices with iOS version of 10.0 or later.
- **iOS Allow Open From Managed To Unmanaged** – Boolean. If *True*, documents in managed apps and accounts also open in other managed apps and accounts.
- **iOS Allow Open From Unmanaged To Managed** – Boolean. If *True*, documents in unmanaged apps and accounts will also open in other unmanaged apps and accounts.
- **iOS Allow Screen Shot** – Boolean. If *True*, device Screen Shots are enabled.

  Note: This property is used by corporate devices only.
- **iOS Allow Siri** – Boolean. If *True*, Siri is enabled.
- **iOS Allow Siri While Locked** – Boolean. If *True*, Siri is enabled when the device is locked.

Device

All **Device** properties are supported by Android only:

- **Device Ownership** – This property is unused at this release. **Please do not use**.
- **Enable Bug Report** – Boolean. If *True*, the user will be able to send bug reports.

VPN

Different **VPN** properties are used for iOS and Android.

The following properties are supported by both Android and iOS:

- **Enable Location Awareness** – Boolean. If *True*, when the user is connected to the corporate WiFi, the VPN on-demand functionality will disconnect the VPN.
- **Vpn Certificate Auth** – Boolean. If *True*, the VPN connection will perform certificate authentication using the Workspace client certificate.
- **Vpn Connection Name** – A user-visible description of the VPN account.
- **Vpn Enabled** – Boolean. If *True*, a VPN configuration will be sent down to the Workspace.
- **Vpn Group** – The VPN group name. This extends IPsec architecture to support PCS that is shared by a group of security appliances.
- **Vpn Host** – The VPN server host name (or IP address).
- **Vpn Numeric Password** – Boolean. If *True*, the Workspace will present the user with a PIN pad rather than a keyboard to enter their password.

- **Vpn Realm** – The Realm that the Workspace users will use.
- **Vpn Role** – The Role that the Workspace users will use.
- **Vpn Save Password** – Boolean. If *True*, the Workspace will cache the password used to connect to the VPN server.
- **Vpn Userid Field** – The Username set in the VPN configuration. This is either:
    - *username* - the user's user name is used.
    - *work email* - or user's corporate email address is used.

The following policies are supported by Android only:

- **On-Demand VPN Timeout (minutes)** – The amount of time (in minutes) during which no traffic is sent over the active tunnel by the application. After this time is elapsed, the tunnel is brought down, and the device starts monitoring for any further traffic.
- **Stealth Mode** – Boolean. If *True*, a UI-less VPN profile uses the certificate in Keystore for authentication, and the Pulse client does not come into foreground during VPN setup. The sign-in URL configured on Pulse Connect Secure server must be configured for certificate authentication.
- **Vpn Connection Type** – The type of VPN being used. Connection types supported are *manual*, *onDemand* and *alwaysOn*.
- **Vpn Verify Certificate** – Boolean. If *True*, the VPN client will only accept trusted certificates. If *False*, the VPN client will accept untrusted certificates.

The following properties are supported by iOS only:

- **Use L3 VPN** – Boolean. If *True*, L3 VPN UDP support is enabled.
- **Vpn Safari Domains** – Specifies only those domains that trigger the VPN connection.

Wifi

All **Wifi** properties are supported by both Android and iOS:

- **Enterprise Wifi Inner Authentication** – The protocol used to authenticate the username and password. Supported protocols are *PAP*, *CHAP*, *MSCHAP* or *MSCHAPv2*.
- **Enterprise Wifi Outer Identity** – An alternate username that is used outside the encrypted tunnel (for example: "anonymous") to conceal the user's identity in unencrypted packets.
- **Wifi Enabled** – Boolean. If *True*, the device will automatically join the network using WiFi.
- **Wifi Password** – The password for the WiFi network, completed by admin. If this is not set, the user is prompted during connection.
- **Wifi Protocol** – The protocol used to connect to the WiFi Network. The options are *WEP*, *WPA2*, *WPA2-Enterprise-EAP-TLS*, *WPA2-Enterprise-EAP-TTLS*, and *WPA2-Enterprise-EAP-PEAP*.

- **Wifi Ssid** – The SSID of the WiFi network.
- **Wifi Username** – The username for the WiFi network, completed by admin. If this is not set, the user is prompted during connection.

iOS ActiveSync

All **iOS ActiveSync** properties are supported by iOS only:

- **iOS Activesync Enabled** – Boolean. If *True*, the Workspace ActiveSync account will be configured on iOS devices.
- **iOS Activesync Name** – A user-visible name of the email account, shown in the Mail and Settings applications.
- **iOS Activesync Prevent Move** – Boolean. If *True*, messages cannot be moved out of this email account into another account.
- **iOS Activesync Prevent Send By 3rd Party Apps** – Boolean. If *True*, the Workspace email account is not available for sending mail in third-party applications.

iOS App Lock

All **iOS App Lock** properties are supported by iOS only:

- **iOS Lock to the App Identifier** – Enables the iOS device to be put into kiosk mode, which limits the apps and usage of some system functions. This text field is an iOS App Lock payload, and is outside the scope of this document. Please refer to Apple's own documentation.

iOS POP/IMAP

All **iOS POP/IMAP** properties are supported by iOS only:

- **iOS Email Description** – A user-visible description of the email account, shown in the Mail and Settings applications.
- **iOS Email Disable Mail Recents Syncing** – Boolean. If *True*, the Workspace email account is excluded from address Recents syncing.
- **iOS Email Enabled** – Boolean. If *True*, an IMAP or POP email account will be configured on iOS devices.
- **iOS Email Incoming Auth** – The authentication scheme for incoming mail. Supported schemes are *None*, *Password*, *MD5 Challenge-Response*, *NTLM*, and *HTTP MD5 Digest*.
- **iOS Email Incoming Host** – The incoming mail server host name (or IP address).
- **iOS Email Incoming Port** – The incoming mail server port number. If no port number is specified, the default port for a given protocol is used.
- **iOS Email Incoming Use Ssl** – Boolean. If *True*, the incoming mail server uses SSL for authentication.

- **iOS Email Outgoing Auth** – The authentication scheme for outgoing mail. Supported schemes are *None*, *Password*, *MD5 Challenge-Response*, *NTLM*, and *HTTP MD5 Digest*.
- **iOS Email Outgoing Host** – The outgoing mail server host name (or IP address).
- **iOS Email Outgoing Port** – The outgoing mail server port number.
- **iOS Email Outgoing Use Ssl** – Boolean. If *True*, the outgoing mail server uses SSL for authentication.
- **iOS Email Prevent Move** – Boolean. If *True*, messages may not be moved out of this email account into another account.
- **iOS Email Prevent Send By 3rd Party Apps** – Boolean. If *True*, the Workspace email account is not available for sending mail in third-party applications.
- **iOS Email Type** – The type of email account, either *IMAP* or *POP*.
- **iOS Email Username** – The Username that is set in the Email configuration. This is either:
    - *username* - the user's user name is used.
    - *work email* - or user's corporate email address is used.

iOS Managed Domains

All **iOS Managed Domains** properties are supported by iOS only:

- **iOS Managed Email Domains** – The domain set for the Workspace ActiveSync connection. The ActiveSync domain must be the enterprise domain which should be same as the exchange server domain.
- **iOS Managed Web Domains** – The domains that are viewed as internal to the organization.

CA Certificate

All **CA Certificate** properties are supported by iOS only:

- **iOS Trusted CA Certificate Enabled** – Boolean. If *True*, enables the SSL trust for the root CA certificate. For details about uploading CA Certificate from Pulse Workspace console, see **"Adding a CA Certificate" on page 26**.

Compliance

Different **Compliance** properties are used for iOS and Android.

The following **Compliance** properties are supported by Android only:

- **Android Pulse Client Denied To Use Location Service** – This property determines whether refusing the use of this service on a device makes the device non-compliant. There are three supported compliance settings:
    - *Allow*. If the user declines the location service, the device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN*. If the user declines the location service, the device is flagged as non-compliant and access to the VPN from the device is restricted.
    - *Wipe*. If the user declines the location service, the device is flagged as non-compliant and the workspace will be wiped from the device.
    - *Block*. If the user declines the location service, the device is flagged as non-compliant, and access to the device is prevented.
    - *Lock*. If the user declines the location service, the device is flagged as non-compliant, and access to the device is prevented.
- **Rooted Detection** – The action the client should take when it detects a Rooted device. The following actions are supported:
    - *Allow* – The Rooted device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN* – The Rooted device is flagged as non-compliant and VPN access is removed.
    - *Lock*. The Rooted device is flagged as non-compliant, and access to the device is prevented.
    - *Wipe* – The Rooted device is flagged as non-compliant and will be wiped.
- **USB Debugging** – Determines the action the client should take when it detects that USB debugging has been enabled. The actions are:
    - *Allow* – The device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN* – The device is flagged as non-compliant, and VPN access is removed.
    - *Block* – The device is flagged as non-compliant and all network access is removed.
    - *Lock* – The device is flagged as non-compliant and is locked.
    - *Wipe* – The device is flagged as non-compliant and will be wiped.

The following **Compliance** properties are supported by iOS only:

- **iOS Pulse Client Denied To Use Location Service** – This property determines whether refusing the use of this service on a device makes the device non-compliant. There are three supported compliance settings:
    - *Allow*. If the user declines the location service, the device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN*. If the user declines the location service, the device is flagged as non-compliant and access to the VPN from the device is restricted.
    - *Wipe*. If the user declines the location service, the device is flagged as non-compliant and the workspace will be wiped from the device.
- **Jail Break Detection** – The action the client should take when it detects a "jailbreak" device. The following actions are supported:
    - *Allow* – The "jailbreak" device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN* – The "jailbreak" device is flagged as non-compliant, and VPN access is removed.
    - *Wipe* – The "jailbreak" device is flagged as non-compliant and will be wiped.
- **Minimum OS Version** – Sets the minimum iOS version.
- **Minimum Pulse Client Version** – Sets the minimum Pulse Client version.
- **Non-Compliant OS Version Action** – If the user provisions a device that has an iOS version lower than the **Minimum OS Version** policy, the device becomes a *non-compliant* device. Actions for a non-compliant device can be one of the following:
    - *Allow* – The device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN* – The device is restricted from VPN access.
    - *Wipe* - The profile is wiped off from the user's device.
- **Non-Compliant Pulse Client Version Action** – If the user provisions a device that has Pulse Client version lower than the **Minimum Pulse Client Version** policy, the device becomes a *non-compliant* device. Actions for a non-compliant device can be one of the following:
    - *Allow* – The device is flagged as non-compliant, but the user's access is not restricted.
    - *Restrict VPN* – The device is restricted from VPN access.
    - *Wipe* – The workspace is wiped off from the user's device.

Nine

The Nine Work email app, provided by Google apps, synchronizes with Exchange Server using ActiveSync, and it is based on Android for Work.

All **Nine** properties are supported by Android only:

- **License Number** – License to use Nine Work email app.

Mail+

All **Mail+** properties are supported by iOS only:

- **Mailplus Allow Open In** – Boolean. If *True*, the user can open documents in other apps.
- **Mailplus Allow Print** – Boolean. If *True*, the user can print mails.
- **Mailplus Auto Config Enabled** – Boolean. If *True*, the Mail+ app configures automatically.
- **Mailplus Disable Copy Paste** – Boolean. If *True*, users cannot use copy and paste. This prevents the user from inadvertently sending sensitive information to third party apps.
- **Mailplus License Key** – The Mail+ license key, which is provided by iKonic Apps.
- **Mailplus Passcode Allow Simple** – Boolean. If *True*, passcode complexity can be simple.
- **Mailplus Passcode Alpha Numeric Required** – Boolean. If *True*, passcodes require alphanumeric characters.
- **Mailplus Passcode Enabled** – Boolean. If *True*, a Mail+ app passcode is supported. This value takes precedence over ActiveSync policies. This does not affect the device passcode.
- **Mailplus Passcode Length** – The minimum overall length of the passcode.
- **Mailplus Passcode Require Special** – The minimum count of special characters in a passcode.
- **Mailplus Passcode Time Out** – The idle time in seconds after which the Mail+ app will be locked or will run in the background.

VPN On Demand

VPN on Demand (VOD) is currently supported by iOS devices running as *managed clients*, see **“Understanding Managed Devices and Managed Clients” on page 42**.

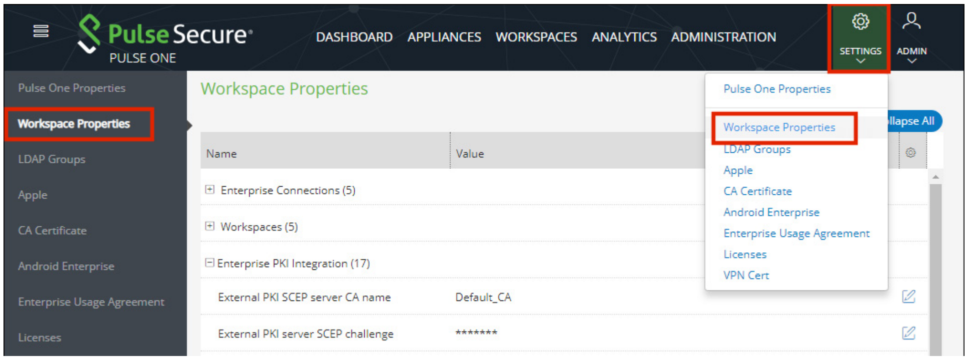
- **VPN OnDemand Enabled** – Boolean. If *True*, VPN on Demand is enabled, see **“Configuring Managed Clients” on page 95**.

Configuring Workspace Properties

To configure Workspace properties:

1. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties**.

FIGURE 213 Workspace Properties



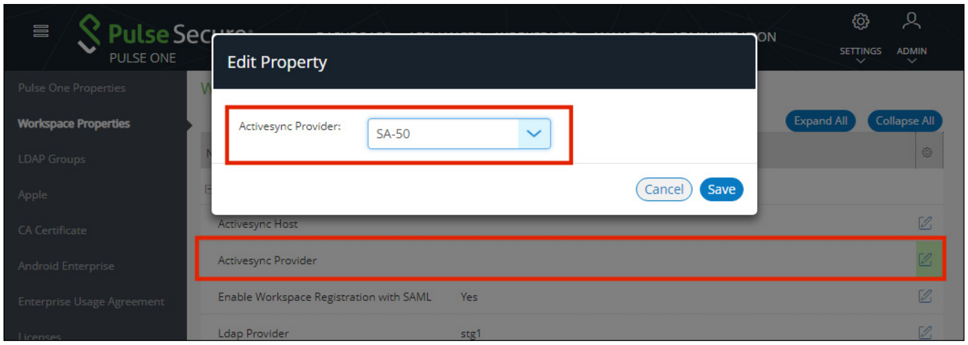
Workspace Properties

Name	Value
⊞ Enterprise Connections (5)	
⊞ Workspaces (5)	
⊟ Enterprise PKI Integration (17)	
External PKI SCEP server CA name	Default_CA
External PKI server SCEP challenge	*******

2. Click the **Edit** button corresponding to the field you want to edit.

3. Change the value and then click **Save**. For example:

FIGURE 214 Edit Property



Edit Property

Activesync Provider: SA-50

Activesync Host	
Activesync Provider	
Enable Workspace Registration with SAML	Yes
Ldap Provider	stg1

Enterprise Connections

The **Enterprise Connections** settings are described below:

- **Activesync Host** – Address of the Pulse Workspace that ActiveSync Proxy will forward ActiveSync connections to. This address must be accessible to the Pulse Workspace ActiveSync Proxy.
- **Activesync Provider** – Pulse Connect Secure appliance to which Pulse One / Pulse Workspace will forward the ActiveSync notifications.
- **Enable Workspace Registration with SAML** – Boolean. If *True*, enables single sign-on.
- **Ldap Provider** – The Pulse Connect Secure appliance that is configured for the User's group membership, based auto-provisioning.

- **SDP Provision Certificate** – This property is required for SDP operation. See the *Pulse Secure Software Defined Perimeter* documentation for full details of its use.
- **VPN provider** – The Pulse Connect Secure appliance that is configured to provide VPN access, see **"Configuring Auto-Config of a VPN Provider on Mobile Devices" on page 186**.

Workspaces

The **Workspaces** settings are described below:

- **Allow the ability to perform full device wipes?** – Boolean. If *True*, a full device wipe can be performed on a target device. See **"Performing Workspace Actions" on page 143**.
- **Desired accuracy for workspace location in meters** – The requested accuracy for the use of device location on iOS. The default is 100 meters for iOS devices. See **"Configuring Device Location" on page 242**.

  Note: This property is not used by Android devices. The location of Android devices is always the best approximation using available network information.
- **Display Advanced AFW Properties** – Boolean. If *True*, shows advanced AFW properties (**App Permissions**).
- **Enable enrollment of managed iOS clients** – Boolean. This controls how iOS mobile devices are enrolled by Pulse Workspace:
  - If *True*, mobile devices will be enrolled as *managed clients.*
  - If *False* (default), mobile devices will be enrolled as *managed workspaces*.

  For full details, see **"Understanding Managed Devices and Managed Clients" on page 42**.
- **Enable International App Stores** – Boolean. If *True*, you can choose apps from international app stores.
- **Enable Location Service** – Boolean. If True, the device location feature is supported on all compatible devices. See **"Working with Device Location" on page 235**.
- **Location Maps Service API Key** – Optional API Key. Where supplied, Google Maps is used to display device location. See **"Working with Device Location" on page 235**.

Enterprise PKI Integration

iOS Operating system has built-in MDM client, which handles the profile management and it has support for Simple Certificate Enrollment Protocol (SCEP). The Android Operating System does not come with the SCEP support, so SCEP functionalities are built into the Pulse Secure Android Client app.

To use SCEP with Windows server, the user needs to enable NDES service on the Windows server, and ensure it is reachable by both Workspace server and client devices. For more details, see **TechNet: Active Directory Certificate Services (AD CS): Network Device Enrollment Service (NDES)**.

The **Enterprise PKI Integration** settings are described below:

- **External PKI SCEP server CA name** – (Optional) Windows NDES server typically accepts any value. If the user has already set up the NDES server to only accept a specific value, they can specify it here.
- **External PKI server SCEP challenge** – If **Use static SCEP challenge for external PKI server** is *True*, specify the challenge password required by the client to enroll the certificate.
- **External PKI server SCEP URL** – This is the NDES service address the client will send requests to. In general, the default location is *https://FQDN-CertSrv/mscep.dll*.
- **Use external PKI server** – This is the master switch of the external PKI feature. Boolean. If *False*, the system uses built-in CA no matter how other configurations were set.
- **Use SCEP to request certificate for Android ActiveSync from external PKI server** – Boolean. If *True*, a SCEP payload is delivered to all onboarded Android devices that use a policy with the **Activesync Allow Authentication via Certificate** property enabled. See **"ActiveSync" on page 171**. The device then automatically retrieves an ActiveSync certificate from the SCEP server.

  Note: If the **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices** property is also *True*, the **Use SCEP to request certificate for Android ActiveSync from external PKI server** property overrides it, and SCEP is used for Android devices.
- **Use SCEP to request certificate for Android VPN from external PKI server** – Boolean. If *True*, the VPN certificate is requested from SCEP for onboarded Android devices.
- **Use SCEP to request certificate for Android Wifi from external PKI server** – Boolean. If *True*, the WiFi certificate is requested from SCEP for onboarded Android devices.
- **Use SCEP to request certificate for iOS ActiveSync from external PKI server** – Boolean. If *True*, a SCEP payload is delivered to all onboarded iOS devices that use a policy with the **Activesync Allow Authentication via Certificate property** enabled. See **"ActiveSync" on page 171**. The device then automatically retrieves an ActiveSync certificate from the SCEP server.

  Note: If the **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices** property is also *True*, the **Use SCEP to request certificate for iOS ActiveSync from external PKI server** property overrides it, and SCEP is used for iOS devices.

- **Use SCEP to request certificate for iOS MDM from external PKI server** – Boolean. If *True*, the iOS MDM certificate is requested from SCEP for onboarded iOS devices. Also, the CA certificate needs to be uploaded from the **CA certificate** settings page.

  Note: If this value is changed, it will change how the Workspace server validates the MDM command signatures sent by iOS devices. As a result, any enrolled devices will need to be re-enrolled to get a new MDM certificate so that it can work again.

- **Use SCEP to request certificate for iOS VPN from external PKI server** – Boolean. If *True*, the VPN certificate is requested from SCEP for onboarded iOS devices.

- **Use SCEP to request certificate for iOS Wifi from external PKI server** – Boolean. If *True*, the WiFi certificate is requested from SCEP for onboarded iOS devices.

- **Use static SCEP challenge for external PKI server** – Boolean. Set to *True* if the SCEP server is set up to accept a static challenge, or any challenge (password disabled). If *True*, you must set **External PKI server SCEP challenge**.

- **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices** – Boolean. If *True*, the ActiveSync certificate is requested from Windows CA server CAWE for all onboarded devices that meet the following criteria:

  - This workspace property is only used on devices whose policy includes an enabled **Activesync Allow Authentication via Certificate** property, see **"ActiveSync" on page 171**.

  - This workspace property is not used for Android devices when the **Use SCEP to request certificate for Android ActiveSync from external PKI server** workspace property is set to *True*. That is, the SCEP property is used instead.

  - This workspace property is not used for iOS devices when the **Use SCEP to request certificate for iOS ActiveSync from external PKI server** workspace property is set to *True*. That is, the SCEP property is used instead.

- **Use Windows CA server CAWE to request iOS MDM certificates** – Boolean. If *True*, the iOS MDM certificate is requested from Windows CA server CAWE for onboarded iOS devices. Also, the CA certificate needs to be uploaded from the **CA certificate** settings page.

  Note: If this value is changed, it will change how the Workspace server validates the MDM command signatures sent by iOS devices. As a result, any enrolled iOS devices will need to be re-enrolled to get a new MDM certificate so that it can work again.

- **Use Windows CA server CAWE to request SDP device certificates** – Boolean. If *True*, the SDP device certificate is requested from Windows CA server CAWE for all onboarded devices. See the *Pulse Secure Software Defined Perimeter* documentation for full details of its use.

- **Use Windows CA server CAWE to request VPN certificates for both Android and iOS devices** – Boolean. If *True*, the VPN certificate is requested from Windows CA server CAWE for all onboarded devices.

- **Use Windows CA server CAWE to request WIFI certificates for both Android and iOS devices** – Boolean. If *True*, the WiFi certificate is requested from SCEP for all onboarded devices.
- **Windows CA Server certsrv URL** – This is the URL of the Windows *certsrv* web page. The *mscep_admin* page under this URL is used to fetch a new SCEP challenge. If the system uses static SCEP challenge, this configuration is not required.
- **Windows CA Server certificate template name** – (Optional) The Windows CA server template name.
- **Windows CA Server certsrv page user name** – Set with a username that has access to the mscep_admin page under the certsrv URL. If the system uses static SCEP challenge, this configuration is not required.
- **Windows CA Server certsrv page user password** – Set with a password that has access to the mscep_admin page under the certsrv URL. If the system uses static SCEP challenge, this configuration is not required.

Misc

The miscellaneous (**Misc**) settings are described below:

- **Support Email** – Pulse Workspace support center's email address. This email address will be shown in the Support information displayed on the device.
- **Support Phone** – Pulse Workspace support center's phone number. This phone number will be shown in the Support information displayed on the device.

Configuring Auto-Config of a VPN Provider on Mobile Devices

Each VPN-enabled mobile device requires a CA certificate to perform certificate-based VPN authentication. This certificate can be downloaded and configured manually, but Pulse Workspace supports the automatic configuration of a VPN provider based on a policy. This enables the automatic download of the required CA certificate to each device that uses the policy.

To do this, you must perform the following tasks:

- "Ensuring that PCS has a CA Certificate Associated With its External Port" on page 186.
- "Ensuring that PCS is Synchronized with Pulse One" on page 188.
- "Configuring a VPN Provider in the Workspace Properties" on page 189.
- "Updating and Publishing a Policy to Use a Specified VPN Provider" on page 191.

After these tasks are complete, all devices that use the policy will have a CA certificate that enables authentication-based access to the VPN on a PCS appliance.

Ensuring that PCS has a CA Certificate Associated With its External Port

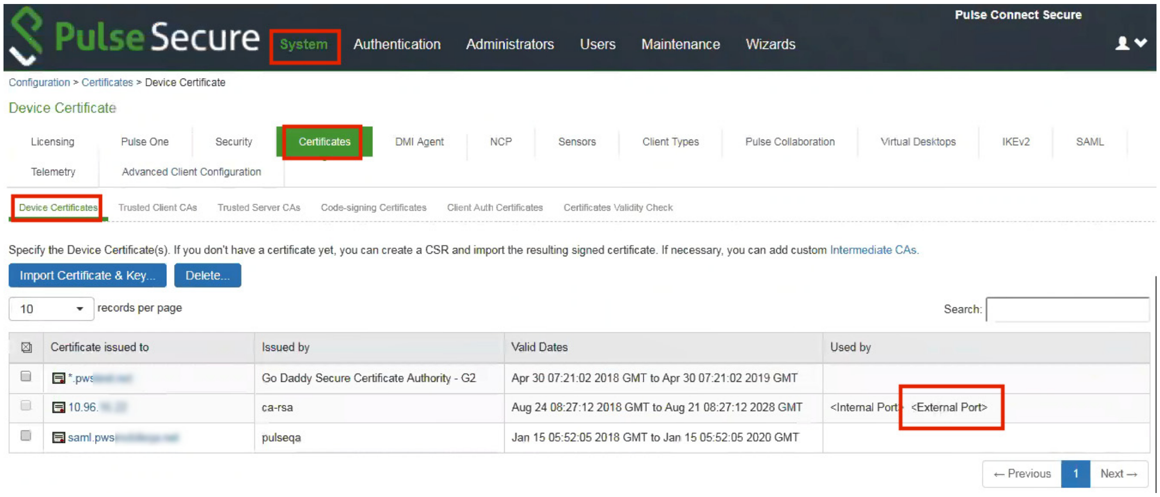
First, you must ensure that the PCS that will act as the VPN provider has a CA certificate assigned to its external port.

To view current CA certificates:

1. Log into the PCS appliance as an administrator.
2. Select the **System** menu, and then select **Configuration > Certificates > Device Certificates**.

   The PCS **Device Certificates** page appears. This page shows all current CA certificates on the PCS appliance. For example:

FIGURE 215 Device Certificates



Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

☒	Certificate issued to	Issued by	Valid Dates	Used by
□	*.pws[redacted]	Go Daddy Secure Certificate Authority - G2	Apr 30 07:21:02 2018 GMT to Apr 30 07:21:02 2019 GMT	
□	10.96.[redacted]	ca-rsa	Aug 24 08:27:12 2018 GMT to Aug 21 08:27:12 2028 GMT	<Internal Port> <External Port>
□	saml.pws[redacted]	pulseqa	Jan 15 05:52:05 2018 GMT to Jan 15 05:52:05 2020 GMT	

In this example:

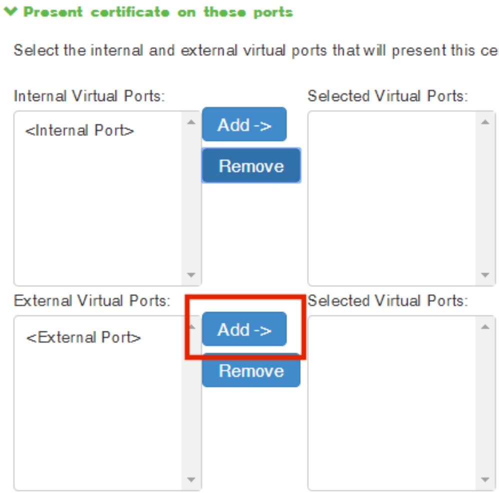
- The *10.96.xx.xx* CA certificate has a **Used by** property that includes <External Port>, which indicates that it is associated and in use on the external interface of the PCS appliance.
- The other certificates have no **Used by** values set. These certificate are not currently assigned to any interface on the PCS appliance.

To assign a CA certificate to the external interface of a PCS:

1. Log into the PCS appliance as an administrator.
2. View all current CA certificates on the appliance on the **Device Certificates** page (see above).
3. Locate the CA certificate that you want to assign to the external port of the PCS.
4. In the **Certificate issued to** column, click the hyperlink for the required CA certificate.

   The **Certificate Details** page appears. Under **Present certificate on these ports**, an unassociated certificate will look as follows:

   FIGURE 216 CA Certificate Not Associated with PCS Interfaces

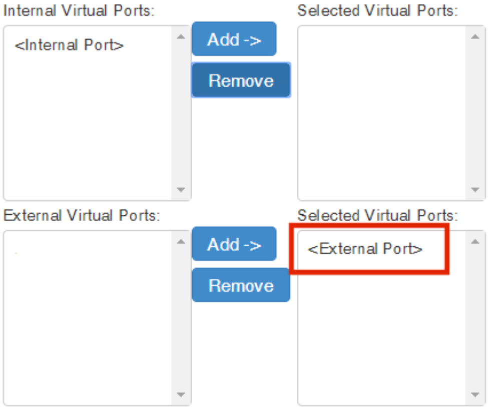


Present certificate on these ports

Select the internal and external virtual ports that will present this certificate:

5. Under **External Virtual Ports**, click **Add** to move <External Port> into **Selected Virtual Ports**. For example:

   FIGURE 217 CA Certificate Associated with the External Interface

6. Click **Save Changes** to close and return to the **Device Certificates** page.

The CA certificate will show that it is **Used by** the <External Port>.

You must now ensure that Pulse One and the PCS are synchronized, see **"Ensuring that PCS is Synchronized with Pulse One" on page 188**.

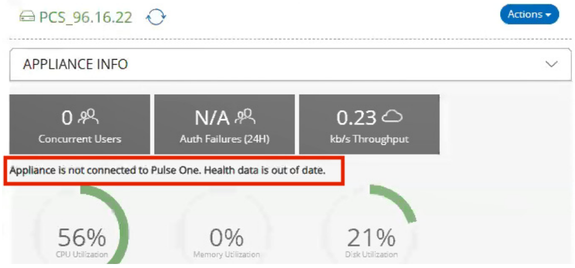
Ensuring that PCS is Synchronized with Pulse One

After you have updated a CA certificate to be associated with the external interface of a PCS appliance, you must then ensure that the PCS configuration is synchronized with the Pulse One appliance.

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu, and then the **Appliances** tab.
3. In the **Appliances** tab, locate the PCS appliance that you want to be the VPN provider for a mobile device.
4. Wait until Pulse One synchronizes with the PCS appliance.

   Before synchronization occurs, the **Appliance Info** panel for the appliance shows the following message:

   FIGURE 218 PCS Appliance Information

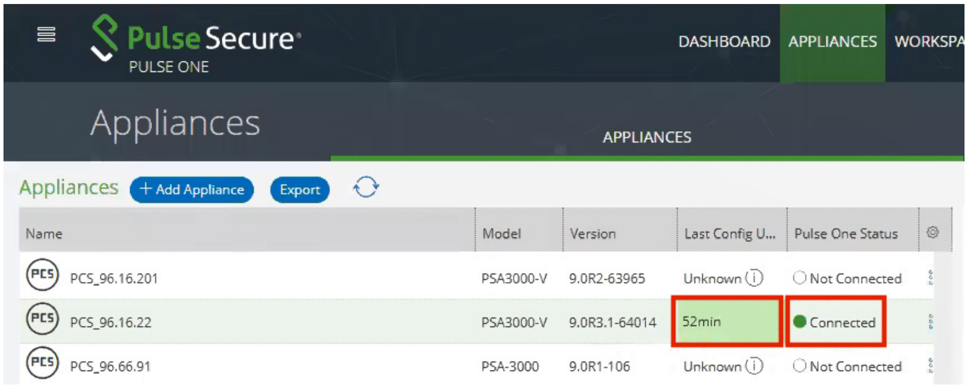
   Appliance is not connected to Pulse One. Health data is out of date.

After the listed PCS appliance meets both of the following conditions, it is synchronized:

- A **Pulse One Status** of Connected.
- A **Last Config Update** that shows the elapsed time since the last update. For example, 25 mins. If this value is shown as Unknown, the device is not yet synchronized.

For example:

FIGURE 219 Synchronized PCS on Pulse One

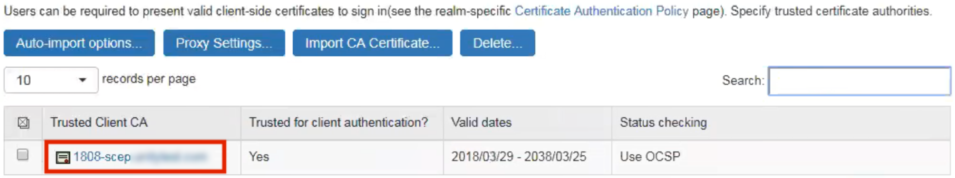


Name	Model	Version	Last Config U...	Pulse One Status
PCS_96.16.201	PSA3000-V	9.0R2-63965	Unknown ⓘ	○ Not Connected
PCS_96.16.22	PSA3000-V	9.0R3.1-64014	52min	● Connected
PCS_96.66.91	PSA-3000	9.0R1-106	Unknown ⓘ	○ Not Connected

In this example, the PCS_96.16.22 appliance is synchronized with Pulse One.

5. (Optional) Confirm the synchronization by verifying the automatic upload of the CA certificate in the **Trusted Client CA** page on a PCS appliance.

FIGURE 220 Confirm Upload of the CA Certificate


Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

☒	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
□	1808-scep [redacted]	Yes	2018/03/29 - 2038/03/25	Use OCSP

You must now configure the VPN Provider workspace property, see **"Configuring a VPN Provider in the Workspace Properties" on page 189**.

Configuring a VPN Provider in the Workspace Properties

After Pulse One and the PCS appliance are synchronized, you can configure the PCS appliance to be a VPN Provider.

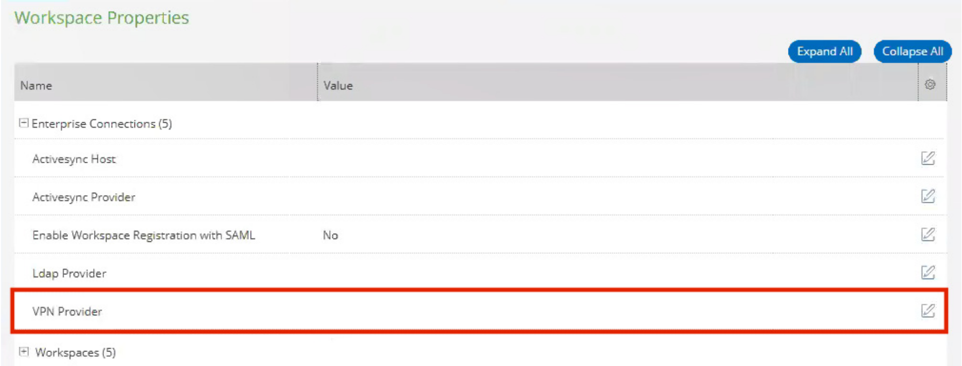
To configure a PCS appliance as a VPN provider:

1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties**.

   The **Workspace Properties** page appears.

3. Expand the Enterprise Connections category. For example:

FIGURE 221 Workspace Properties

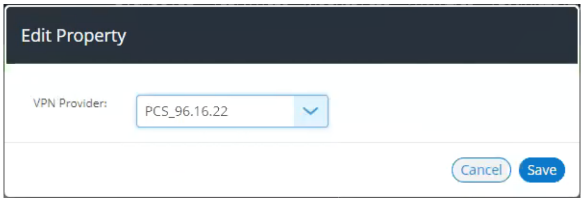


Name	Value
⊟ Enterprise Connections (5)	
Activesync Host	
Activesync Provider	
Enable Workspace Registration with SAML	No
Ldap Provider	
VPN Provider	
⊞ Workspaces (5)	

4. Click the **Edit** (✎) icon for the **VPN Provider** entry.

   The **Edit Property** dialog appears. For example:

   FIGURE 222 Edit VPN Provider



VPN Provider: PCS_96.16.22

5. Select the required PCS appliance as the **VPN Provider**.

   Note: You cannot select a PCS appliance that is in an appliance group as the **VPN provider**.

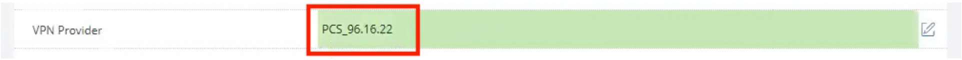
   In this example, the *PCS_96.16.22* PCS appliance is selected.

6. Click **Save**.

   Note: If you selected a PCS appliance running a version that is earlier than v9.0R3, the selection is accepted, but you must reboot the selected appliance to complete the configuration.

   The **Workspace Properties** page updates. For example:

   FIGURE 223 Updated Workspace Properties



VPN Provider	PCS_96.16.22

After the VPN workspace property is set, you can update any policy that requires the use of the selected VPN provider, see **"Updating and Publishing a Policy to Use a Specified VPN Provider" on page 191**.

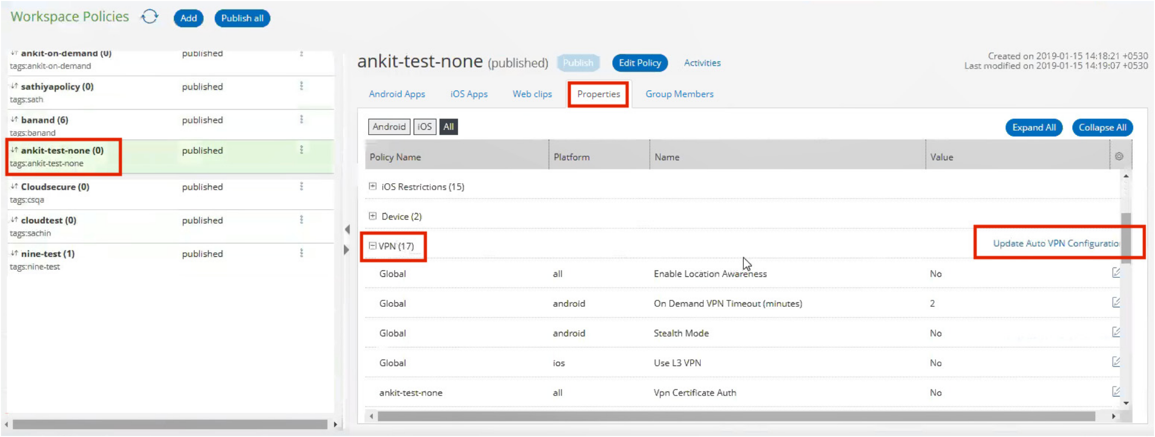
Updating and Publishing a Policy to Use a Specified VPN Provider

After the workspace properties are set, you can update the VPN policy properties on any policy that requires them. You can then publish the policy to all devices.

To update the VPN policy properties for a policy:

1. Log into Pulse One as an administrator.
2. Select the **Workspaces** menu.
3. Select the **Policies** tab.
4. Select the required policy.
5. Click the **Properties** tab for the selected policy.
6. Expand the *VPN* category to view current VPN settings. For example:

FIGURE 224 VPN Policy Properties: Auto Update VPN Configuration



ankit-on-demand (0) tags:ankit-on-demand	published
sathiyapolicy (0) tags:sath	published
banand (6) tags:banand	published
ankit-test-none (0) tags:ankit-test-none	published
Cloudsecure (0) tags:csqa	published
cloudtest (0) tags:sachin	published
nine-test (1) tags:nine-test	published

ankit-test-none (published)

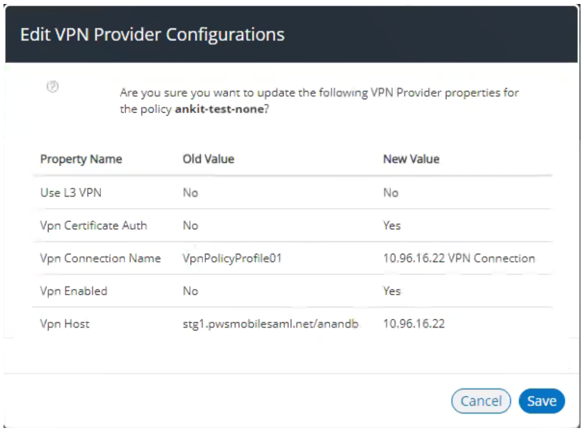
Created on 2019-01-15 14:18:21 +0530
Last modified on 2019-01-15 14:19:07 +0530

Policy Name	Platform	Name	Value
⊞ iOS Restrictions (15)			
⊞ Device (2)			
⊟ VPN (17)			
Global	all	Enable Location Awareness	No
Global	android	On Demand VPN Timeout (minutes)	2
Global	android	Stealth Mode	No
Global	ios	Use L3 VPN	No
ankit-test-none	all	Vpn Certificate Auth	No

7. Next to the VPN category, click **Update Auto VPN Configuration**.

   The **Edit VPN Provider Configurations** dialog appears. This indicates current settings and new settings from the VPN provider CA certificate. For example:

   FIGURE 225 Edit VPN Provider Configurations

   Edit VPN Provider Configurations

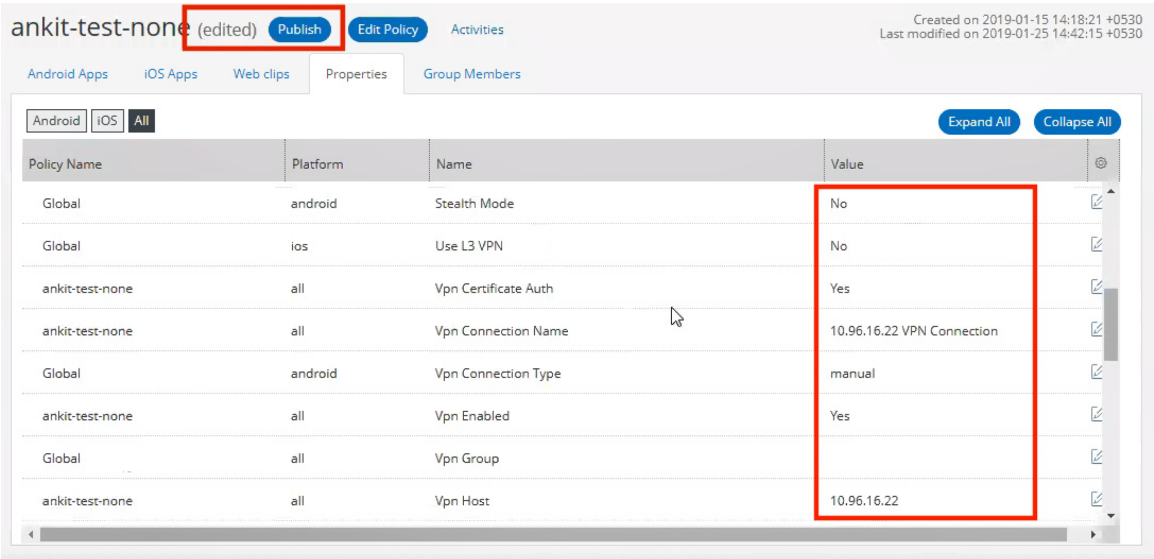
   Are you sure you want to update the following VPN Provider properties for the policy **ankit-test-none**?

Property Name	Old Value	New Value
Use L3 VPN	No	No
Vpn Certificate Auth	No	Yes
Vpn Connection Name	VpnPolicyProfile01	10.96.16.22 VPN Connection
Vpn Enabled	No	Yes
Vpn Host	stg1.pwsmobilesaml.net/anandb	10.96.16.22

8. Click **Save** to confirm the changes.

   The **Policies** tab updates to show the new VPN values, and the policy shows as Edited. For example:

   FIGURE 226 Updated VPN Policy Properties

   ankit-test-none (edited)

   Created on 2019-01-15 14:18:21 +0530
   Last modified on 2019-01-25 14:42:15 +0530

Policy Name	Platform	Name	Value
Global	android	Stealth Mode	No
Global	ios	Use L3 VPN	No
ankit-test-none	all	Vpn Certificate Auth	Yes
ankit-test-none	all	Vpn Connection Name	10.96.16.22 VPN Connection
Global	android	Vpn Connection Type	manual
ankit-test-none	all	Vpn Enabled	Yes
Global	all	Vpn Group	
ankit-test-none	all	Vpn Host	10.96.16.22

9. Click **Publish**.

   The policy's state changes from *edited* to *publishing* and then *published*.

   This applies the policy to all mobile devices that use the policy.

The process is now complete.

Configuring ActiveSync

This section describes the following ActiveSync processes:

- **“Configuring Office365 as an ActiveSync Proxy” on page 193**.
- **“Configuring a Security Appliance as an ActiveSync Proxy” on page 194**.

Configuring Office365 as an ActiveSync Proxy

To configure *Office365* as an ActiveSync proxy:

1. Navigate to **Policies**.
2. Select the policy name for which you would like to add ActiveSync configuration.
3. Click **Properties**.
4. Under **ActiveSync**, configure the following:
    - **ActiveSync Accept All Certificates**: *true*
    - **ActiveSync Domain**: *pulsesecure.net*
    - **ActiveSync Server**: *outlook.office365.com*
    - **ActiveSync Server Proxy**: *None*
    - **ActiveSync SSL**: *true*
    - **ActiveSync UserID Field**: *email* or *username*
        - If **ActiveSync Userid Field** is set as *username*, in the *Gmail* and *Google Calendar* apps it shows *activesync_domain\Username*.
        - If **ActiveSync Userid Field** is set as *email*, in the *Gmail* and *Google Calendar* apps it shows *username@domain.com*.

    Note: The *Divide Productivity* app is no longer supported and no more available in Google Play Store. Instead, Google's *Gmail* and *Google Calendar* apps provide universal *Exchange* support on Android and enterprise-focused features like managed configurations, scheduling, rich text formatting, and Exchange ActiveSync 16 support. For details, refer to see **End of Life for the Divide Productivity app**.
5. For Android policies only:
    - Navigate to **Policies > <policy_name> > Properties**.
    - Under **Space**, set **Android Email Auto Configuration Enabled** to *true*.

6. For iOS policies:
    - Navigate to **Policies > <policy_name> > Properties**.
    - Under **iOS ActiveSync**, set **iOS ActiveSync Enabled** to *true*.
7. Click **Publish**.

Configuring a Security Appliance as an ActiveSync Proxy

This feature enables a Pulse Connect Secure gateway to function as an ActiveSync proxy for Mobile devices that are onboarded through Pulse Workspace Server. Pulse Connect Secure gateway will be able to filter out and reject ActiveSync connection requests coming from unauthorized mobile devices and allow only those devices that have been successfully provisioned on Pulse Workspace Server.

- **"Configuring Email Policy Attributes for ActiveSync" on page 194**.
- **"Specifying Role-Based Options" on page 195**.
- **"Configuring the Appliance for ActiveSync" on page 197**.

Configuring Email Policy Attributes for ActiveSync

To configure policy attributes:

1. Navigate to **Policies**.
2. Select the policy name for which you would like to add ActiveSync configuration.
3. Click **Properties**.
4. Under **ActiveSync**, configure the following:
    - **ActiveSync Accept All Certificates**: *true*
    - **ActiveSyncDomain**: *pulsesecure.net*
    - **ActiveSync server**: *mail.pulsesecure.net*
    - **ActiveSync Server Proxy**: *Security appliance*
    - **ActiveSync SSL**: *true*
    - **ActiveSync UserID Field**: *username*
5. For Android policies only:
    - Navigate to **Policies > <policy_name> > Properties**.
    - Under **Space**, set **Android Email Auto Configuration Enabled** to *true*.

6. For iOS policies:

    - Navigate to **Policies > <policy_name> > Properties**.
    - Under **iOS ActiveSync**, set **iOS ActiveSync Enabled** to *true*.

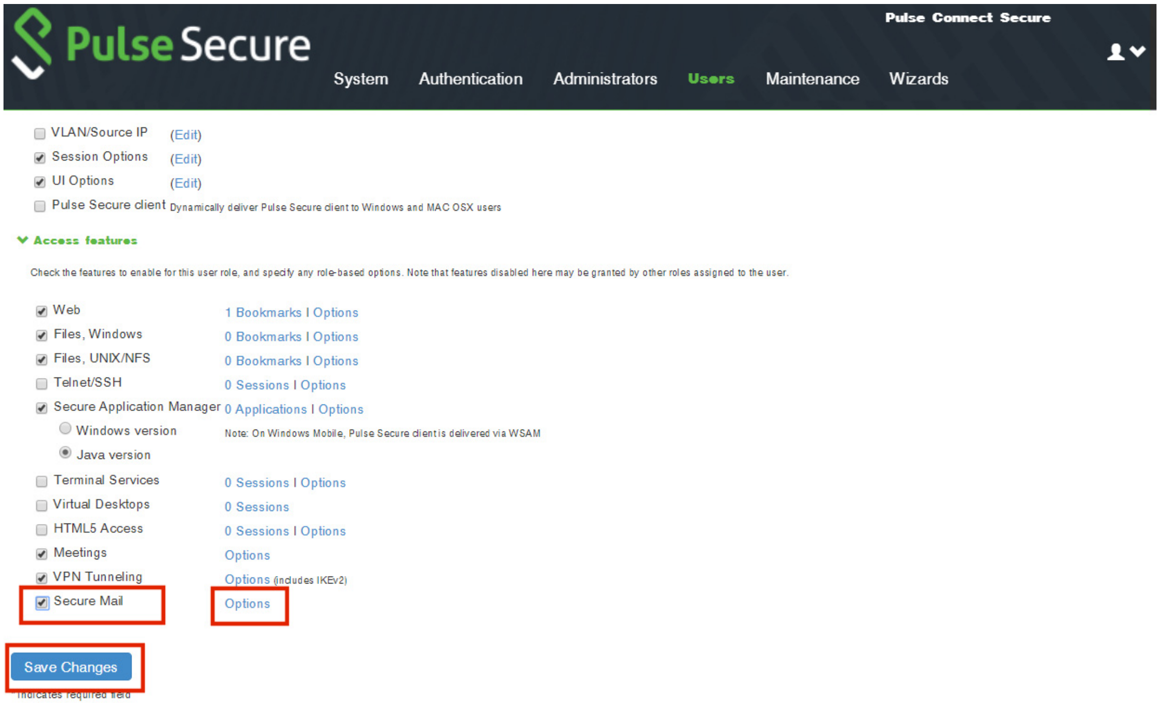
7. Click **Publish**.

Specifying Role-Based Options

It is recommended that admin creates a new role for Pulse Workspace onboarded devices. Assuming that admin creates a new role with the name as “secure_email”, perform the following procedure:

1. Navigate to **Users > User Roles**.
2. Select the *secure_email* role.
3. Enable the **Secure Mail** check box.
4. Under **Access features**, click **Save Changes**.

FIGURE 227 Secure Email Options



□ VLAN/Source IP (Edit)
☑ Session Options (Edit)
☑ UI Options (Edit)
□ Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

Access features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

☑ Web	1 Bookmarks I Options
☑ Files, Windows	0 Bookmarks I Options
☑ Files, UNIX/NFS	0 Bookmarks I Options
□ Telnet/SSH	0 Sessions I Options
☑ Secure Application Manager	0 Applications I Options
○ Windows version	Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
● Java version	
□ Terminal Services	0 Sessions I Options
□ Virtual Desktops	0 Sessions
□ HTML5 Access	0 Sessions I Options
☑ Meetings	Options
☑ VPN Tunneling	Options (includes IKEv2)
☑ Secure Mail	Options

Save Changes

* Indicates required field

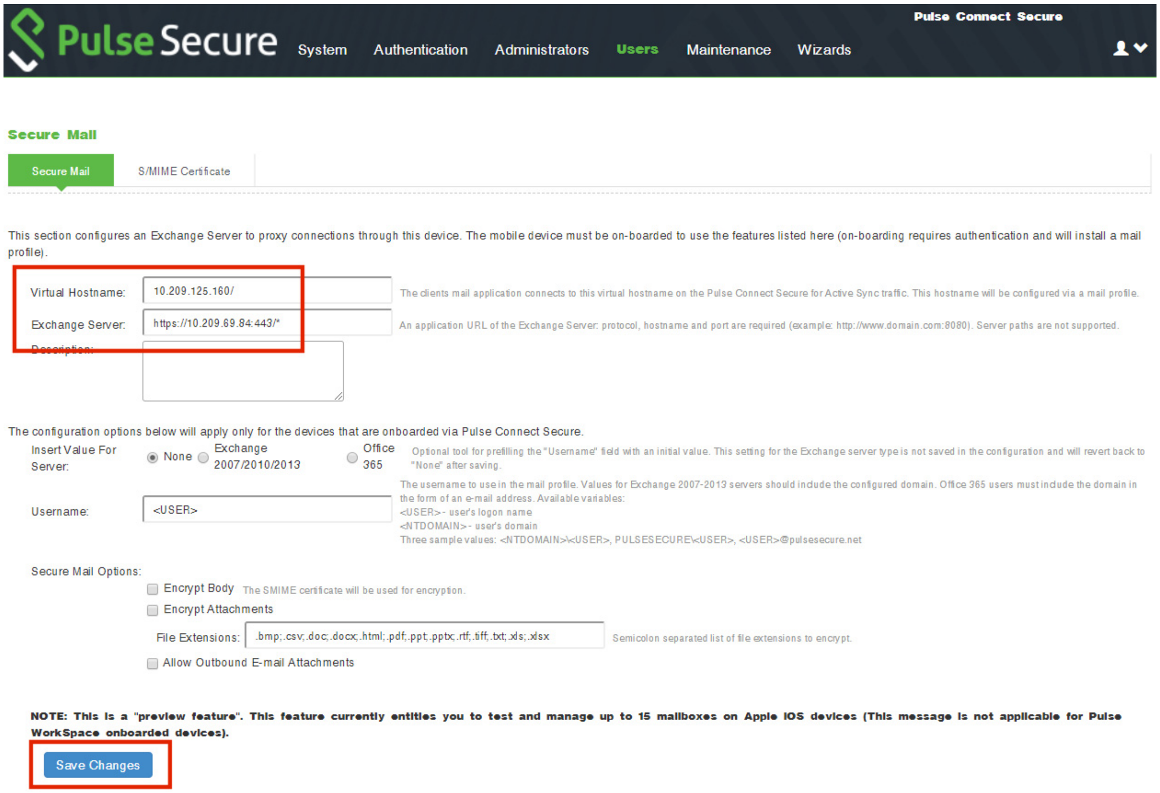
5. Navigate back to the **Access features** for the *secure_email* role and click **Options**.

    The **Secure Mail** page appears.

6. Configure a **Virtual Hostname** which is resolvable on mobile devices.

7. Enter the **Exchange Server** address.

FIGURE 228 Virtual Hostname



Secure Mail

This section configures an Exchange Server to proxy connections through this device. The mobile device must be on-boarded to use the features listed here (on-boarding requires authentication and will install a mail profile).

Virtual Hostname: 10.209.125.160/
The clients mail application connects to this virtual hostname on the Pulse Connect Secure for Active Sync traffic. This hostname will be configured via a mail profile.

Exchange Server: https://10.209.69.84:443/*
An application URL of the Exchange Server: protocol, hostname and port are required (example: http://www.domain.com:8080). Server paths are not supported.

Description:

The configuration options below will apply only for the devices that are onboarded via Pulse Connect Secure.

Insert Value For Server: ● None ○ Exchange 2007/2010/2013 ○ Office 365
Optional tool for prefilling the "Username" field with an initial value. This setting for the Exchange server type is not saved in the configuration and will revert back to "None" after saving.

Username: <USER>
The username to use in the mail profile. Values for Exchange 2007-2013 servers should include the configured domain. Office 365 users must include the domain in the form of an e-mail address. Available variables:
<USER> - user's logon name
<NTDOMAIN> - user's domain
Three sample values: <NTDOMAIN>\<USER>, PULSESECURE\<USER>, <USER>@pulsesecure.net

Secure Mail Options:

□ Encrypt Body The SMIME certificate will be used for encryption.
□ Encrypt Attachments
File Extensions: .bmp;.csv;.doc;.docx;.html;.pdf;.ppt;.pptx;.rtf;.tiff;.txt;.xls;.xlsx Semicolon separated list of file extensions to encrypt.
□ Allow Outbound E-mail Attachments

NOTE: This is a "preview feature". This feature currently entitles you to test and manage up to 15 mailboxes on Apple IOS devices (This message is not applicable for Pulse WorkSpace onboarded devices).

8. Click **Save Changes**.

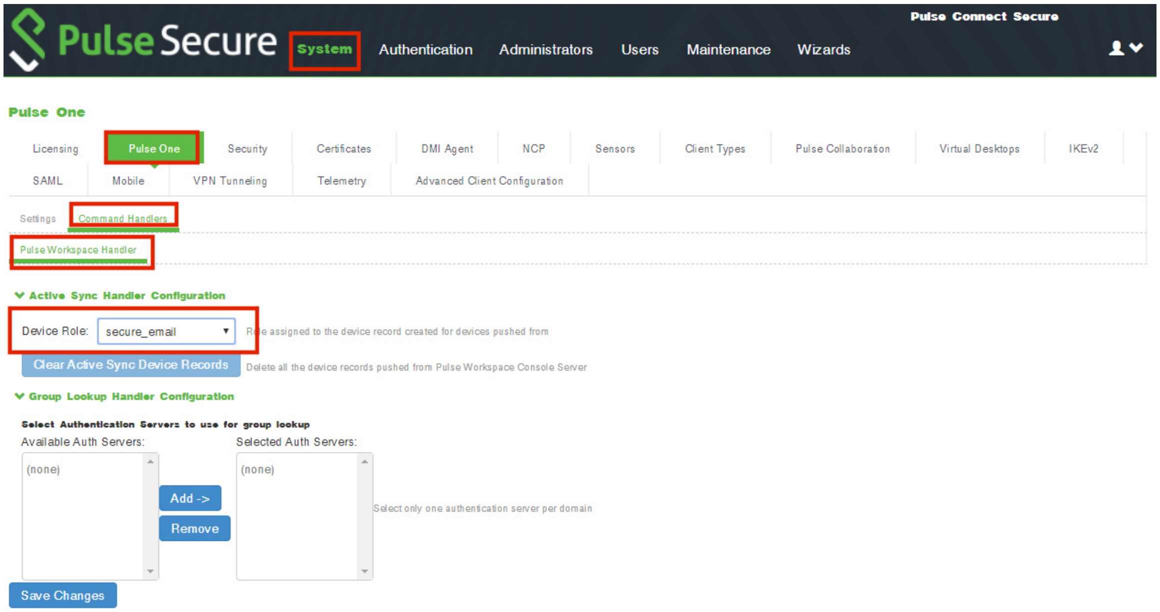
9. Navigate to **System > Configuration > Pulse One > Command Handlers**.

   The **Pulse One** page appears.

10. Select the **Pulse Workspace Handler** tab.

11. For the **Device Role**, select the role configured in previous step. That is, the *secure_email* role.

FIGURE 229 Pulse Workspace Handler



Device Role: secure_email — Role assigned to the device record created for devices pushed from

Clear Active Sync Device Records — Delete all the device records pushed from Pulse Workspace Console Server

Select Authentication Servers to use for group lookup

Available Auth Servers: (none)

Selected Auth Servers: (none)

Select only one authentication server per domain

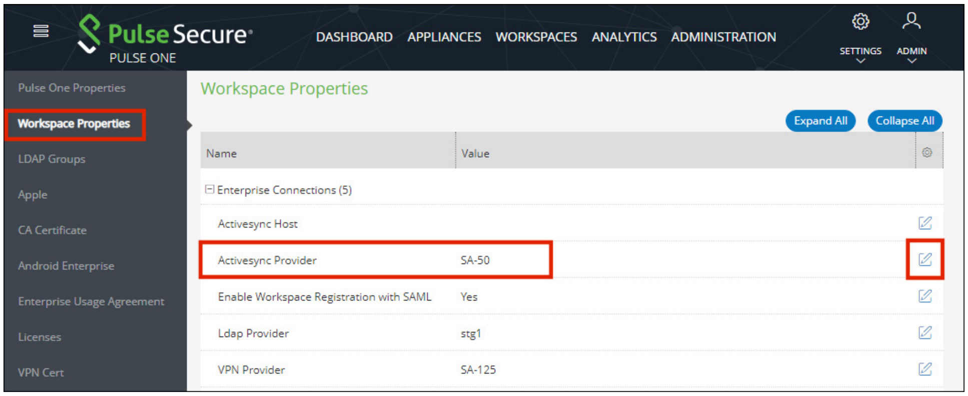
12. Click **Save Changes**.

Configuring the Appliance for ActiveSync

To configure the PCS appliance for ActiveSync:

1. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties.**

FIGURE 230 Workspace Properties



Name	Value
⊟ Enterprise Connections (5)	
Activesync Host	
Activesync Provider	SA-50
Enable Workspace Registration with SAML	Yes
Ldap Provider	stg1
VPN Provider	SA-125

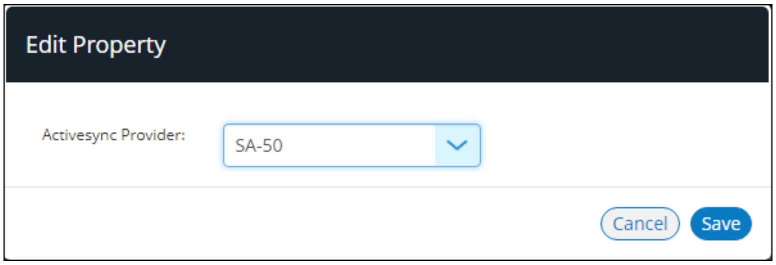
2. The **Activesync Provider** field must be set to the Connect Secure device. This requires ActiveSync configuration in the Pulse Connect Secure server, and for the details refer to the section “ActiveSync Configuration” in the *Pulse Workspace Configuration Guide*.

3. Click the **Edit** (✎) icon.

   The **Edit Property** dialog appears.

4. Modify the **ActiveSync** property of the policy. For example:

FIGURE 231 ActiveSync property



Edit Property

Activesync Provider: SA-50

5. Click **Save**.

Configuring Certificate-Based ActiveSync

This feature enables the delivery of an ActiveSync certificate to mobile devices managed by Pulse Workspace. The device user can then select the ActiveSync certificate on the first use of any supported server/app.

The use of certificate-based ActiveSync is currently supported by the following server:

- *Microsoft Exchange Server 2013*.

  Note: To configure certificate authentication in Exchange Server, see **https://docs.microsoft.com/en-us/Exchange/plan-and-deploy/post-installation-tasks/configure-certificate-based-auth?view=exchserver-2016**.

  Note: This configuration only supports the on-premises Exchange Server, and not the cloud-based *Office365*.

The use of certificate-based ActiveSync is currently supported by the following email clients:

- On Android: *Gmail* and *Nine Work* apps.
- On iOS: the native iOS email app.

Currently, Pulse Workspace supports two delivery mechanisms for ActiveSync certificates:

- Pulse Workspace pushes a SCEP Payload to the onboarded Android and iOS devices. Each device then automatically fetches the ActiveSync certificate from the SCEP Server, see **“Working with ActiveSync Certificates via SCEP” on page 199**.
- Pulse Workspace fetches the ActiveSync certificate from a Windows CAWE server and pushes it to Android and iOS onboarded device, see **“Working with ActiveSync Certificates via Windows CAWE” on page 200**.

Working with ActiveSync Certificates via SCEP

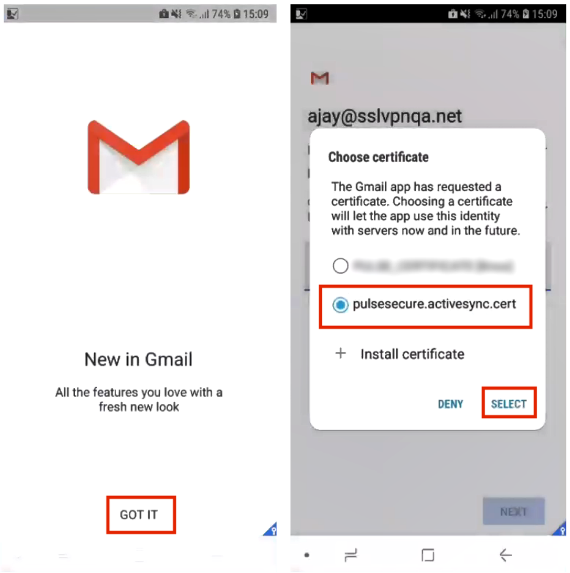
To enable the delivery of an ActiveSync certificate via SCEP:

1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties**.
3. Expand the *ActiveSync* category.
4. If you want SCEP to be used to deliver an ActiveSync certificate to Android devices, set the **Use SCEP to request certificate for Android ActiveSync from external PKI server** workspace property to *True*.
5. If you want SCEP to be used to deliver an ActiveSync certificate to iOS devices, set the **Use SCEP to request certificate for iOS ActiveSync from external PKI server** workspace property to *True*.
6. Select the **Workspaces** menu.
7. Select the **Policies** tab.
8. Select a policy used by devices that require the delivery of an ActiveSync certificate.
9. Click the **Properties** tab for the selected policy.
10. Expand the *Enterprise PKI Integration* category.
11. Set the **Activesync Allow Authentication via Certificate** policy property to *True*.
12. Publish the policy to all devices.

    Each affected device will then receive an SCEP payload, and will then automatically retrieve the required ActiveSync certificate from the SCEP server.

On each device, when a supported app (see **"Configuring Certificate-Based ActiveSync" on page 198**) is first used, the user is asked for an ActiveSync certificate instead of a username and password. The user should select the ActiveSync certificate from the list of available certificates on the device. For example:

FIGURE 232 First Use of Gmail



New in Gmail

All the features you love with a fresh new look

GOT IT

ajay@sslvpnqa.net

Choose certificate

The Gmail app has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

○ [redacted]

● pulsesecure.activesync.cert

+ Install certificate

DENY SELECT

NEXT

Working with ActiveSync Certificates via Windows CAWE

To enable the delivery of an ActiveSync certificate via SCEP:

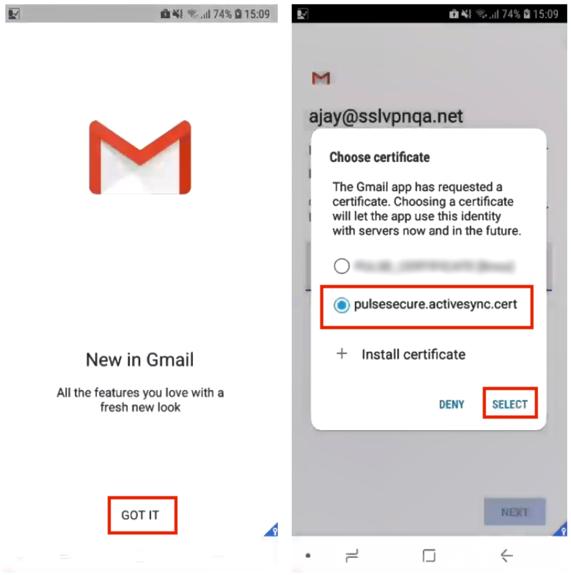
1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties**.
3. Expand the *ActiveSync* category.
4. If you want Windows CAWE to deliver an ActiveSync certificate to Android devices:
    - Set the **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices** to *True*.
    - Set the **Use SCEP to request certificate for Android ActiveSync from external PKI server** workspace property to *False*.
5. If you want Windows CAWE to deliver an ActiveSync certificate to iOS devices:
    - Set the **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices** to *True*.
    - Set the **Use SCEP to request certificate for iOS ActiveSync from external PKI server** workspace property to *False*.

6. Select the **Workspaces** menu.
7. Select the **Policies** tab.
8. Select a policy used by devices that require the delivery of an ActiveSync certificate.
9. Click the **Properties** tab for the selected policy.
10. Expand the *Enterprise PKI Integration* category.
11. Set the **Activesync Allow Authentication via Certificate** policy property to *True*.
12. Publish the policy to all devices.

    An ActiveSync certificate will be delivered by Windows CAWE to each affected device directly.

On each device, when a supported app (see **“Configuring Certificate-Based ActiveSync” on page 198**) is first used, the user is asked for an ActiveSync certificate instead of a username and password. The user should select the ActiveSync certificate from the list of available certificates on the device. For example:

FIGURE 233 First Use of Gmail



New in Gmail

All the features you love with a fresh new look

ajay@sslvpnqa.net

Choose certificate

The Gmail app has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

● pulsesecure.activesync.cert

Configuring Jail Break Compliance Detection

This section describes iOS compliance and jailbreak detection in Pulse Workspace.

- **"Overview of Jailbroken Devices" on page 202**.
- **"Configuring Certificate-Based Authentication" on page 203**.
- **"Configuring User Roles" on page 205**.
- **"Configuring Realm and Role Mapping Rules" on page 206**.
- **"Configuring the Sign-In Policy" on page 209**.
- **"Configuring the Compliance Property" on page 210**.

Overview of Jailbroken Devices

Jailbreaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system, and therefore bypass usage and access limitations imposed by Apple.

With a jailbroken device, an iOS user can install applications that are not available through the Apple App Store.

Jailbroken devices possess a greater risk of running malicious applications.

Support for jailbroken devices in Pulse Workspace addresses the following questions:

- How can an enterprise track network access by non-company-issued (BYOD) devices?
- Can an enterprise implement a policy that will restrict the mobile devices that access the network and protected resources, in the same way that SSL VPN solutions restrict user access?

Pulse Workspace addresses these issues with the Workspace data records, which can be used in the access management framework to enforce security policies.

After the device has been registered with the Workspace, the Pulse Secure client checks for the compliance of the device. If it identifies the device as non-compliant, it updates the status in the Workspace server. Based on the policy defined on the **Jail Break Detection** compliance property, it takes the action and report the status of the device as non-compliant. When the Jailbroken device attempts to connect the VPN, the PCS gateway checks for certain device attributes before allowing the access to the network.

PCS makes the Compliance status API calls to the Pulse Workspace server to make sure that the device meets the compliance requirements established by the Workspace. If the device is not compliant with the MDM, PCS restricts the VPN access to the device.

Note: Jailbreaking is one or many compliance considerations evaluated by Pulse Workspace, see **"Compliance" on page 178**.

Note: This works only for certificate-based authentication on Pulse Connect Secure v8.2R3 or later.

Configuring Certificate-Based Authentication

This section describes the process of configuring the MDM server and certificate server.

- "Configuring the MDM Authentication Server" on page 203.
- "Configuring the Certificate Server" on page 204.

Configuring the MDM Authentication Server

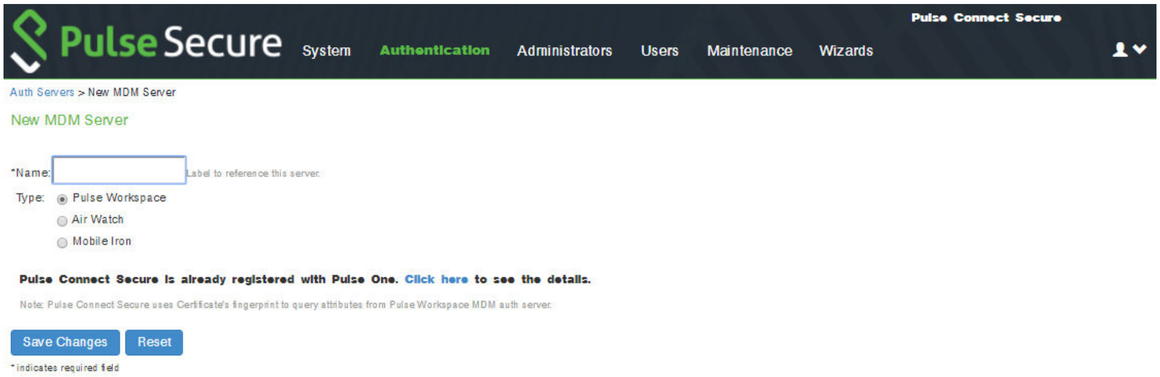
The MDM authentication server configuration is used by the system to communicate with the MDM. In the device access management framework, the MDM server is used as the device authorization server.

To configure the authentication server:

1. Select **Authentication > Auth. Servers** to navigate to the **Authentication Servers** page.
2. Under **New**, select *MDM Server* and click **New Server**.

   The **New MDM Server** page appears.

   FIGURE 234 Configure MDM Server



Auth Servers > New MDM Server

New MDM Server

*Name: Label to reference this server.

Type: ● Pulse Workspace
○ Air Watch
○ Mobile Iron

Pulse Connect Secure is already registered with Pulse One. Click here to see the details.

Note: Pulse Connect Secure uses Certificate's fingerprint to query attributes from Pulse Workspace MDM auth server.

*indicates required field

3. Enter a **Name** for the MDM server.
4. Click **Pulse Workspace**.
5. Click **Save Changes**.

Configuring the Certificate Server

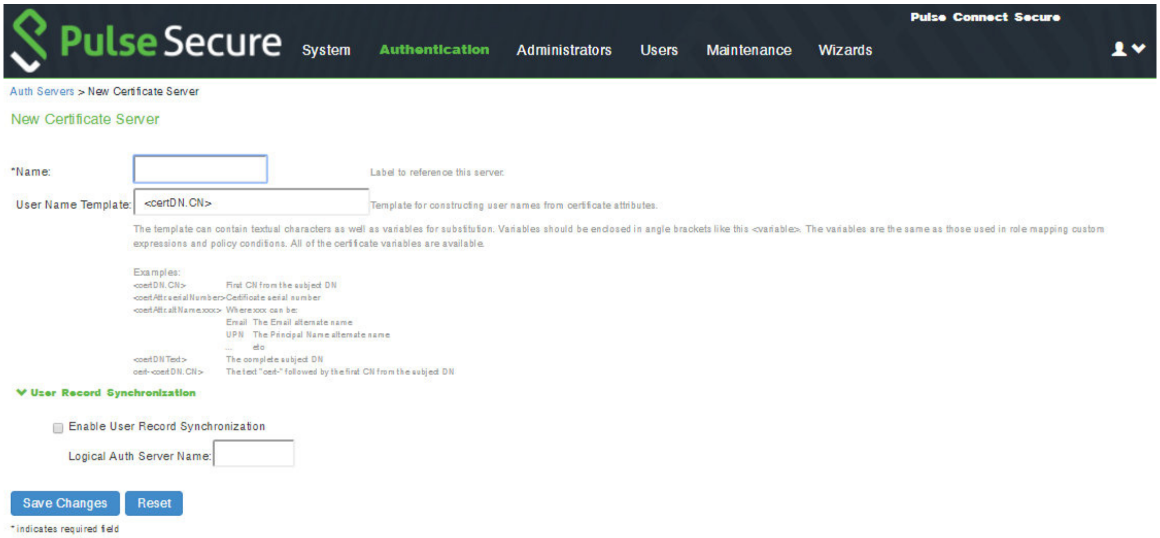
The certificate server configuration enables device users to authenticate using the certificate pushed to the device by the MDM. The certificates are used for user authentication, and the users do not have to enter user credentials.

To configure the certificate server:

1. Select **Authentication > Auth. Servers** to navigate to the **Authentication Servers** page.
2. Under **New**, select *Certificate Server* and click **New Server**.

   The **New Certificate Server** page appears.

   FIGURE 235 Configure Certificate Server



Auth Servers > New Certificate Server

New Certificate Server

*Name: Label to reference this server.

User Name Template: <certDN.CN> Template for constructing user names from certificate attributes.

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. The variables are the same as those used in role mapping custom expressions and policy conditions. All of the certificate variables are available.

```
Examples:
<certDN.CN>             First CN from the subject DN
<certAttr.serialNumber>Certificate serial number
<certAttr.altName.xxx>  Where xxx can be:
                        Email  The Email alternate name
                        UPN    The Principal Name alternate name
                        ...    etc
<certDNText>            The complete subject DN
cert-<certDN.CN>        The text "cert-" followed by the first CN from the subject DN
```

User Record Synchronization

□ Enable User Record Synchronization

Logical Auth Server Name:

Save Changes Reset

*indicates required field

3. Enter a certificate authentication **Name**.
4. Click **Save Changes**.

Configuring User Roles

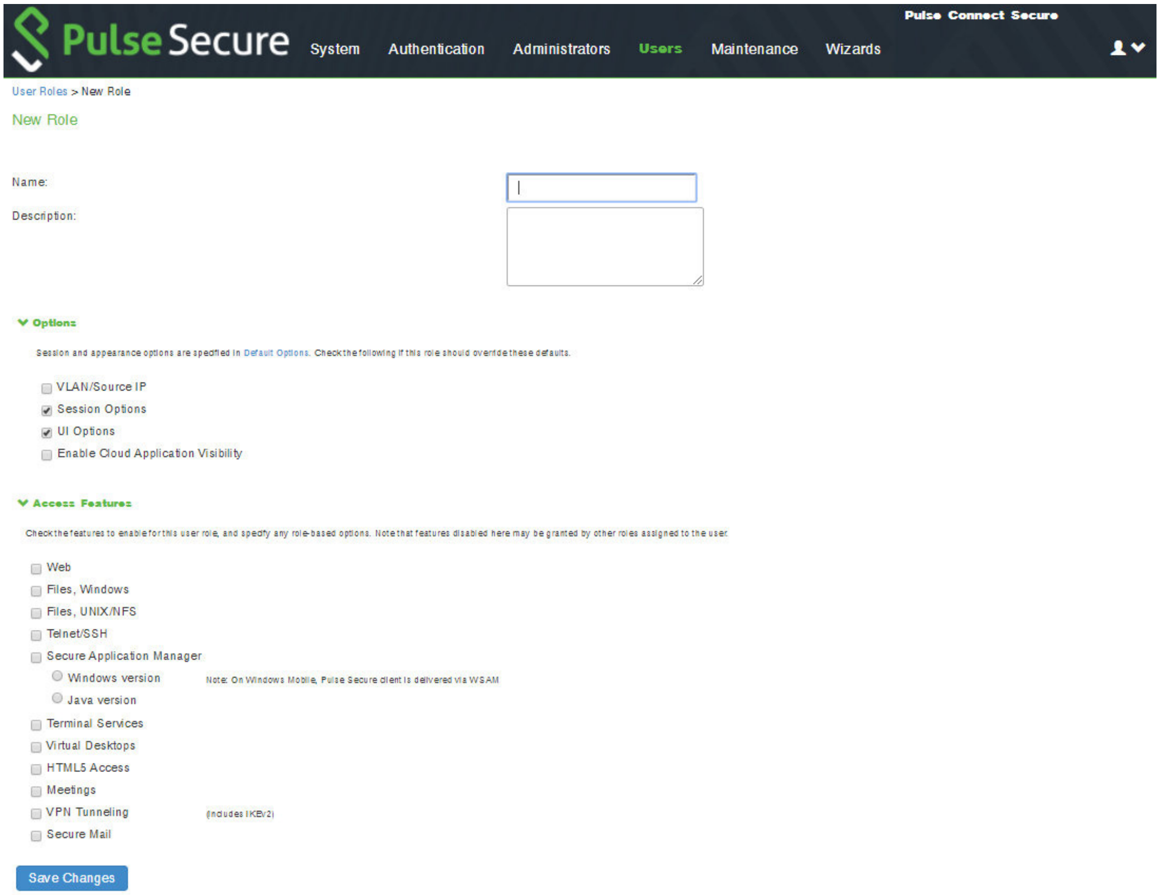
User roles are classifiers for network access control policies. You create a set of roles to use in your classification scheme whether, for example:

- The device status is MDM enrollment complete or incomplete.
- The device status is MDM-policy compliant or non-compliant.
- The device is employee owned or company owned.
- The device platform is iOS, Android, or neither.

To configure user roles:

1. Select **Users > User Roles** to navigate to the **User Roles** page.
2. Click **New Role** to display the **New Role** page.

FIGURE 236 New Role



New Role

Name:

Description:

Options

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

□ VLAN/Source IP
☑ Session Options
☑ UI Options
□ Enable Cloud Application Visibility

Access Features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

□ Web
□ Files, Windows
□ Files, UNIX/NFS
□ Telnet/SSH
□ Secure Application Manager
○ Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
○ Java version
□ Terminal Services
□ Virtual Desktops
□ HTML5 Access
□ Meetings
□ VPN Tunneling (includes IKEv2)
□ Secure Mail

3. Provide **Name**, **Description** (optional), **Options**, and **Access Features**.
4. Click **Save Changes**.

Note: You can also use system-created user roles.

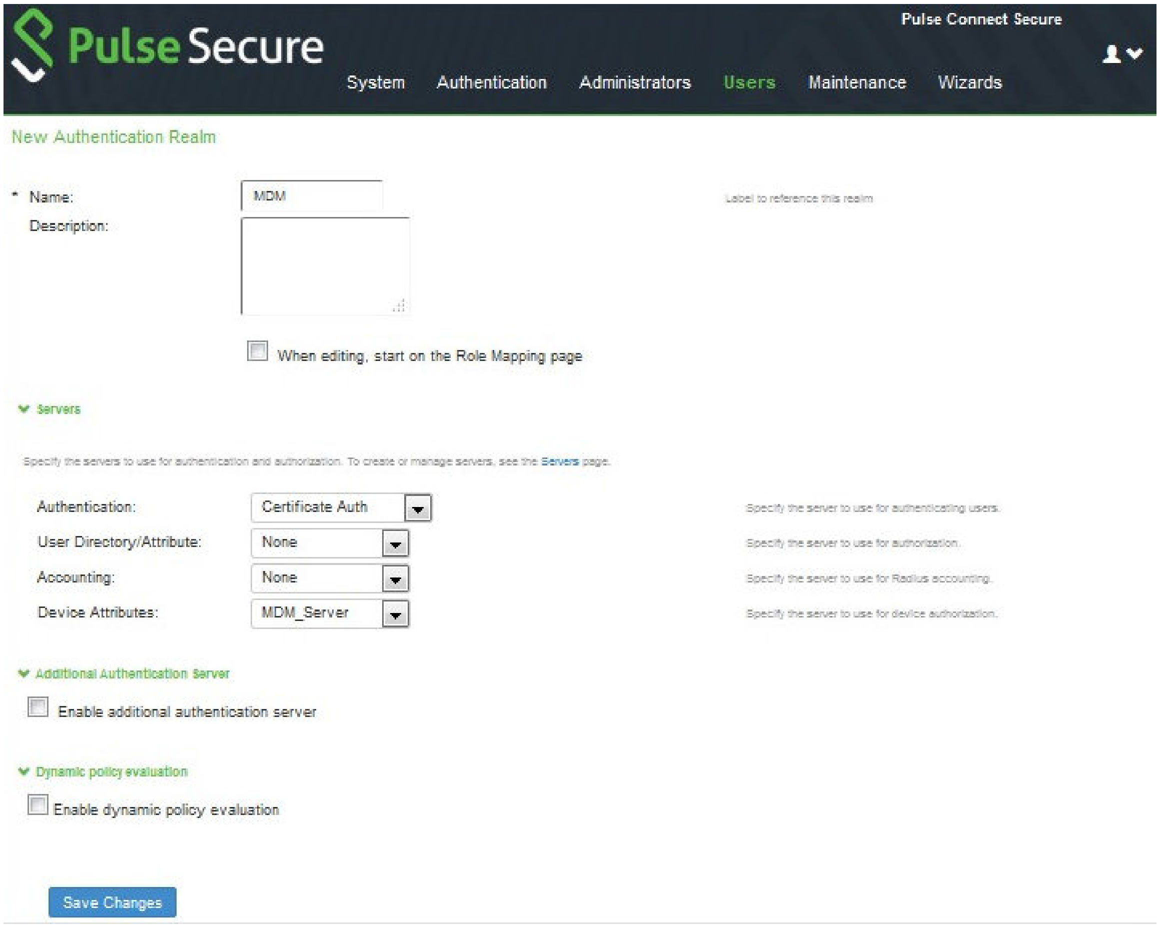
Configuring Realm and Role Mapping Rules

The user realm configuration associates the authentication server data and MDM server data with user roles.

To configure the realm and role mapping rules:

1. Select **Users > User Realms** to navigate to the **User Authentication Realms** page.
2. Click **New Realm** to display the **New Authentication Realm** page.

FIGURE 237 Configure Realm and Role Mapping Rules



New Authentication Realm

* Name: MDM — Label to reference this realm

Description:

□ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication: Certificate Auth — Specify the server to use for authenticating users.

User Directory/Attribute: None — Specify the server to use for authorization.

Accounting: None — Specify the server to use for Radius accounting.

Device Attributes: MDM_Server — Specify the server to use for device authorization.

Additional Authentication Server

□ Enable additional authentication server

Dynamic policy evaluation

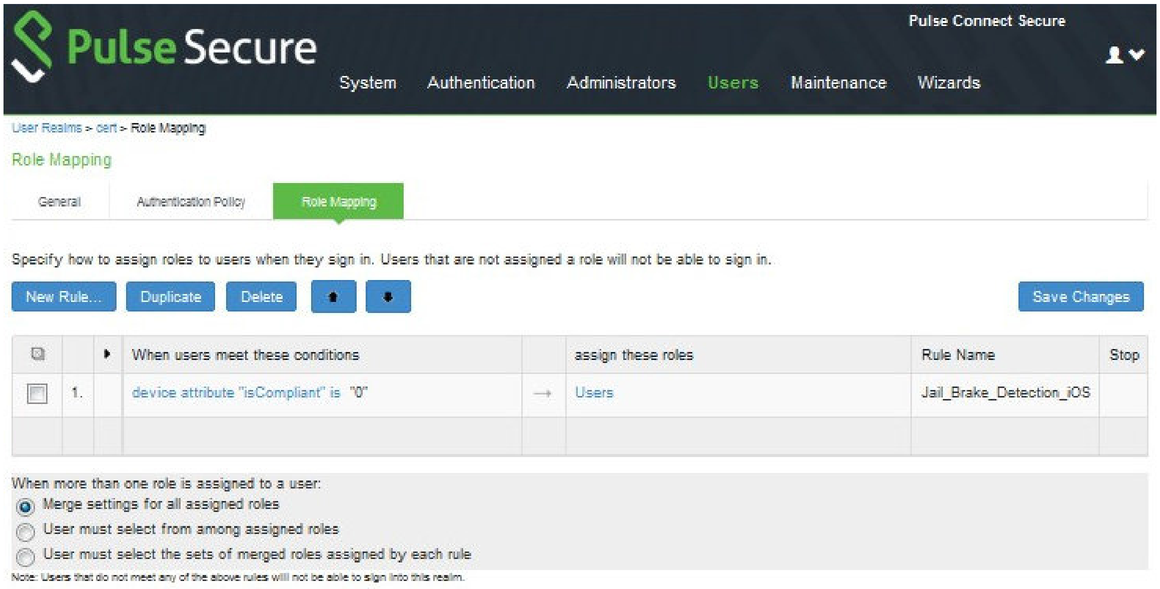
□ Enable dynamic policy evaluation

3. Provide the following properties for the new authentication realm:
   - **Name**, and an optional **Description**.
   - For **Authentication**, select *Certificate Auth*.
   - For **Device Attributes**, select *MDM Server*.

4. Click **Save Changes**.

   The **Role Mapping** page appears.

   FIGURE 238 Create New Rule



Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

□		▸	When users meet these conditions		assign these roles	Rule Name	Stop
□	1.		device attribute "isCompliant" is "0"	→	Users	Jail_Brake_Detection_iOS	

When more than one role is assigned to a user:

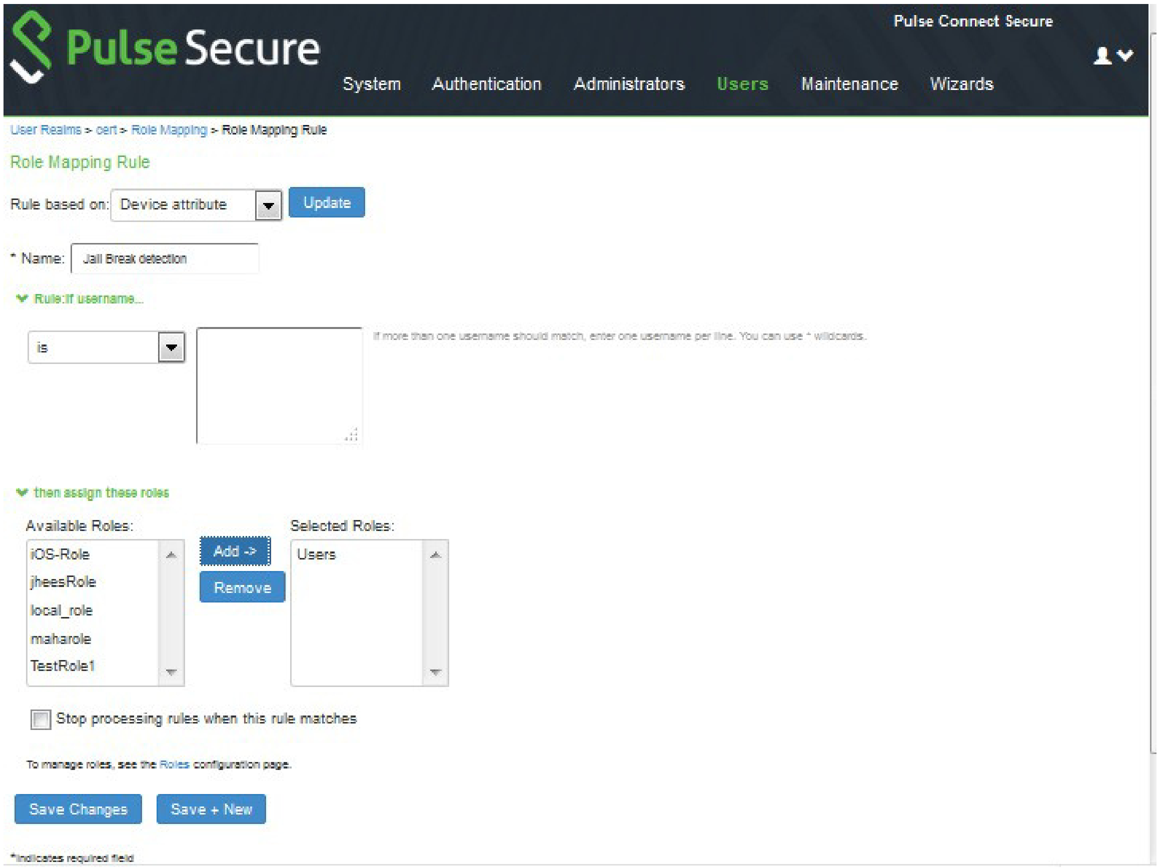
● Merge settings for all assigned roles
○ User must select from among assigned roles
○ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

5. Select the **Role Mapping** tab and click **New Rule**.

The **Role Mapping Rule** page appears.

FIGURE 239 Role Mapping Rule



User Realms > cert > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: Device attribute

* Name: Jail Break detection

Rule:If username...

is

If more than one username should match, enter one username per line. You can use * wildcards.

then assign these roles

Available Roles: iOS-Role, jheesRole, local_role, maharole, TestRole1

Selected Roles: Users

□ Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

*indicates required field

6. For the **Rule based on** drop-down list, select *Device attribute*.
7. Click **Update**.
8. Provide a **Name** for the role.
9. Set the **isCompliant** attribute to *is*, and provide a value of *0* or *1* depending on the requirement.
10. Assign the required roles using **Add** and **Remove**.
11. Click **Save Changes**.

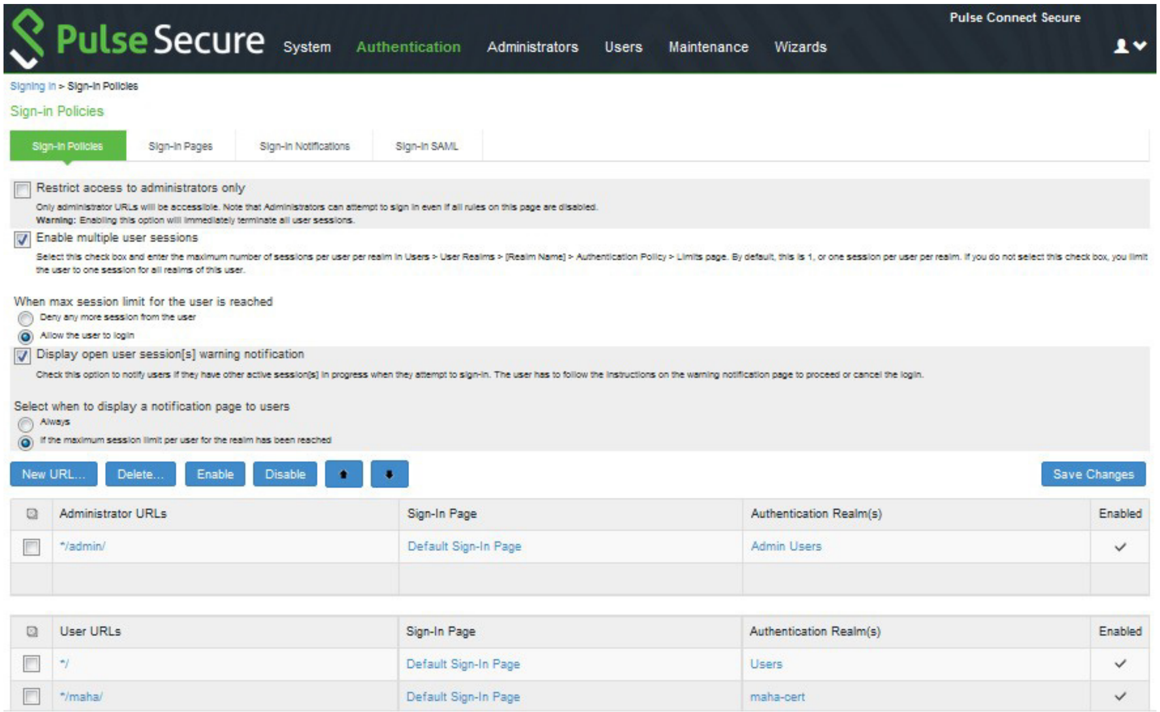
Configuring the Sign-In Policy

A sign-in policy associates devices with a realm.

To configure a sign-in policy:

1. Select **Authentication > Signing In > Sign-In Policies** to navigate to the **Sign-In Policies** page.

   FIGURE 240 Sign-In Policies



□ Restrict access to administrators only

Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

☑ Enable multiple user sessions

Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or one session per user per realm. If you do not select this check box, you limit the user to one session for all realms of this user.

When max session limit for the user is reached

○ Deny any more session from the user
● Allow the user to login

☑ Display open user session[s] warning notification

Check this option to notify users if they have other active session[s] in progress when they attempt to sign-in. The user has to follow the instructions on the warning notification page to proceed or cancel the login.

Select when to display a notification page to users

○ Always
● If the maximum session limit per user for the realm has been reached

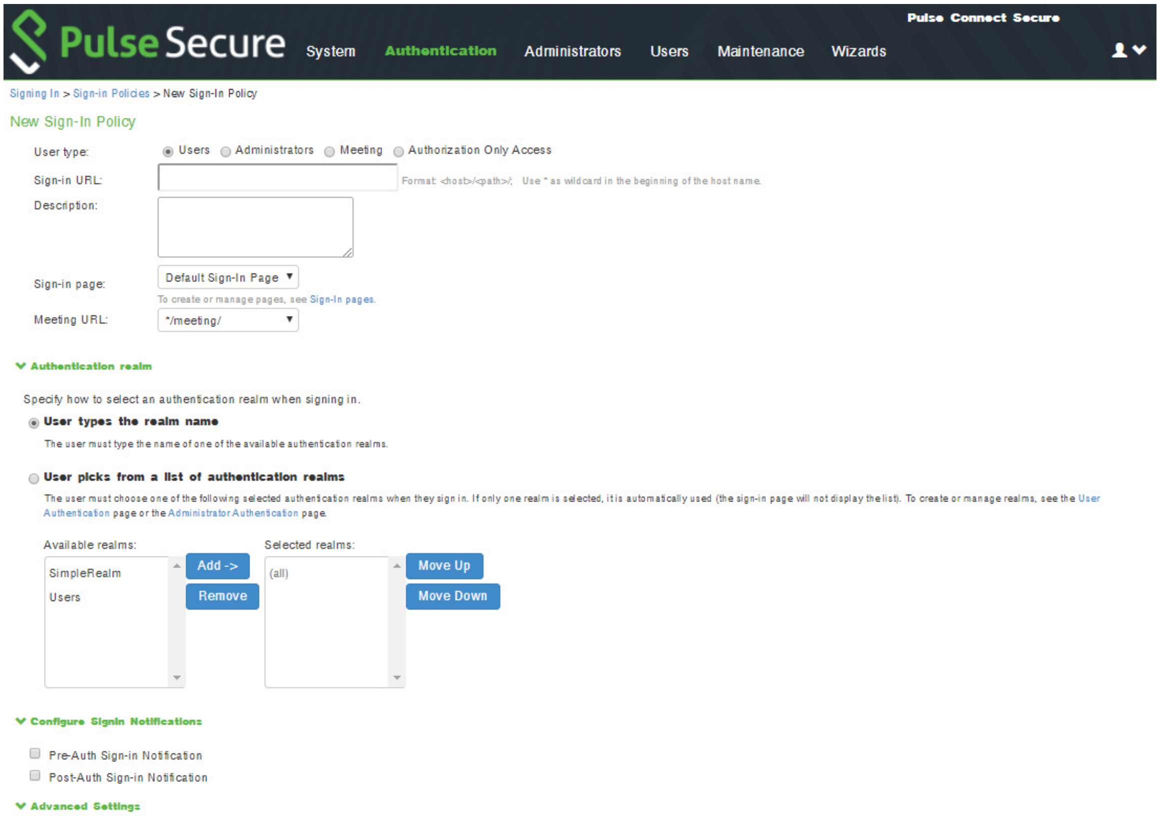
□	Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
□	*/admin/	Default Sign-In Page	Admin Users	✓

□	User URLs	Sign-In Page	Authentication Realm(s)	Enabled
□	*/	Default Sign-In Page	Users	✓
□	*/maha/	Default Sign-In Page	maha-cert	✓

2. Click **New URL**..

The **New Sign-In Policy** page appears.

FIGURE 241 New Sign-In Policy



New Sign-In Policy

User type: ● Users ○ Administrators ○ Meeting ○ Authorization Only Access

Sign-in URL: Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: Default Sign-In Page

To create or manage pages, see Sign-In pages.

Meeting URL: */meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

● User types the realm name

The user must type the name of one of the available authentication realms.

○ User picks from a list of authentication realms

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the User Authentication page or the Administrator Authentication page.

Available realms: SimpleRealm, Users

Selected realms: (all)

Configure SignIn Notifications

□ Pre-Auth Sign-in Notification

□ Post-Auth Sign-in Notification

Advanced Settings

3. Specify a **Sign-in URL**, and (optionally) a **Description**.
4. In **Authentication Realms**, use **Add** and **Remove** to populate the **Selected realms** list.
5. Click **Save Changes**.

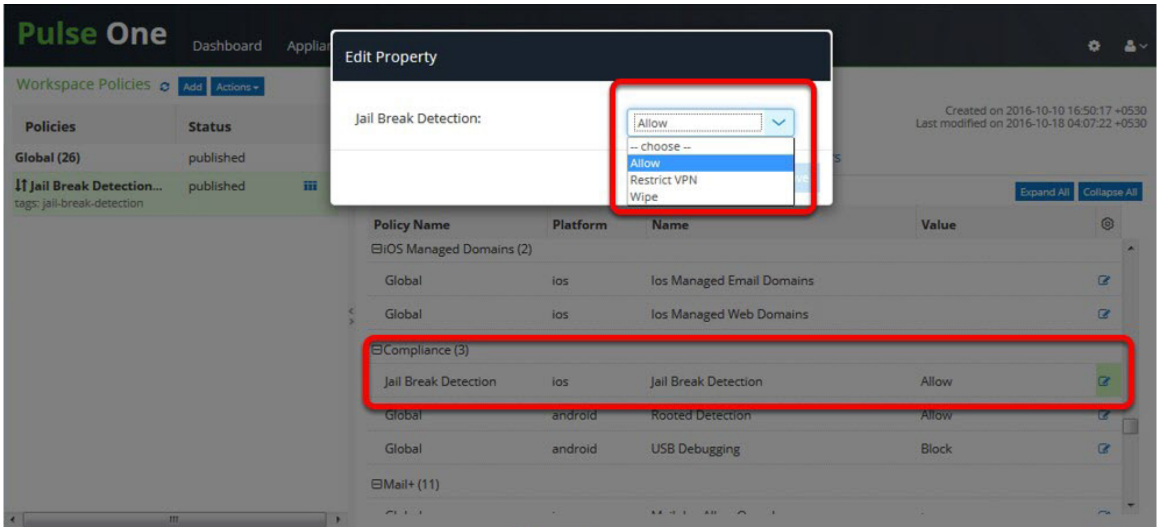
Configuring the Compliance Property

To configure compliance property on Pulse Workspace:

1. Add a new user workspace.
2. Add a policy and a tag to the newly created user workspace.

3. Configure the **Jail Break Detection** iOS policy property.

FIGURE 242 Jail Break Detection Policy Property



Edit Property

Jail Break Detection: Allow

Created on 2016-10-10 16:50:17 +0530
Last modified on 2016-10-18 04:07:22 +0530

Policies	Status
Global (26)	published
Jail Break Detection... tags: jail-break-detection	published

Policy Name	Platform	Name	Value
⊟iOS Managed Domains (2)			
Global	ios	Ios Managed Email Domains	
Global	ios	Ios Managed Web Domains	
⊟Compliance (3)			
Jail Break Detection	ios	Jail Break Detection	Allow
Global	android	Rooted Detection	Allow
Global	android	USB Debugging	Block
⊟Mail+ (11)			

4. Select compliance based on your requirement - *Allow*, *Restrict VPN*, or *Wipe*.

5. Configure the VPN profile for the policy. For example: *https://<ipaddress>/certificate*.

6. Provision the iOS device that is jail broken, and ensure that the VPN profile get pushed. The action selected in the jail break iOS policy property is performed.

Configuring Enterprise WiFi

Enterprise IT administrators can create and manage WiFi profiles, which allows users with Android and iOS devices to connect to corporate networks.

For a list of Enterprise WiFi protocols that are supported, see the WiFi parameter table in Configuring Pulse Workspace Policy Properties.

The WiFi configuration includes:

- “Configuring Enterprise WiFi on Pulse Policy Secure” on page 212.
- “Configuring Enterprise WiFi Policy Properties” on page 216.

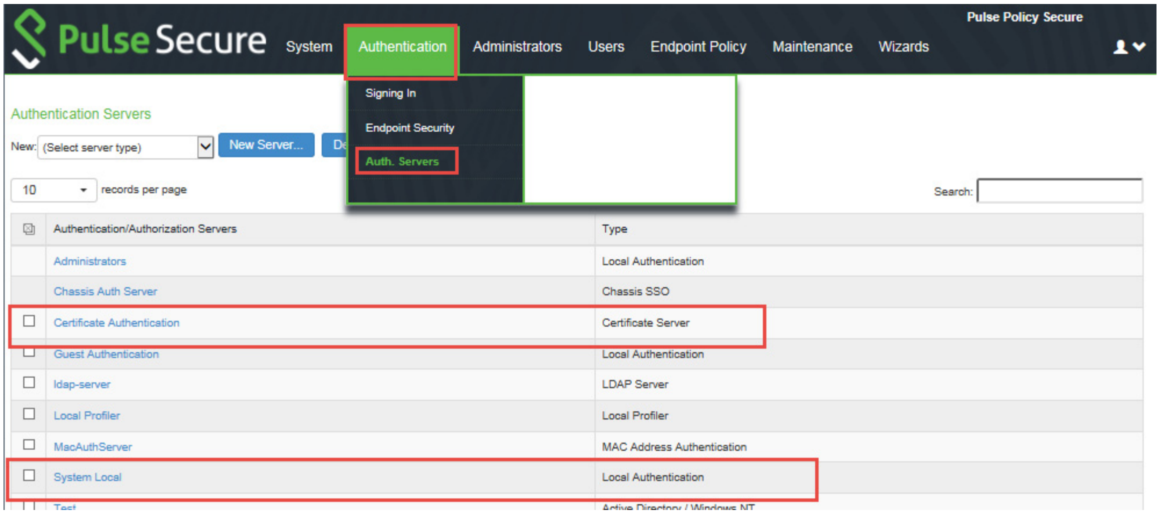
Configuring Enterprise WiFi on Pulse Policy Secure

Note: Before configuring WiFi protocol support in Pulse Policy Secure, ensure that router used is with WLC capabilities.

To configure WiFi protocol support in Pulse Policy Secure:

1. Log in to the Pulse Policy Secure server.
2. Select **Authentication > Auth. Servers**.

FIGURE 243 Authentication Servers

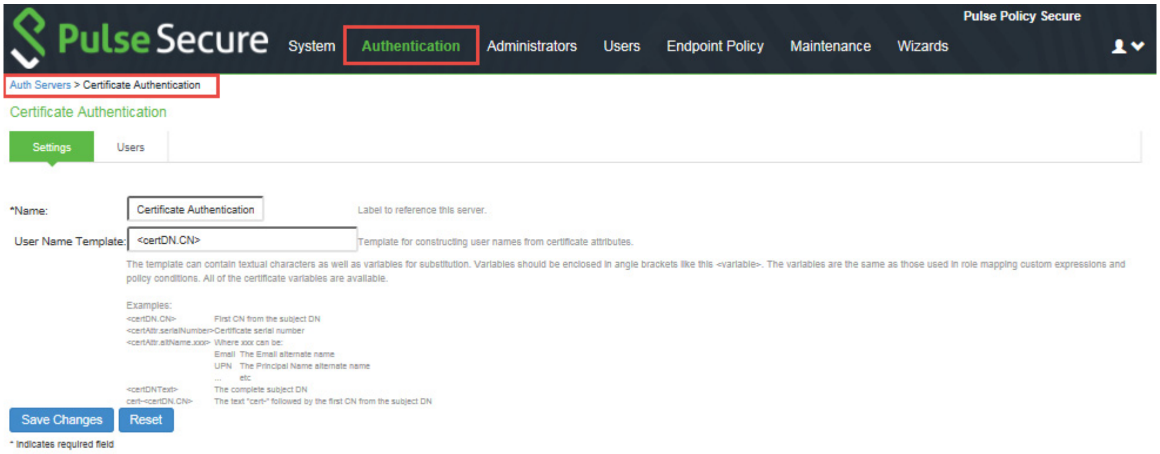


	Authentication/Authorization Servers	Type
	Administrators	Local Authentication
	Chassis Auth Server	Chassis SSO
□	Certificate Authentication	Certificate Server
□	Guest Authentication	Local Authentication
□	ldap-server	LDAP Server
□	Local Profiler	Local Profiler
□	MacAuthServer	MAC Address Authentication
□	System Local	Local Authentication
□	Test	Active Directory / Windows NT

3. Create a new authentication server.

4. (Optional) Click the **Certificate Authentication** hyperlink if your preferred protocol type is EAP-TLS.

FIGURE 244 Certificate Authentication Server



Auth Servers > Certificate Authentication

Certificate Authentication

*Name: Certificate Authentication — Label to reference this server.

User Name Template: <certDN.CN> — Template for constructing user names from certificate attributes.

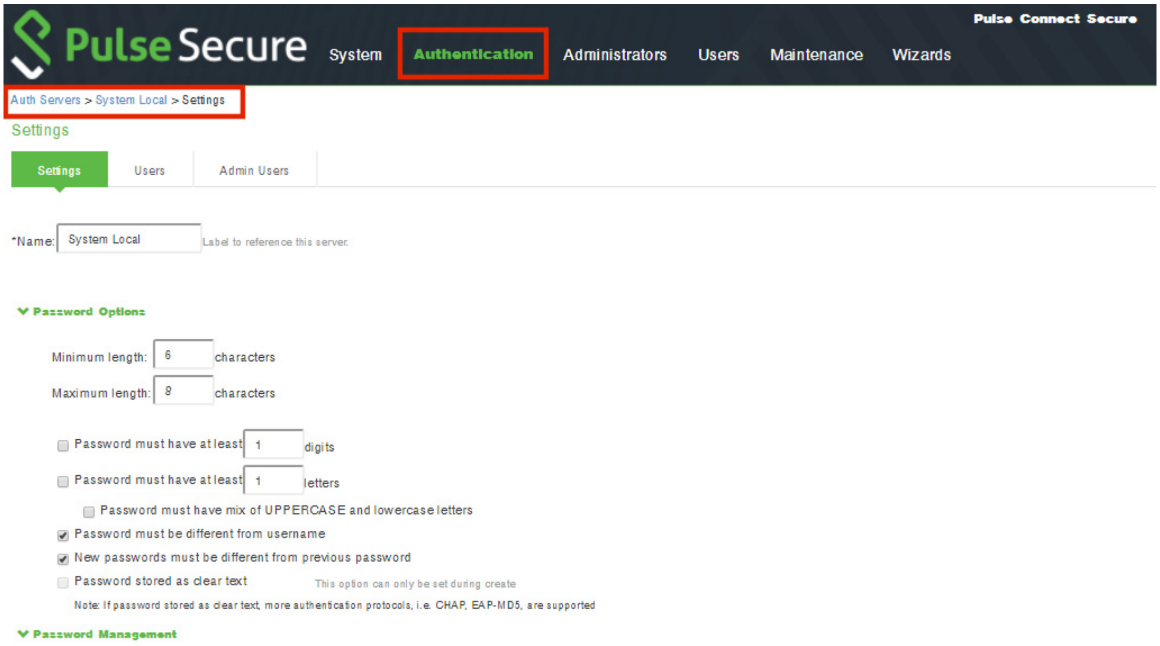
The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. The variables are the same as those used in role mapping custom expressions and policy conditions. All of the certificate variables are available.

```
Examples:
<certDN.CN>              First CN from the subject DN
<certAttr.serialNumber>Certificate serial number
<certAttr.altName.xxx>   Where xxx can be:
                         Email  The Email alternate name
                         UPN    The Principal Name alternate name
                         ...    etc
<certDNText>             The complete subject DN
cert-<certDN.CN>         The text "cert-" followed by the first CN from the subject DN
```

* indicates required field

5. (Optional) Click the **System Local** hyperlink if your preferred protocol type is EAP-TTLS / EAP-PEAP.

FIGURE 245 System Local Settings



Auth Servers > System Local > Settings

Settings

*Name: System Local — Label to reference this server.

Password Options

Minimum length: 6 characters

Maximum length: 8 characters

□ Password must have at least 1 digits

□ Password must have at least 1 letters

□ Password must have mix of UPPERCASE and lowercase letters

☑ Password must be different from username

☑ New passwords must be different from previous password

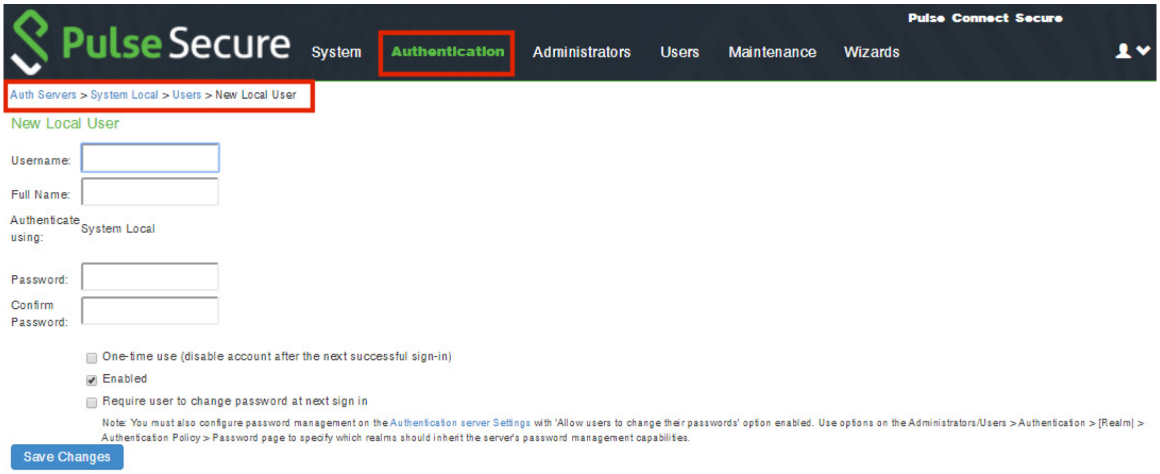
□ Password stored as clear text — This option can only be set during create

Note: If password stored as clear text, more authentication protocols, i.e. CHAP, EAP-MD5, are supported

Password Management

6. Create a new user.

FIGURE 246 Create User



Auth Servers > System Local > Users > New Local User

New Local User

Username:	
Full Name:	
Authenticate using:	System Local
Password:	
Confirm Password:	

□ One-time use (disable account after the next successful sign-in)

☑ Enabled

□ Require user to change password at next sign in

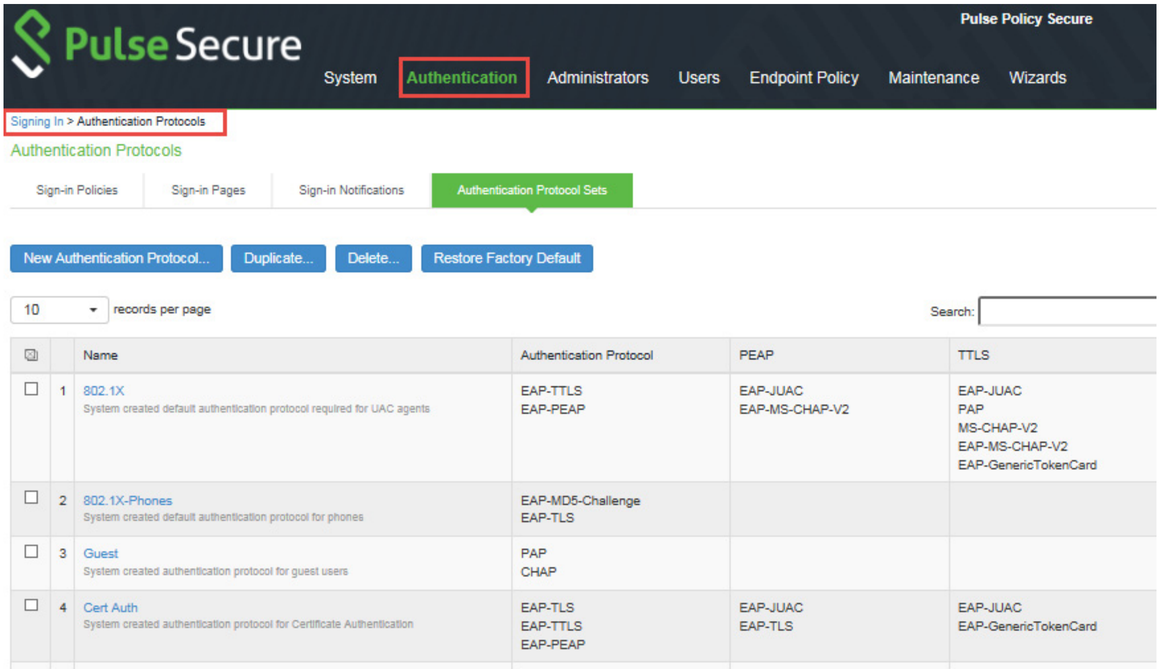
Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

Save Changes

7. Select **Authentication > Signing In > Authentication Protocol Sets**.

8. Select the protocols to enable on PPS.

FIGURE 247 Authentication Protocol Sets



Signing In > Authentication Protocols

Authentication Protocols

10 records per page Search:

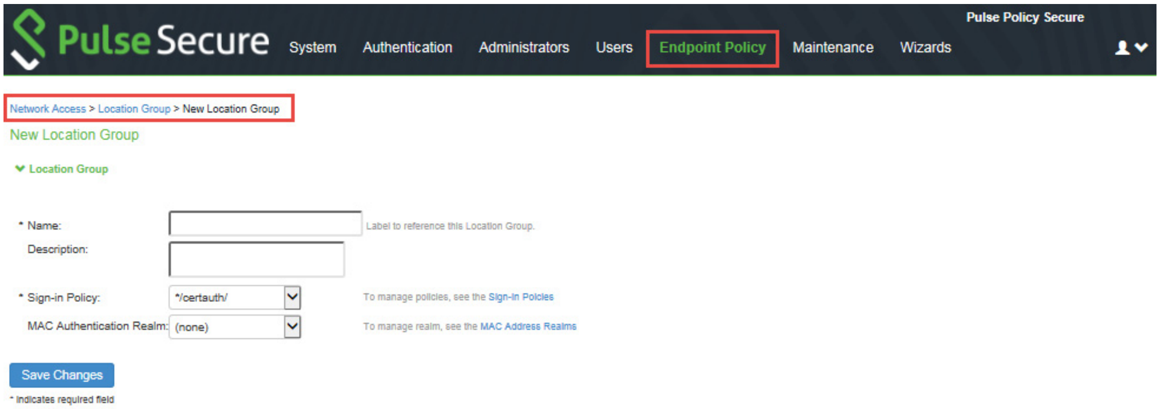
□		Name	Authentication Protocol	PEAP	TTLS
□	1	802.1X System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard
□	2	802.1X-Phones System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS		
□	3	Guest System created authentication protocol for guest users	PAP CHAP		
□	4	Cert Auth System created authentication protocol for Certificate Authentication	EAP-TLS EAP-TTLS EAP-PEAP	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard

9. Configure the RADIUS Client for authentication.

10. Go to **Endpoint Policy > Network Access - Location Group**.

11. Click **New Location Group** and provide the location group **Name**, **Sign In Policy** and **MAC Authentication Realm** details.

FIGURE 248 New Location Group



Network Access > Location Group > New Location Group

New Location Group

Location Group

* Name: Label to reference this Location Group.

Description:

* Sign-in Policy: */certauth/ To manage policies, see the Sign-in Policies

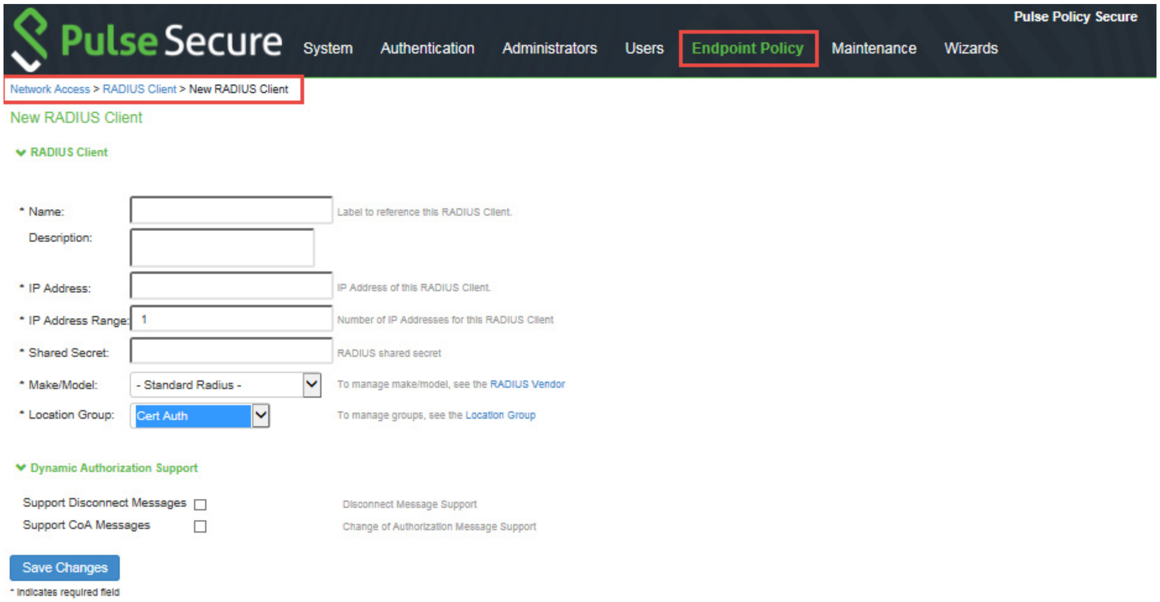
MAC Authentication Realm: (none) To manage realm, see the MAC Address Realms

* Indicates required field

12. Go to **Endpoint Policy > Network Access > RADIUS Client**.

13. Click **New RADIUS Client** and fill in the RADIUS client properties.

FIGURE 249 New RADIUS Client



Network Access > RADIUS Client > New RADIUS Client

New RADIUS Client

RADIUS Client

* Name: Label to reference this RADIUS Client.

Description:

* IP Address: IP Address of this RADIUS Client.

* IP Address Range: 1 Number of IP Addresses for this RADIUS Client

* Shared Secret: RADIUS shared secret

* Make/Model: - Standard Radius - To manage make/model, see the RADIUS Vendor

* Location Group: Cert Auth To manage groups, see the Location Group

Dynamic Authorization Support

Support Disconnect Messages □ Disconnect Message Support

Support CoA Messages □ Change of Authorization Message Support

* Indicates required field

Configuring Enterprise WiFi Policy Properties

To configure Pulse Workspace policy properties:

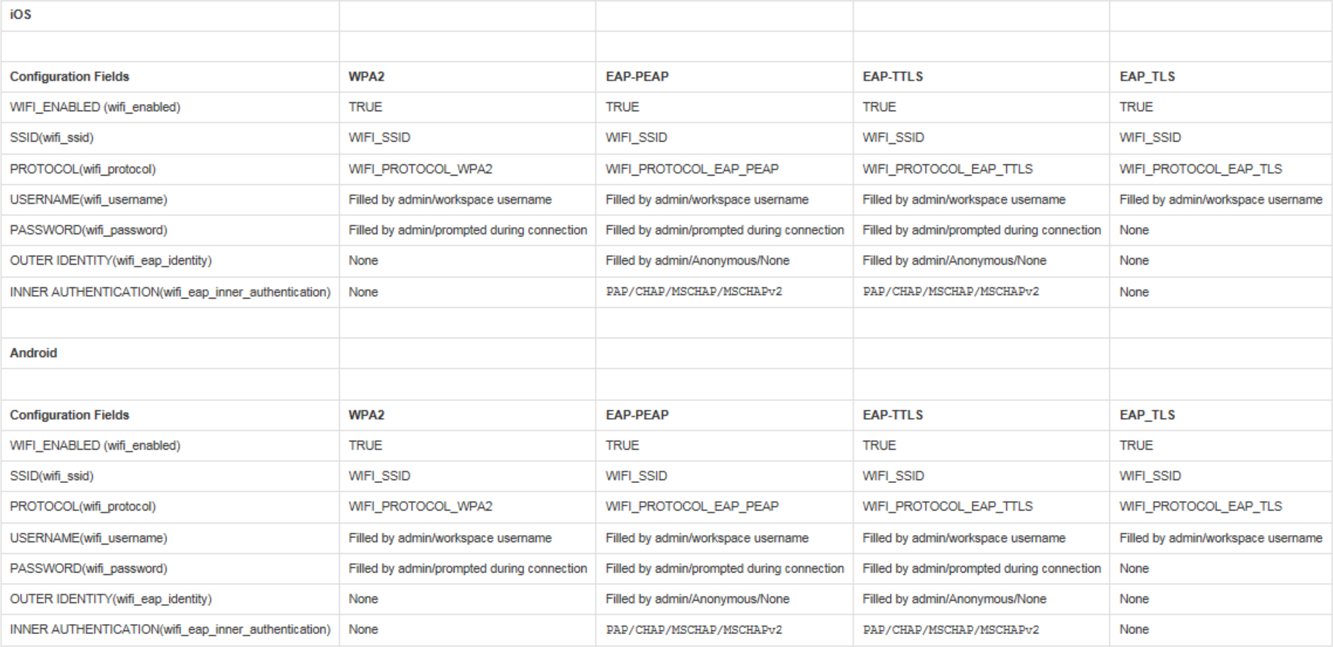
1. Log in to Pulse One admin console.
2. Select the **Workspaces** menu, and then select **Policies**.
3. Create a new policy.
4. Select the policy from the list. In the details pane, select the **Properties** tab and choose appropriate values for the following WiFi parameters. For details about the WiFi parameters, see the table of WiFi parameters below.
5. **Enterprise Wifi Inner Authentication** – Select the protocol that will be used to authenticate the username and password (*None*, *PAP*, *CHAP*, *MSCHAP*, or *MSCHAPv2*). The *None* option is valid only for Android devices.
    - **Wifi Protocol** - If you are using WiFi inner authentication, select *WPA2-Enterprise-EAP-TTLS* / *WPA2-Enterprise-EAP-PEAP* protocol.
6. Save and publish the policy.
7. Connect using SSID that is mentioned in WiFi policy on the device.

Note: For Android devices, before connecting using SSID, manually set the password for using EAP-TTLS / EAP-PEAP protocols.

WiFi Parameter	Description
Enterprise Wifi Inner Authentication	Select the protocol that will be used to authenticate the username and password (*None*, *PAP*, *CHAP*, *MSCHAP*, or *MSCHAPv2*). The *None* option is valid only for Android devices.
Enterprise Wifi Outer Identity	Specify an alternate username to be used outside the encrypted tunnel, such as anonymous, to conceal the user's identity in unencrypted packets.
Wifi Enabled	If enabled, sets the device to automatically join the network.
Wifi Password	Filled by admin / prompted during connection.
Wifi Protocol	Select the type of authentication used by the network, and specify the password or enterprise settings, as required: • **WEP:** Wired Equivalent Privacy used for a non-enterprise network. Enter the network shared key in the displayed text box. • **WPA2:** WiFi Protected Access used for a non- enterprise network. Select the encryption method (AES or TKIP) and enter the network shared key in the displayed text box (applies to Windows clients only). • **WPA2-Enterprise:** WiFi Protected Access used for an enterprise network. Select the Extensible Authentication Protocols (EAP) supported by the network's RADIUS authentication server. Workspace adds support for *EAP-TLS*, *EAP-TTLS*, *EAP-PEAP*.

WiFi Parameter	Description
Wifi SSID	Enter the password that is required to join the WiFi network if the network password is static. Select the **Show Characters** check box to disable hidden characters within the field. It is displayed based on the **Security Type**.
Wifi Username	Enter the password that is required to join the WiFi network if the network password is static. Select the **Show Characters** check box to disable hidden characters within the field. It is displayed based on the **Security Type**.

FIGURE 250 Defining WiFi Profiles



iOS				
Configuration Fields	**WPA2**	**EAP-PEAP**	**EAP-TTLS**	**EAP_TLS**
WIFI_ENABLED (wifi_enabled)	TRUE	TRUE	TRUE	TRUE
SSID(wifi_ssid)	WIFI_SSID	WIFI_SSID	WIFI_SSID	WIFI_SSID
PROTOCOL(wifi_protocol)	WIFI_PROTOCOL_WPA2	WIFI_PROTOCOL_EAP_PEAP	WIFI_PROTOCOL_EAP_TTLS	WIFI_PROTOCOL_EAP_TLS
USERNAME(wifi_username)	Filled by admin/workspace username	Filled by admin/workspace username	Filled by admin/workspace username	Filled by admin/workspace username
PASSWORD(wifi_password)	Filled by admin/prompted during connection	Filled by admin/prompted during connection	Filled by admin/prompted during connection	None
OUTER IDENTITY(wifi_eap_identity)	None	Filled by admin/Anonymous/None	Filled by admin/Anonymous/None	None
INNER AUTHENTICATION(wifi_eap_inner_authentication)	None	PAP/CHAP/MSCHAP/MSCHAPv2	PAP/CHAP/MSCHAP/MSCHAPv2	None
Android				
Configuration Fields	**WPA2**	**EAP-PEAP**	**EAP-TTLS**	**EAP_TLS**
WIFI_ENABLED (wifi_enabled)	TRUE	TRUE	TRUE	TRUE
SSID(wifi_ssid)	WIFI_SSID	WIFI_SSID	WIFI_SSID	WIFI_SSID
PROTOCOL(wifi_protocol)	WIFI_PROTOCOL_WPA2	WIFI_PROTOCOL_EAP_PEAP	WIFI_PROTOCOL_EAP_TTLS	WIFI_PROTOCOL_EAP_TLS
USERNAME(wifi_username)	Filled by admin/workspace username	Filled by admin/workspace username	Filled by admin/workspace username	Filled by admin/workspace username
PASSWORD(wifi_password)	Filled by admin/prompted during connection	Filled by admin/prompted during connection	Filled by admin/prompted during connection	None
OUTER IDENTITY(wifi_eap_identity)	None	Filled by admin/Anonymous/None	Filled by admin/Anonymous/None	None
INNER AUTHENTICATION(wifi_eap_inner_authentication)	None	PAP/CHAP/MSCHAP/MSCHAPv2	PAP/CHAP/MSCHAP/MSCHAPv2	None

Configuring VPN On Demand

VPN On Demand (VOD) enables individual apps to connect automatically to a VPN when they are launched.

- **“Configuring VPN On Demand on iOS Devices” on page 218**.
- **“Configuring VPN On Demand on Android Devices” on page 229**.

Note: VPN On Demand is also supported for Managed Clients, see **“Configuring Managed Clients” on page 95**.

Configuring VPN On Demand on iOS Devices

This section describes the configuration and use of VPN On Demand (VOD) for iOS devices.

- **“Overview: iOS VPN On Demand” on page 218**.
- **“Configuring the Pulse Connect Secure Server” on page 219**.
- **“Configuring the Pulse Workspace Per App VPN” on page 224**.
- **“Registering iOS Devices and Installing Pulse Secure Client App” on page 228**.

Overview: iOS VPN On Demand

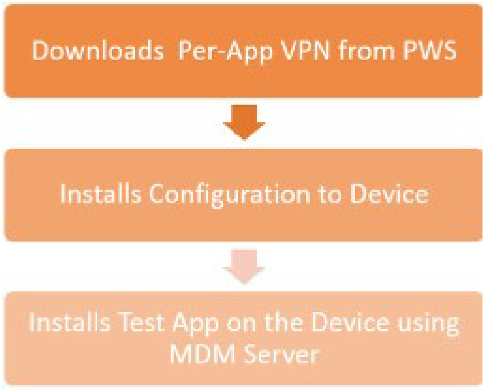
The Apple VPN framework supports per-application level layer-4 tunneling.

- *Traditional VPN* - All network traffic - including personal emails, connections to social and gaming networks, and personal web browsing - is through the corporate network's secure tunnel. This is created between a user's device and the VPN server. It impacts the user by reducing the network performance and the corporate by using corporate bandwidth that routes the employee’s personal data.
- *Per App VPN* - Apps can be configured to automatically connect to VPN when they are launched. Using this feature, only the corporate-managed apps will transfer the data over the VPN, and the employee's other personal data - such as personal web browsing, and connections to gaming and social networks - will not use the VPN. Apple recommends using the configurations applied through an MDM Server.

When the Per-App VPN rule is applied to the device, VPN will be started automatically in the following circumstances:

- When the user launches an application.
- When the user launches the Safari browser.

FIGURE 251 User Work Flow


Downloads Per-App VPN from PWS
Installs Configuration to Device
Installs Test App on the Device using MDM Server

After the device is configured and a test app is installed, the user can start the VPN as follows. Either by:

- Manually launch the Pulse Client and start the VPN, OR
- Manually launch the 3rd Party APP, which automatically starts the VPN.

The VPN Framework contacts the Pulse Client VPN Plug-in (VPNFlow API), which enables the VPN Framework to intercept the network traffic at the application layer.

Configuring the Pulse Connect Secure Server

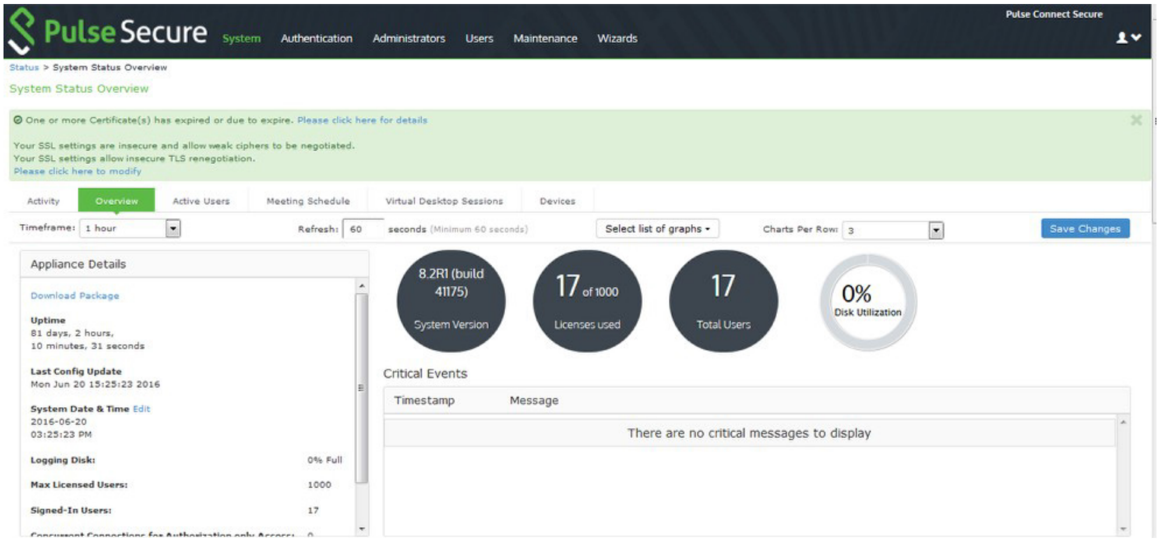
This section provides step by step instructions to configure Pulse Connect Secure.

Note: It is assumed that the administrator has a basic understanding of the Pulse Workspace and PCS VPN solution. For additional details, please refer to the Pulse Connect Secure documentation.

To configure Pulse Connect Secure:

1. Log in to PCS Admin Console as an admin user.

FIGURE 252 PCS Admin Console



One or more Certificate(s) has expired or due to expire. Please click here for details

Your SSL settings are insecure and allow weak ciphers to be negotiated.
Your SSL settings allow insecure TLS renegotiation.
Please click here to modify

Timeframe: 1 hour

Refresh: 60 seconds (Minimum 60 seconds)

Charts Per Row: 3

Uptime
81 days, 2 hours,
10 minutes, 31 seconds

Last Config Update
Mon Jun 20 15:25:23 2016

System Date & Time Edit
2016-06-20
03:25:23 PM

Logging Disk: 0% Full

Max Licensed Users: 1000

Signed-In Users: 17

Concurrent Connections for Authorization only Access: 0

8.2R1 (build 41175) System Version

17 of 1000 Licenses used

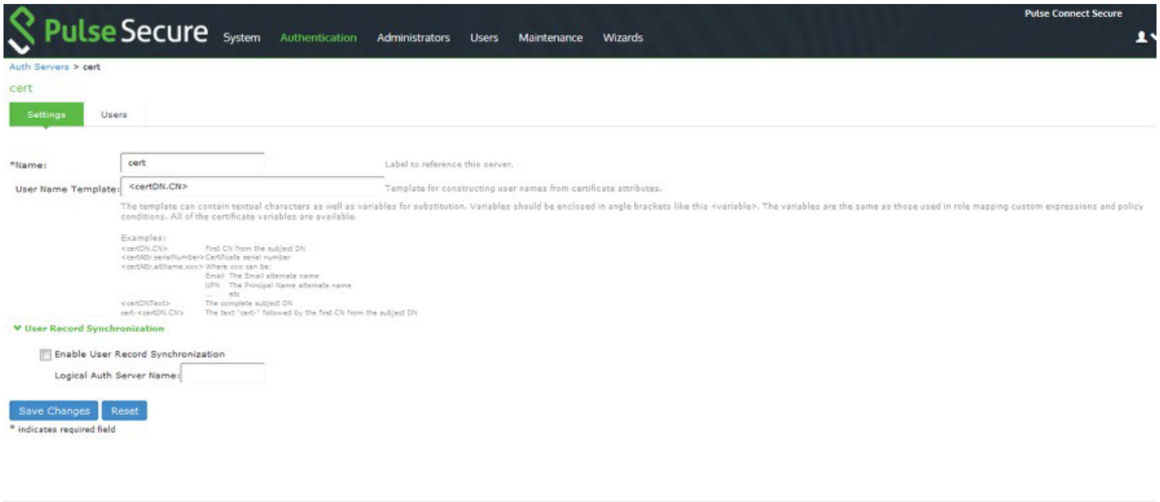
17 Total Users

0% Disk Utilization

There are no critical messages to display

2. Navigate to **Authentication > Auth. Servers > <auth_server> > Settings**, and create a certificate authorization configuration.

FIGURE 253 Create Certificate Authorization Configuration



*Name: cert — Label to reference this server.

User Name Template: <certDN.CN> — Template for constructing user names from certificate attributes.

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. The variables are the same as those used in role mapping custom expressions and policy conditions. All of the certificate variables are available.

```
Examples:
<certDN.CN>                 First CN from the subject DN
<certAttr.serialNumber>     Certificate serial number
<certAttr.altName.xxx>      Where xxx can be:
                            Email  The Email alternate name
                            UPN    The Principal Name alternate name
                            ...    etc
<certDNText>                The complete subject DN
cert-<certDN.CN>            The text "cert-" followed by the first CN from the subject DN
```

User Record Synchronization

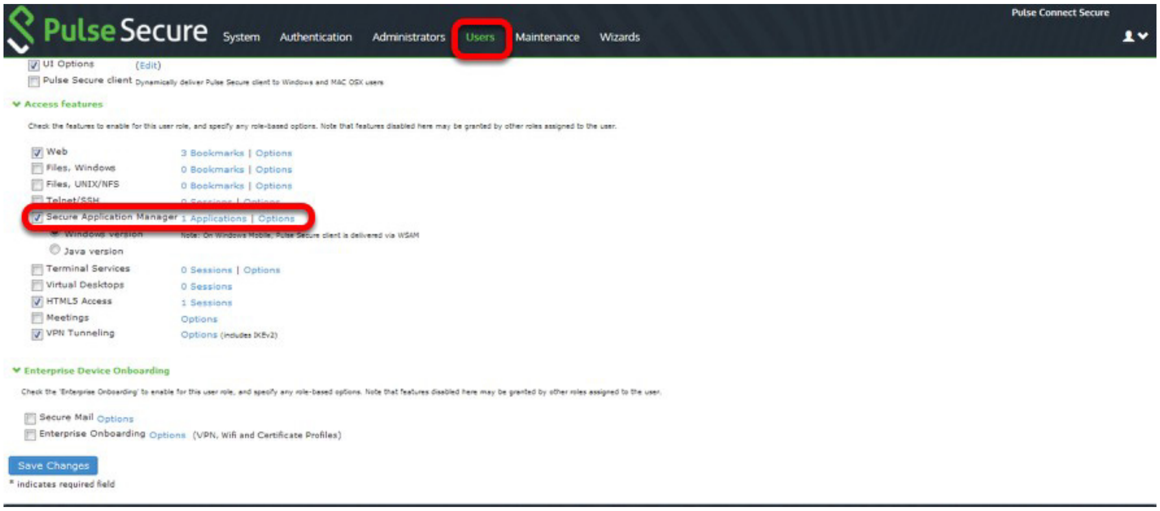
□ Enable User Record Synchronization

Logical Auth Server Name:

* indicates required field

3. Navigate to the **Roles** page, create a new role, and under **Access Features**, enable **WSAM**.

FIGURE 254 Create New Role



☑ UI Options (Edit)

□ Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

Access features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

☑ Web — 3 Bookmarks | Options
□ Files, Windows — 0 Bookmarks | Options
□ Files, UNIX/NFS — 0 Bookmarks | Options
□ Telnet/SSH — 0 Sessions | Options
☑ Secure Application Manager — 1 Applications | Options
● Windows version — Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
○ Java version
□ Terminal Services — 0 Sessions | Options
□ Virtual Desktops — 0 Sessions
☑ HTML5 Access — 1 Sessions
□ Meetings — Options
☑ VPN Tunneling — Options (includes IKEv2)

Enterprise Device Onboarding

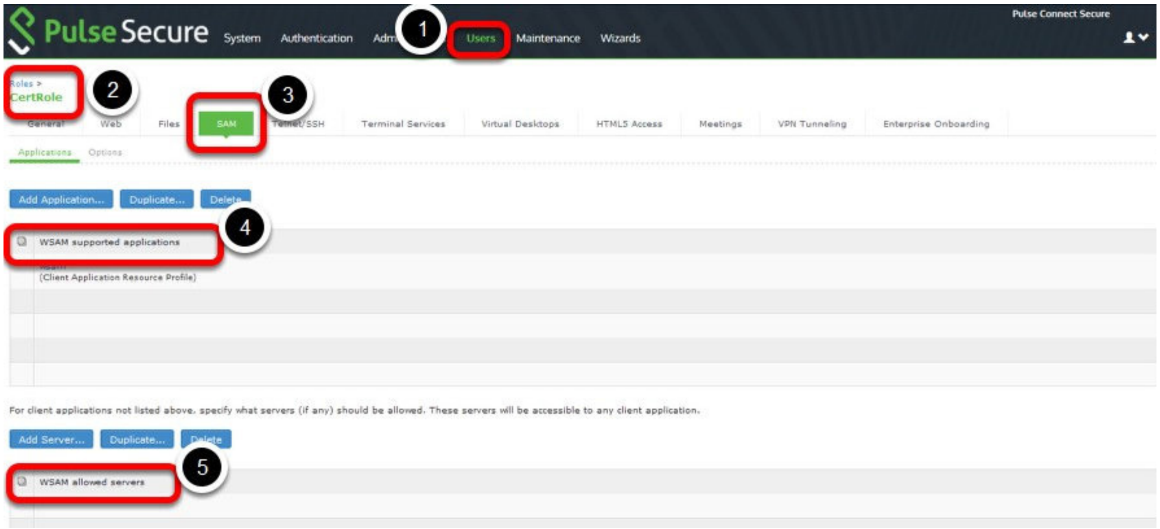
Check the 'Enterprise Onboarding' to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

□ Secure Mail Options
□ Enterprise Onboarding Options (VPN, Wifi and Certificate Profiles)

* indicates required field

4. Navigate to the **SAM** applications page, and create a WSAM supported application and a WSAM-enabled server with *Allow all* settings.

FIGURE 255 WSAM Supported Application and Servers



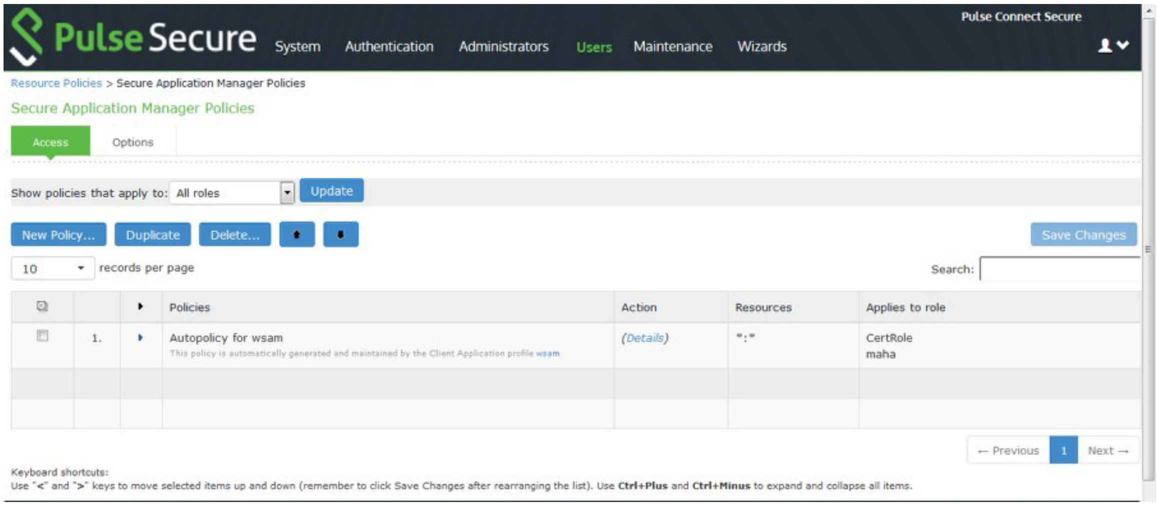
WSAM supported applications
wsam
(Client Application Resource Profile)

For client applications not listed above, specify what servers (if any) should be allowed. These servers will be accessible to any client application.

WSAM allowed servers

5. Navigate to **Users > Resource Policies > SAM > Access control**, create a SAM ACL with an *Allow All* option, and assign it to required Roles.

FIGURE 256 Assign SAM Access Control



Resource Policies > Secure Application Manager Policies

Secure Application Manager Policies

Show policies that apply to: All roles

10 records per page

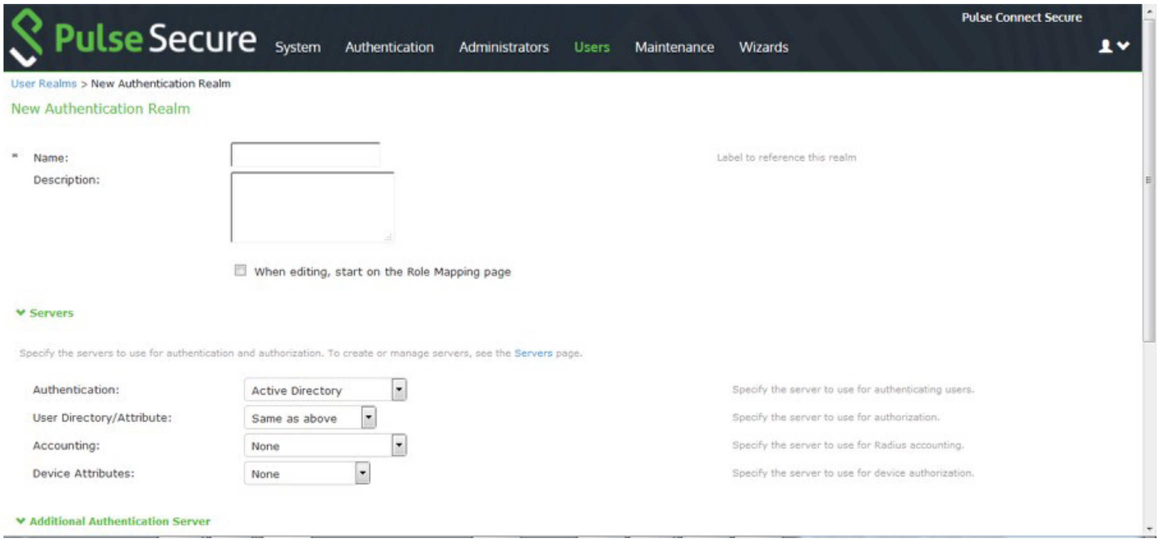
Search:

☐		▸	Policies	Action	Resources	Applies to role
☐	1.	▸	Autopolicy for wsam This policy is automatically generated and maintained by the Client Application profile wsam	(Details)	*:*	CertRole maha

Keyboard shortcuts:
Use "<" and ">" keys to move selected items up and down (remember to click Save Changes after rearranging the list). Use **Ctrl+Plus** and **Ctrl+Minus** to expand and collapse all items.

6. Navigate to **Users > User Realms**, create a new Realm and assign it with one of the supported Authentication Servers.

FIGURE 257 Create Realm



User Realms > New Authentication Realm

New Authentication Realm

* Name:		Label to reference this realm
Description:		

□ When editing, start on the Role Mapping page

Servers

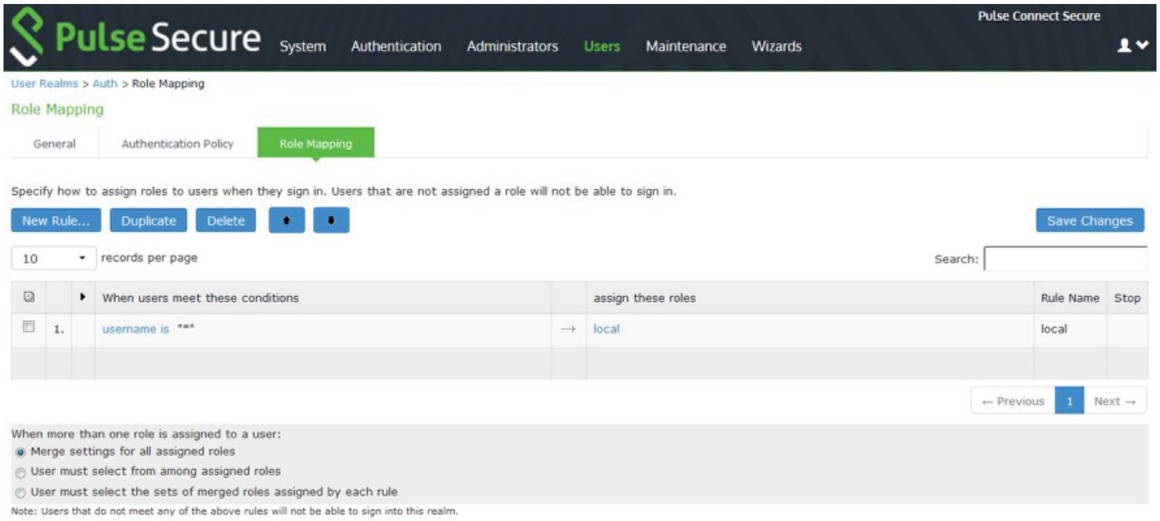
Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication:	Active Directory	Specify the server to use for authenticating users.
User Directory/Attribute:	Same as above	Specify the server to use for authorization.
Accounting:	None	Specify the server to use for Radius accounting.
Device Attributes:	None	Specify the server to use for device authorization.

Additional Authentication Server

7. Navigate to **Users > User Realms > <select user> > Role Mapping**, create a Role mapping rule and assign it to the corresponding Role.

FIGURE 258 Create Role Mapping Rule



User Realms > Auth > Role Mapping

Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

10 records per page

Search:

□			When users meet these conditions		assign these roles	Rule Name	Stop
□	1.		username is "*"	→	local	local	

When more than one role is assigned to a user:

● Merge settings for all assigned roles

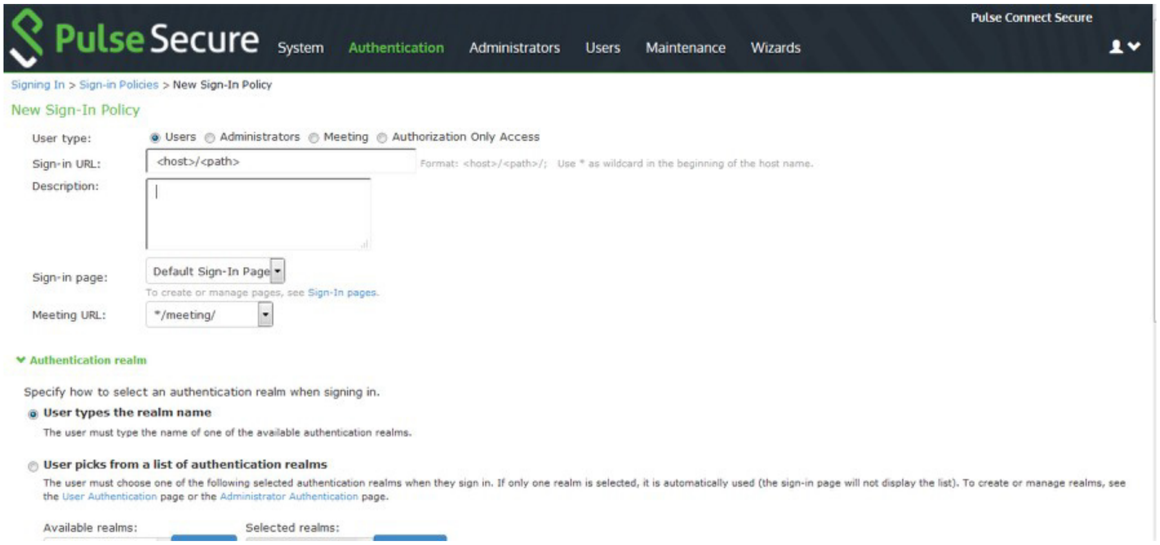
○ User must select from among assigned roles

○ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

8. Navigate to **Authentication > Signing In > Sign In Policies**, create a new Sign-In URL and assign it to the corresponding realm.

FIGURE 259 Create New Sign-In URL



Signing In > Sign-in Policies > New Sign-In Policy

New Sign-In Policy

User type: ● Users ○ Administrators ○ Meeting ○ Authorization Only Access

Sign-in URL: <host>/<path> Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: Default Sign-In Page

To create or manage pages, see Sign-In pages.

Meeting URL: */meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

● **User types the realm name**

The user must type the name of one of the available authentication realms.

○ **User picks from a list of authentication realms**

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the User Authentication page or the Administrator Authentication page.

Available realms: Selected realms:

For more details about PCS configuration, refer to PCS Administration Guide.

Configuring the Pulse Workspace Per App VPN

This section describes the configuration of Per App VPN:

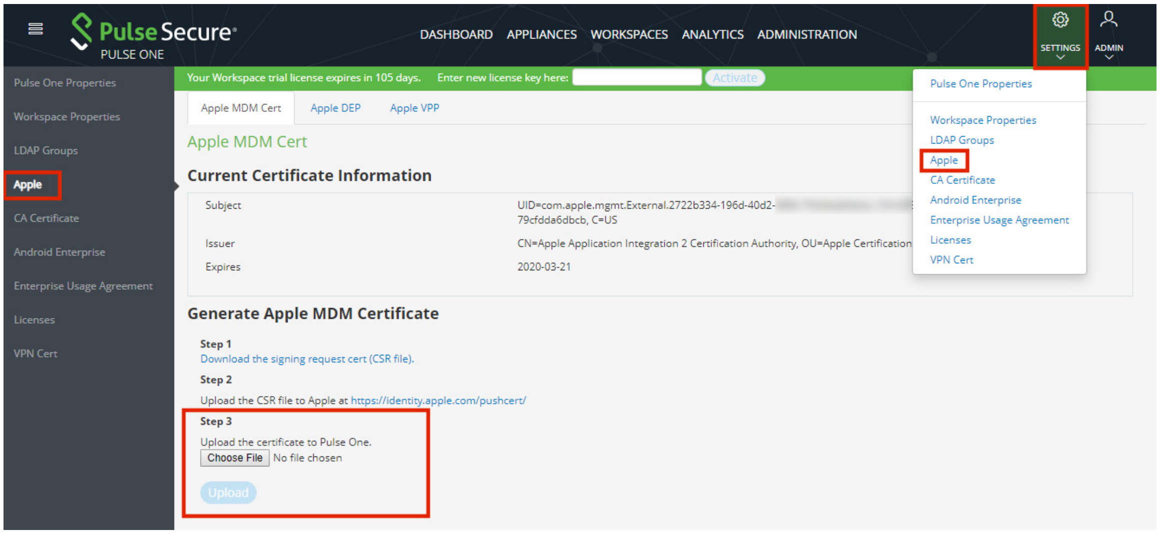
- “Adding an iOS MDM Certificate” on page 224.
- “Downloading a VPN Certificate” on page 227.

Adding an iOS MDM Certificate

An Apple MDM push certificate allows your Workspace management console to push policies, updates and actions to your managed iOS devices.

1. Click the settings icon on top-right-corner of the page and select **Apple MDM Cert**.

   FIGURE 260 Upload Apple MDM Certificate to Pulse One

   Your Workspace trial license expires in 105 days. Enter new license key here:

   Apple MDM Cert

   Current Certificate Information

   Subject UID=com.apple.mgmt.External.2722b334-196d-40d2-[redacted]79cfdda6dbcb, C=US

   Issuer CN=Apple Application Integration 2 Certification Authority, OU=Apple Certification

   Expires 2020-03-21

   Generate Apple MDM Certificate

   Step 1
   Download the signing request cert (CSR file).

   Step 2
   Upload the CSR file to Apple at https://identity.apple.com/pushcert/

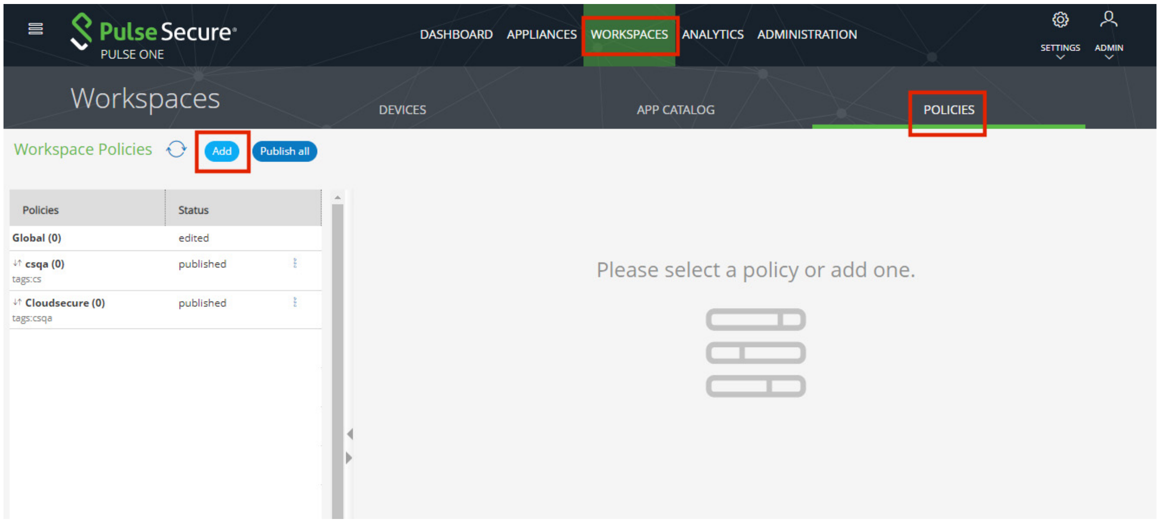
   Step 3
   Upload the certificate to Pulse One.
   No file chosen

   The **Apple MDM Cert** management page appears.

2. Upload the MDM certificate to Pulse One.

3. Click the **Workspaces** menu and then the **Policies** tab.

FIGURE 261 Creating Per App VPN Policy



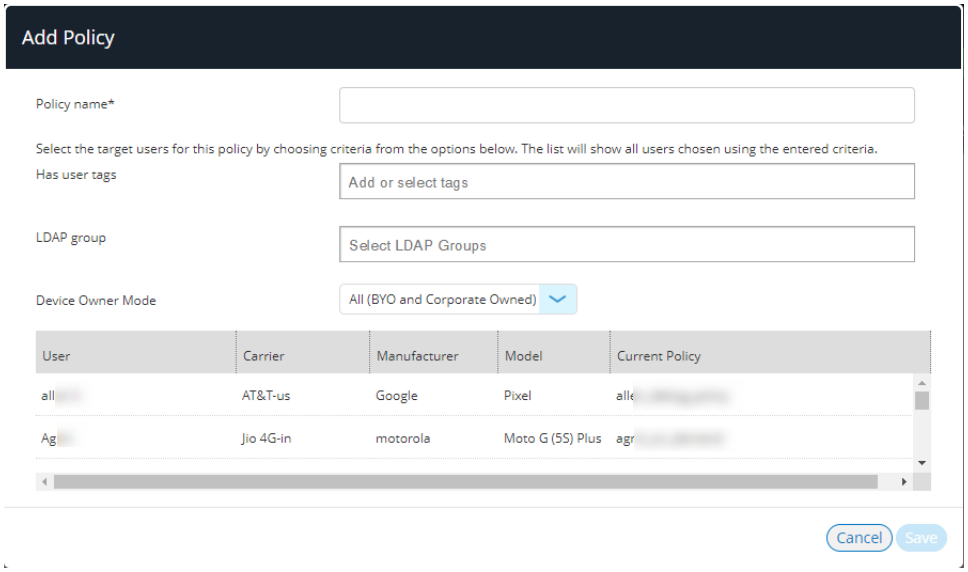
Policies	Status
Global (0)	edited
csqa (0) tags:cs	published
Cloudsecure (0) tags:csqa	published

Please select a policy or add one.

4. In the **Workspace Policies** section, click **Add**.

The **Add Policy** dialog appears.

FIGURE 262 Add Policy Details


Add Policy

Policy name*

Select the target users for this policy by choosing criteria from the options below. The list will show all users chosen using the entered criteria.

Has user tags: Add or select tags

LDAP group: Select LDAP Groups

Device Owner Mode: All (BYO and Corporate Owned)

User	Carrier	Manufacturer	Model	Current Policy
all[redacted]	AT&T-us	Google	Pixel	alle[redacted]
Ag[redacted]	Jio 4G-in	motorola	Moto G (5S) Plus	agr[redacted]

5. Set a **Policy name**. This is a label for you to identify the policy.

6. Add tags to **Has user tags**.

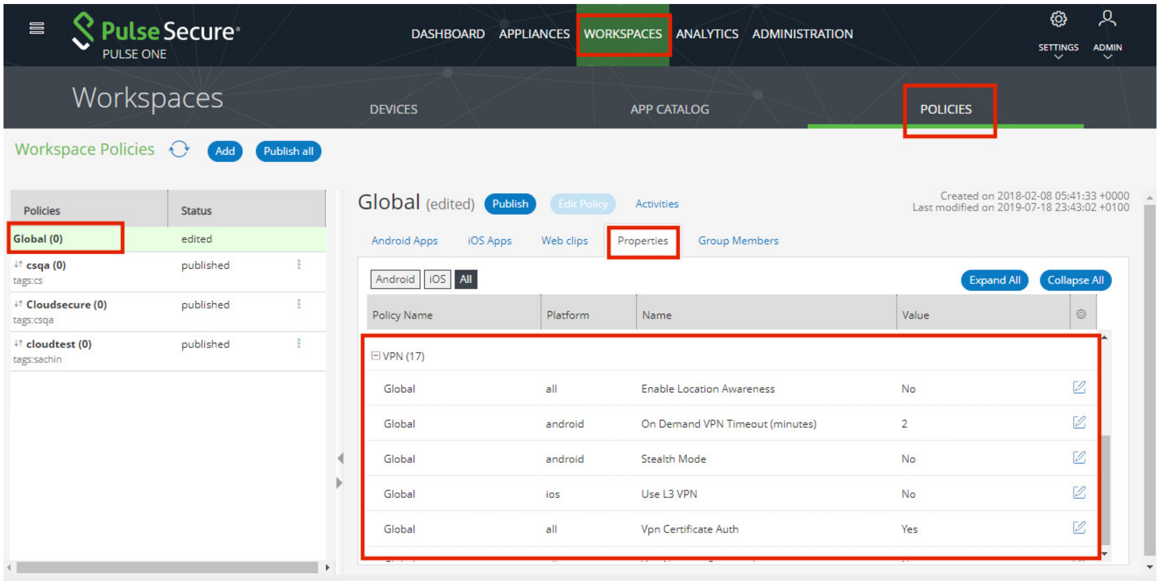
7. Set the policies target criteria and **LDAP group**.

8. Click **Save**.

Note: The generated **Host URL** and **Code** will be used later to register your appliance.

9. Select the **Properties** tab and define a VPN Profile.

FIGURE 263 Add Policy Details



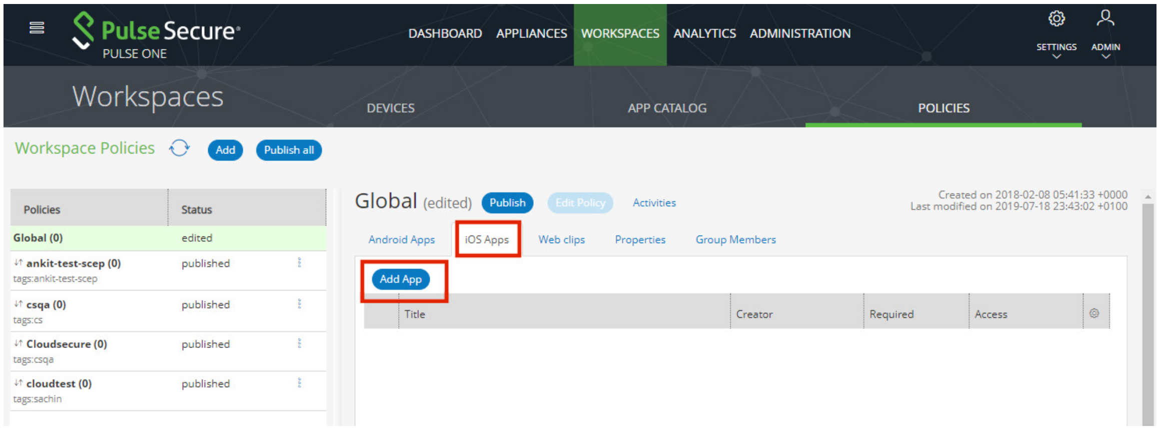
Created on 2018-02-08 05:41:33 +0000
Last modified on 2019-07-18 23:43:02 +0100

Policies	Status
Global (0)	edited
csqa (0) tags:cs	published
Cloudsecure (0) tags:csqa	published
cloudtest (0) tags:sachin	published

Policy Name	Platform	Name	Value
VPN (17)			
Global	all	Enable Location Awareness	No
Global	android	On Demand VPN Timeout (minutes)	2
Global	android	Stealth Mode	No
Global	ios	Use L3 VPN	No
Global	all	Vpn Certificate Auth	Yes

10. Select the **iOS Apps** tab.

FIGURE 264 iOS Apps



Created on 2018-02-08 05:41:33 +0000
Last modified on 2019-07-18 23:43:02 +0100

Policies	Status
Global (0)	edited
ankit-test-scep (0) tags:ankit-test-scep	published
csqa (0) tags:cs	published
Cloudsecure (0) tags:csqa	published
cloudtest (0) tags:sachin	published

Title	Creator	Required	Access

11. Click **Add App**.

    The **Add App from App Catalog** dialog appears.

12. Select the required app and click **Add**.

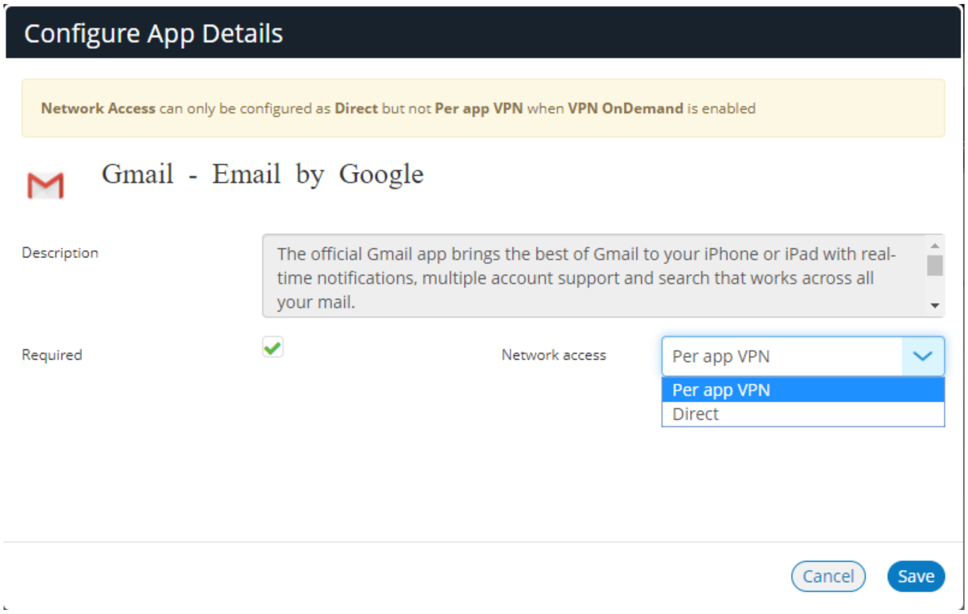
    The app is added to the list of iOS apps for the policy.

13. In the list, select the app, click its menu and select **Edit app rule**.

    The **Configure App Details** dialog appears.

14. Select the **Network access** as *Per app VPN*.

FIGURE 265 Configure App Details



Configure App Details

Network Access can only be configured as **Direct** but not **Per app VPN** when **VPN OnDemand** is enabled

Gmail - Email by Google

Description: The official Gmail app brings the best of Gmail to your iPhone or iPad with real-time notifications, multiple account support and search that works across all your mail.

Required: ✓

Network access: Per app VPN

15. Click **Save**.

When a policy is created, it starts in the *edited* state. You can now add applications and properties to the policy before applying the policy to your mobile devices.

After you have completed editing the policy, click **Publish**. You will see the policies state change to publishing and then published. This will apply the policy to the mobile devices.

Downloading a VPN Certificate

The Workspace Management Server includes an integrated Certificate Authority (CA) and an Online Certificate Status Protocol (OCSP) servers.

These can be used to issue certificates to Workspaces for client certificate based VPN authentication.

You can use the VPN Cert window to download your Workspace Root CA certificate. This will be used when configuring your VPN.

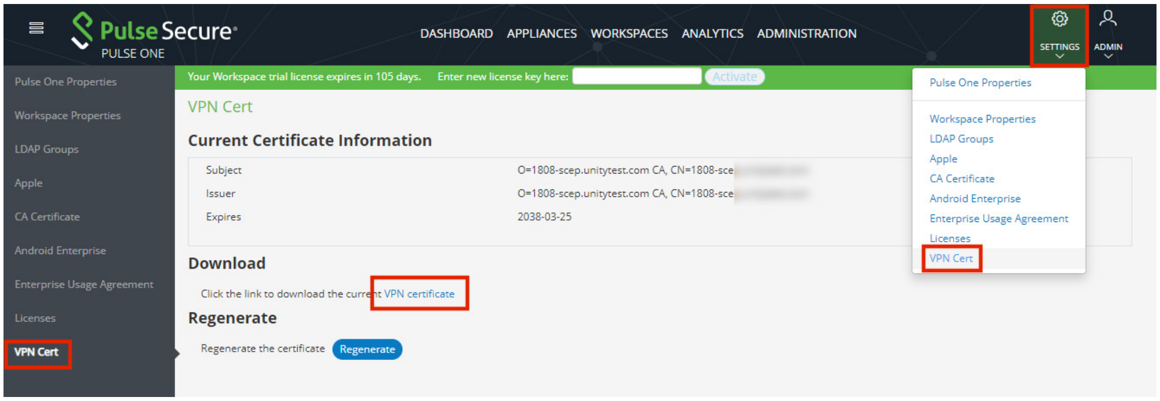
To download VPN certificate:

1. Click the settings icon on top-right corner of the page.

2. Select **VPN Cert**.

The **VPN Cert** page appears.

FIGURE 266 VPN Cert



Your Workspace trial license expires in 105 days. Enter new license key here:

VPN Cert

Current Certificate Information

Subject	O=1808-scep.unitytest.com CA, CN=1808-sce
Issuer	O=1808-scep.unitytest.com CA, CN=1808-sce
Expires	2038-03-25

Download

Click the link to download the current VPN certificate

Regenerate

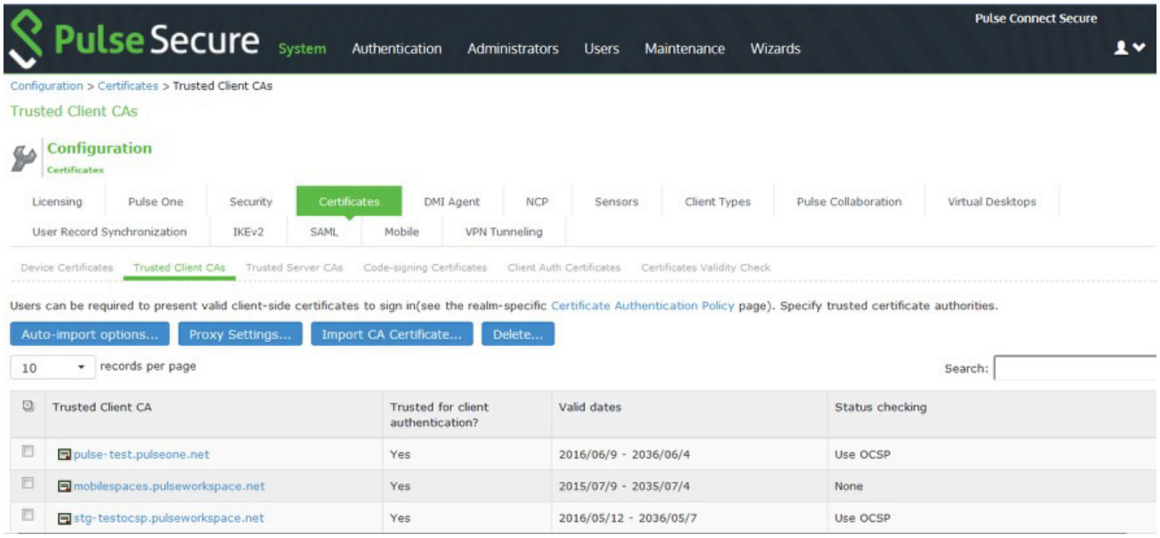
Regenerate the certificate

3. In the **VPN Cert** page, under **Download**, click **VPN Certificate**.

4. Download the Workspace CA cert from the Pulse One server.

5. Log into Pulse Connect Secure, access the **Certificates > Trusted Client CAs** tab.

FIGURE 267 Trusted Client CA Page



Configuration > Certificates > Trusted Client CAs

Trusted Client CAs

Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

10 records per page

Search:

□	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
□	pulse-test.pulseone.net	Yes	2016/06/9 - 2036/06/4	Use OCSP
□	mobilespaces.pulseworkspace.net	Yes	2015/07/9 - 2035/07/4	None
□	stg-testocsp.pulseworkspace.net	Yes	2016/05/12 - 2036/05/7	Use OCSP

6. Click **Import CA Certificate** to upload the certificate.

Registering iOS Devices and Installing Pulse Secure Client App

To register an iOS BYOD device and install the Pulse Secure Client app, perform the procedures described in **"Onboarding iOS BYOD Devices" on page 43**.

Configuring VPN On Demand on Android Devices

This section describes the configuration and use of VPN On Demand (VOD) for Android devices.

- **"Overview: Android VPN On Demand" on page 229**.
- **"Configuring VPN On Demand on Pulse Workspace" on page 230**.
- **"Registering an Android Device and Installing the Pulse Secure Client App" on page 231**.

Overview: Android VPN On Demand

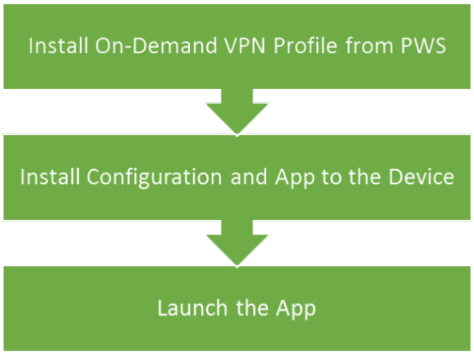
VPN on Demand (VOD) is supported for Android mobile devices.

- *Traditional VPN* – After the corporate network's secure tunnel is created between a user's device and the VPN server, it remains connected even if there is no traffic through the tunnel. It impacts the user as it consumes more licenses since a given endpoint will always be connected. Also, there will be more battery drain due to the unnecessary VPN connection.
- *VPN On Demand* – Apps can be configured to automatically connect to VPN when they are launched. This feature is intended to be used only within the Android work profile, since it is predominantly being used at an app level and only Pulse Workspace is aware of the apps in the work profile. Using this feature, only the corporate managed apps will transfer the data over the VPN and the employee's other personal data like personal web browsing, connections to gaming and social networks will not use the VPN.

When the VPN On Demand profile is applied to the device, VPN will be started automatically in the following two conditions:

- When user launches the application.
- When the application sends traffic in the background.

FIGURE 268 User Work Flow


Install On-Demand VPN Profile from PWS
Install Configuration and App to the Device
Launch the App

In VPN On Demand, a blocking interface is set up on the device which monitors the VPN configured apps for the network traffic. Whenever an application whose network access type is "require VPN", tries to perform any network activity, the blocking interface detects this. It thereafter authenticates the user, tears down the blocking interface and establishes the VPN connection.

Configuring VPN On Demand on Pulse Workspace

Before you proceed with the configuration, ensure Android for Work is enrolled within your EMM console. For the enrollment details, see **"Configuring Android Enterprise" on page 113**.

Also ensure that the required apps are added to the App Catalog in the EMM console. For adding apps to the EMM console, see **"Adding an Android App to the App Catalog" on page 113**.

This section describes the procedures involved in VPN On Demand configuration. These include:

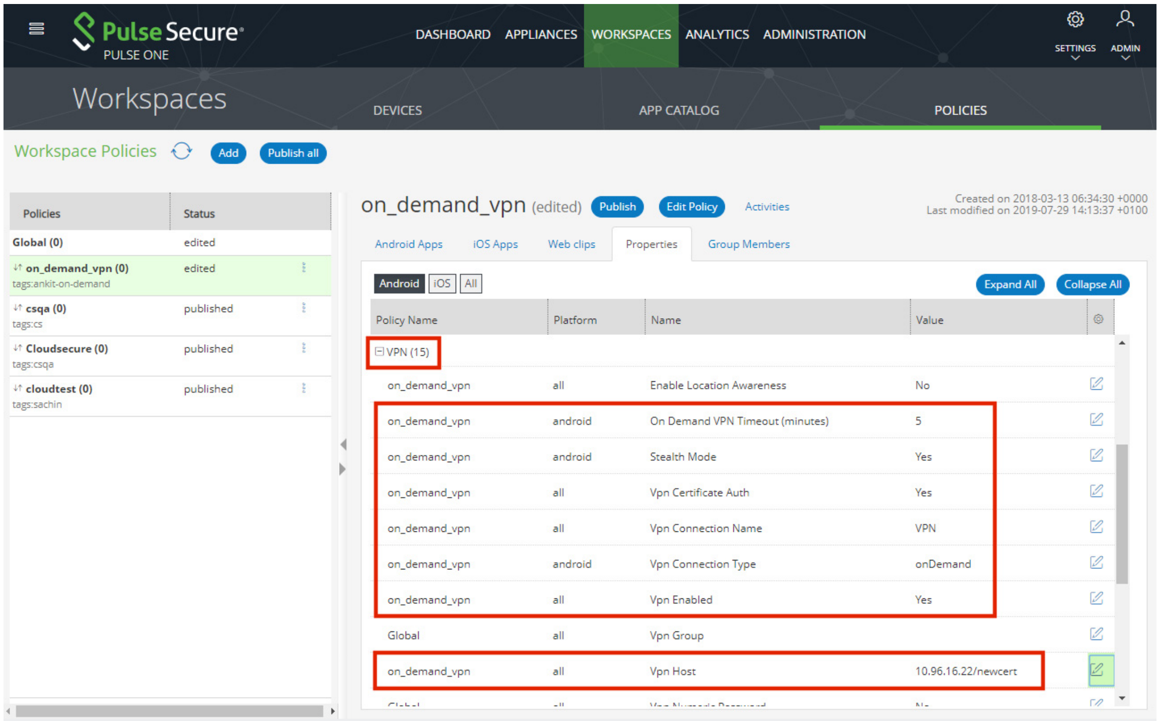
- Configuring On-Demand VPN related attributes in the policy.
- Adding apps which require VPN in the policy.

To configure VPN On Demand related attributes in the policy, perform the following steps:

1. Log in to Pulse One admin console.
2. Select the **Workspaces** menu, and then select **Policies**.
3. Create a new policy (if required), see **"Creating a Policy" on page 164**.
4. Select the required policy.
5. Click the **Properties** tab.
6. Expand the *VPN* category and configure the following properties:
    - **On Demand VPN Timeout (minutes)**: (Optional) For example, *5*.
    - **Stealth Mode**: *True*.
    - **Vpn Certificate Auth**: *Yes*.
    - **Vpn Connection Name**. For example: *VPN*.
    - **Vpn Connection Type**: *onDemand*.
    - **Vpn Enabled**: *Yes*.
    - **Vpn Host**. For example: *https://10.11.12.13/newcert*.
    - **Vpn Verify Certificate**: *Yes*.

7. Click **Publish**.

FIGURE 269 Policy Properties



on_demand_vpn (edited)

Created on 2018-03-13 06:34:30 +0000
Last modified on 2019-07-29 14:13:37 +0100

Policies	Status
Global (0)	edited
on_demand_vpn (0) tags:ankit-on-demand	edited
csqa (0) tags:cs	published
Cloudsecure (0) tags:csqa	published
cloudtest (0) tags:sachin	published

Policy Name	Platform	Name	Value
⊟ VPN (15)			
on_demand_vpn	all	Enable Location Awareness	No
on_demand_vpn	android	On Demand VPN Timeout (minutes)	5
on_demand_vpn	android	Stealth Mode	Yes
on_demand_vpn	all	Vpn Certificate Auth	Yes
on_demand_vpn	all	Vpn Connection Name	VPN
on_demand_vpn	android	Vpn Connection Type	onDemand
on_demand_vpn	all	Vpn Enabled	Yes
Global	all	Vpn Group	
on_demand_vpn	all	Vpn Host	10.96.16.22/newcert
Global	all	Vpn Numeric Password	No

To add the apps from App Catalog to the policy with **Network Access** as *Require VPN* and publish, see **"Adding an Android App to a Policy" on page 130**.

Registering an Android Device and Installing the Pulse Secure Client App

To register an Android BYOD device and install the Pulse Secure Client app, perform the procedures described in **"Onboarding Android BYOD Devices" on page 53**.

Configuring Kerberos-Based Authentication

Kerberos-based authentication is supported on iOS devices at v7.0 or later.

Kerberos-based authentication is configured by the administrator using the **Single Sign On** workspace properties for a policy, see **"Single Sign On" on page 170**.

To configure Kerberos-based authentication:

1. Log in to Pulse One admin console.
2. Select the **Workspaces** menu, and then select **Policies**.
3. Create a new policy (if required), see **"Creating a Policy" on page 164**.
4. Select the required policy.
5. Select the **Properties** tab.
6. Expand the *Single Sign On* category and configure the following properties:
   - **Account Name** – The name for the account.
   - **Authentication Realm** – The Kerberos realm name. This value is case sensitive.
   - **Enabled** – Set this to *Yes* to enable Kerberos authentication.
   - **Package names allowed to use Kerberos Auth** – (Optional) A list of application identifiers that are allowed to use this login. Each line of the property represents a single app. For example:

     com.microsoft.outlook
     com.google.mail.

     Note: If this field not specified, all app identifiers match automatically.
   - **Principal Name** – Set this to the macro string value <*USER_USERNAME*>.

     Note: This macro value is automatically replaced with the user's name when connecting to a device.
   - **URL Prefix Matches to use Kerberos Auth** – A list of URLs prefixes that must be matched to use this account for Kerberos authentication over HTTP. Each line of this property represents a URL. For example:

     http://demo.pwskerb.example1
     http://demo.pwskerb.example2

     Note: Kerberos authentication for the user will be performed manually once, on the first match of any of the listed URLs. For all subsequent uses of any URL, Kerberos authentication will be performed automatically.

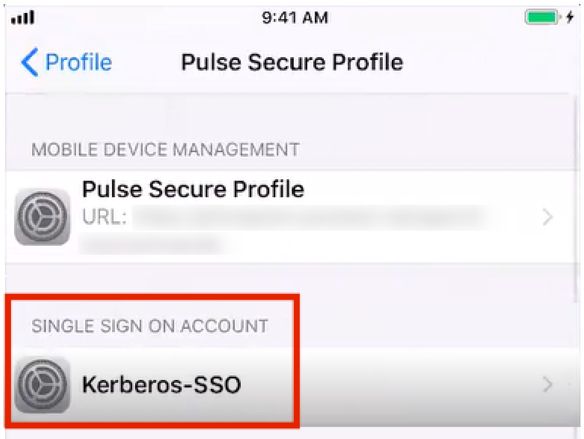
7. Click **Publish** to push the updated policy to all affected devices.

   Note: Any new iOS devices (BYOD or corporate) that use the policy will receive all settings automatically when they are onboarded.

8. (Optional) To confirm the presence of Kerberos authentication on an individual device:

   - On the iOS device, access **Settings** > **General** > **Device Management** > **Pulse Secure Profile** > **More Details**.
   - Under **Single Sign On Account**, a Kerberos entry will be present. The name of the entry is the **Account** policy property. For example:

     FIGURE 270 iOS Device Management: Kerberos

     9:41 AM

     < Profile

     Pulse Secure Profile

     MOBILE DEVICE MANAGEMENT

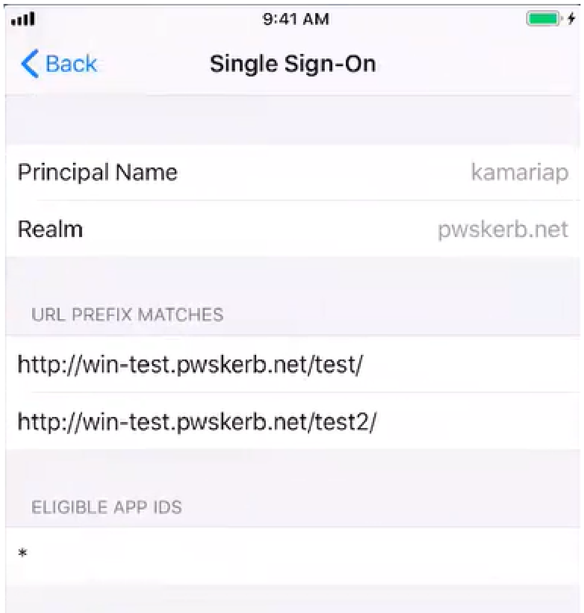
     Pulse Secure Profile
     URL: [redacted]

     SINGLE SIGN ON ACCOUNT

     Kerberos-SSO

   - Tap the Kerberos entry to view its details. For example:

     FIGURE 271 iOS Device Management: Kerberos Details

     9:41 AM

     < Back

     Single Sign-On

     Principal Name kamariap

     Realm pwskerb.net

     URL PREFIX MATCHES

     http://win-test.pwskerb.net/test/

     http://win-test.pwskerb.net/test2/

     ELIGIBLE APP IDS

     *

In this example:

  - The **Principal Name**, which has the macro value <USER_USERNAME> in the workspace properties for the policy, is replaced by the specific user name.
  - There are two configured **URL Prefix Matches**.
  - There are no configured **Eligible App IDs** (app identifiers). As a result, a wildcard asterisk (*) setting ensures that all app identifiers match.

- When the user accesses a matching resource for the first time using Kerberos authentication, a Kerberos login page appears. After a valid login is used, the login page will no longer appear for any attempts to access a matching resource.

Working with Device Location

This section describes the device location functionality in Pulse Workspace.

- “Overview of Device Location” on page 235.
- “Creating a Google API Key” on page 236.
- “Configuring Device Location” on page 242.
- “Locating a Device” on page 249.
- “Working with Lost Mode for a Device” on page 250.

Note: Device location requires iOS v10 or later, or Android 8.0 or later.

Overview of Device Location

Pulse Workspace supports the admin ability to locate a device.

Note: Device location requires iOS v10 or later, or Android 8.0 or later.

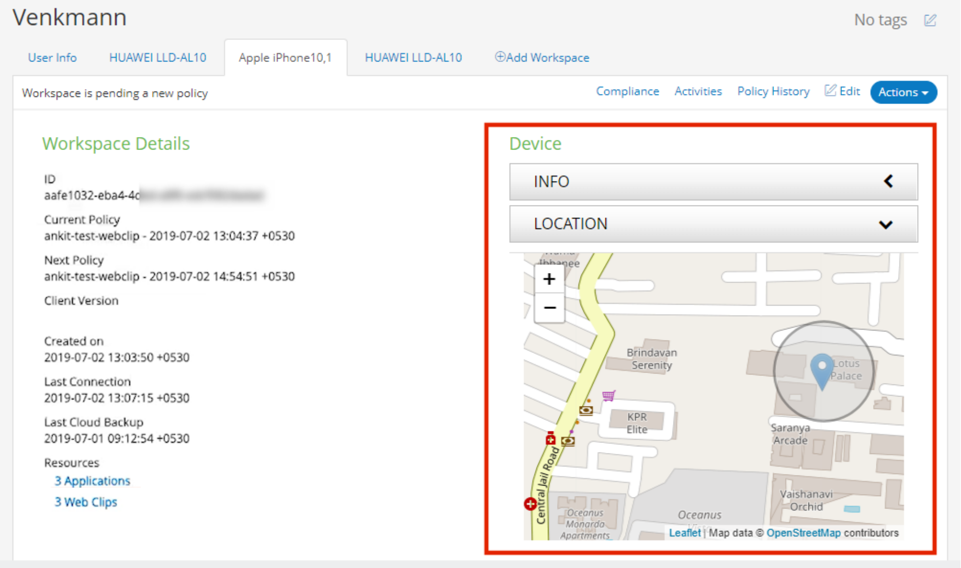
Device location can be enabled by admins and configured for use through policies applied to devices. Pulse Workspace uses an Apple/Google push service to send a notification to the Pulse Client App which is installed on a device. The Pulse Client then uses location services to locate the device and notify Pulse Workspace.

The most-recently retrieved device location is displayed in a map in the workspace details on the **Devices** tab:

- For iOS devices, the requested accuracy of the device’s location is indicated by a circle.
- For Android devices, the calculated accuracy of the device’s location is indicated by a circle.

For example:

FIGURE 272 Device Location Map



Workspace is pending a new policy

Workspace Details

ID
aafe1032-eba4-4c[redacted]

Current Policy
ankit-test-webclip - 2019-07-02 13:04:37 +0530

Next Policy
ankit-test-webclip - 2019-07-02 14:54:51 +0530

Client Version

Created on
2019-07-02 13:03:50 +0530

Last Connection
2019-07-02 13:07:15 +0530

Last Cloud Backup
2019-07-01 09:12:54 +0530

Resources
3 Applications
3 Web Clips

The location is updated whenever a locate request is manually issued from the **Actions** pull-down menu.

Note: By default, the *Leaflet* browser map plug-in is used. If you have a Google API key, you can optionally use a Google Maps browser plug-in to display the map, see **"Creating a Google API Key" on page 236**.

Creating a Google API Key

Note: The activities described in this section are optional, and apply to both iOS and Android devices.

Note: Device location requires iOS v10 or later, or Android 8.0 or later.

The device location feature uses an embedded map on the **Devices** tab.

By default, the Leaflet map browser plug-in is used. If you have a Google API key, you can optionally use a Google Maps browser plug-in to display the map.

Perform the following steps to create a Google API key:

- **"Enabling the Maps JavaScript API" on page 236**.
- **"Creating a Google Cloud Project" on page 238**.
- **"Generating a Google API Key for a Project" on page 240**.

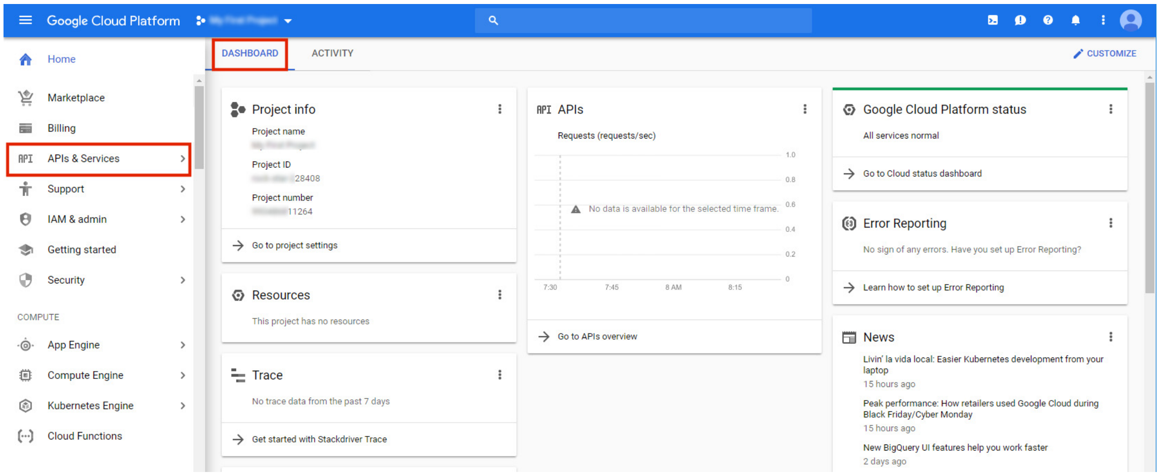
Enabling the Maps JavaScript API

Before you can create a Google API key for Google Maps, you must enable the Google Maps JavaScript API.

To enable the Google Maps JavaScript API:

1. Access the Google Cloud Platform website **https://cloud.google.com** from your browser.
2. Register for a Google Cloud Platform account, including your billing details.
3. Access the **Dashboard** tab for your account. For example:

FIGURE 273 Google Cloud Platform Dashboard



Google Cloud Platform [redacted]

Project info

Project name
[redacted]

Project ID
[redacted]28408

Project number
[redacted]11264

Go to project settings

Resources

This project has no resources

Trace

No trace data from the past 7 days

Get started with Stackdriver Trace

APIs

Requests (requests/sec)

No data is available for the selected time frame.

Go to APIs overview

Google Cloud Platform status

All services normal

Go to Cloud status dashboard

Error Reporting

No sign of any errors. Have you set up Error Reporting?

Learn how to set up Error Reporting

News

Livin' la vida local: Easier Kubernetes development from your laptop
15 hours ago

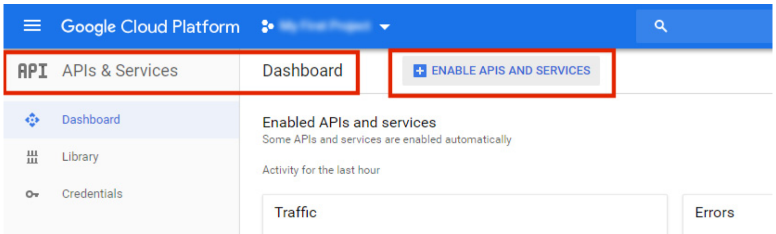
Peak performance: How retailers used Google Cloud during Black Friday/Cyber Monday
15 hours ago

New BigQuery UI features help you work faster
2 days ago

4. In the left menu, click **APIs & Services** and then click **Dashboard**.

   The **APIs & Services Dashboard** appears. For example:

   FIGURE 274 Google Cloud APIs and Services Dashboard



Enabled APIs and services

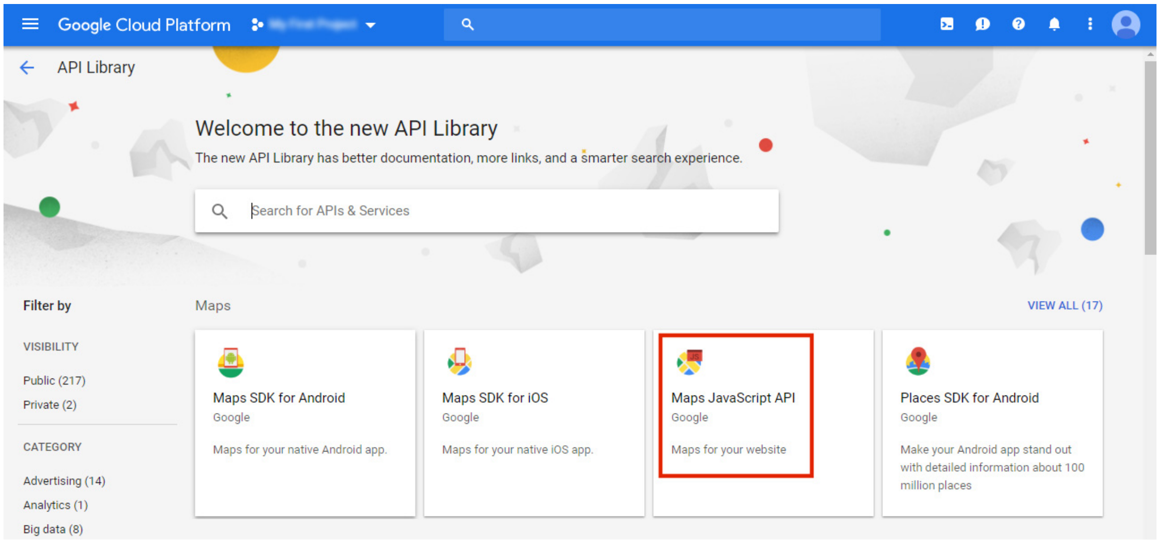
Some APIs and services are enabled automatically

Activity for the last hour

5. Click **Enable APIs and Services**.

   The **API Library** page appears. For example:

   FIGURE 275 Google Cloud API Library



Welcome to the new API Library

The new API Library has better documentation, more links, and a smarter search experience.

Maps SDK for Android
Google
Maps for your native Android app.

Maps SDK for iOS
Google
Maps for your native iOS app.

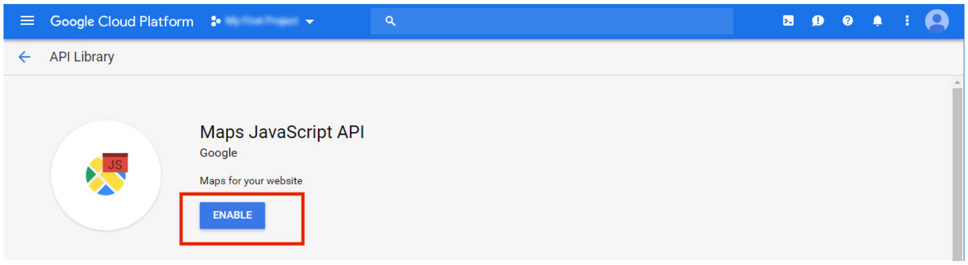
Maps JavaScript API
Google
Maps for your website

Places SDK for Android
Google
Make your Android app stand out with detailed information about 100 million places

6. Under **Maps**, click **Maps JavaScript API**.

   The **Maps JavaScript API** page appears.

   FIGURE 276 Google Cloud Maps JavaScript API

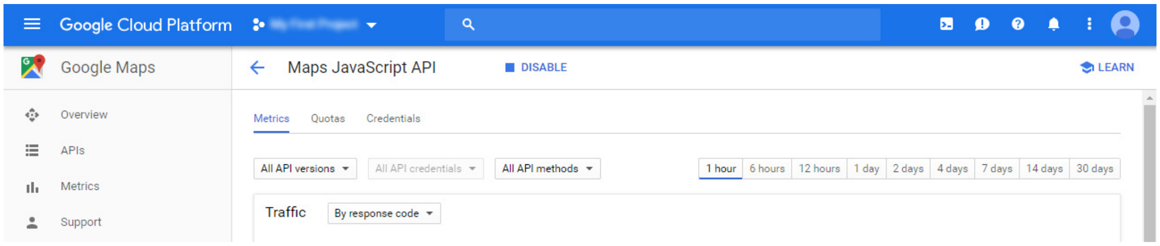


Maps JavaScript API
Google
Maps for your website

7. Click **Enable**.

   The **Maps JavaScript API** page updates.

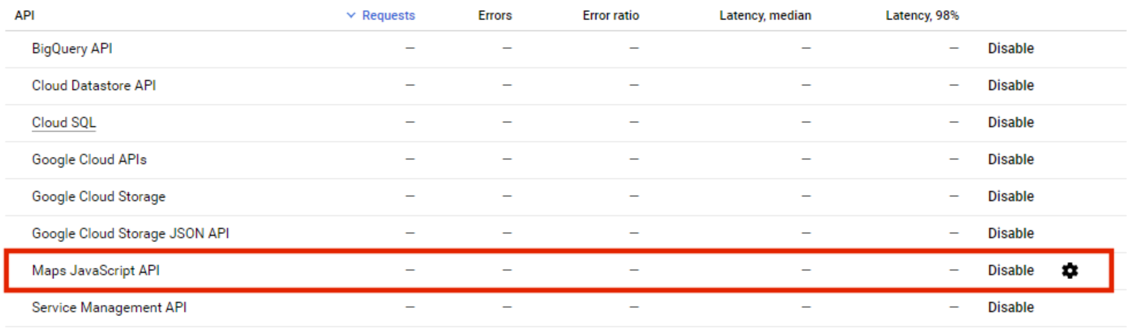
   FIGURE 277 Google Cloud Maps JavaScript API Updated



8. Return to the **APIs & Services Dashboard** and view the list of APIs.

   The list now includes Maps JavaScript API. For example:

   FIGURE 278 Google Cloud **APIs and Services Dashboard Updated**



API	Requests	Errors	Error ratio	Latency, median	Latency, 98%	
BigQuery API	–	–	–	–	–	Disable
Cloud Datastore API	–	–	–	–	–	Disable
Cloud SQL	–	–	–	–	–	Disable
Google Cloud APIs	–	–	–	–	–	Disable
Google Cloud Storage	–	–	–	–	–	Disable
Google Cloud Storage JSON API	–	–	–	–	–	Disable
Maps JavaScript API	–	–	–	–	–	Disable
Service Management API	–	–	–	–	–	Disable

After you have enabled the Maps JavaScript API, you can create/select the required Google Cloud Platform project, see **"Creating a Google Cloud Project" on page 238**.

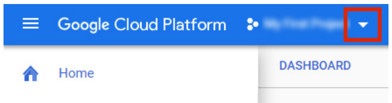
Creating a Google Cloud Project

Before you can create a Google API key for the required Google Cloud Platform project, you must create and access the required project.

To create a Google Cloud project:

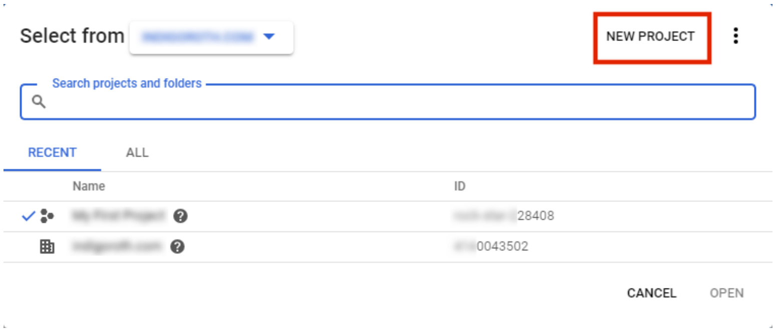
1. Access the Google Cloud Platform website (**https://cloud.google.com**) in your browser.
2. Log into your account.
3. Access the **Dashboard** tab for your account.
4. Click the down arrow next to your current project name. For example:

   FIGURE 279 Google Cloud Project Pull-Down



The **Select from** dialog appears. For example:

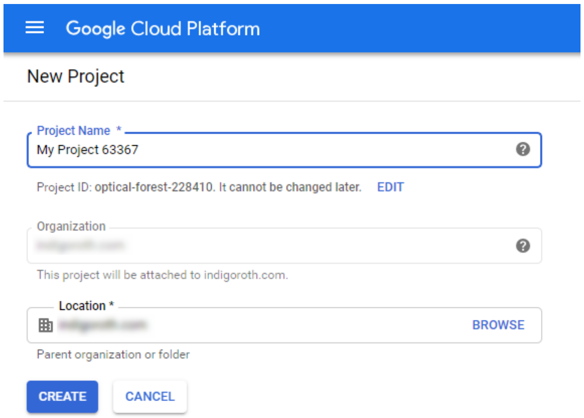
FIGURE 280 Google Cloud Select Project



Name	ID
✓	28408
	0043502

5. (Optional) Click **New Project**, complete the **New Project** page for your required project and click **Create**. For example:

FIGURE 281 Google Cloud New Project



Project Name * My Project 63367

Project ID: optical-forest-228410. It cannot be changed later.

Organization

This project will be attached to indigoroth.com.

Location *

Parent organization or folder

6. In the **Select From** dialog, select the required project and click **Open**.

7. The selected project appears in your Google Cloud Platform dashboard.

After you have opened the required project in your dashboard, you can generate the Google API key for the project, see **"Generating a Google API Key for a Project" on page 240**.

Generating a Google API Key for a Project

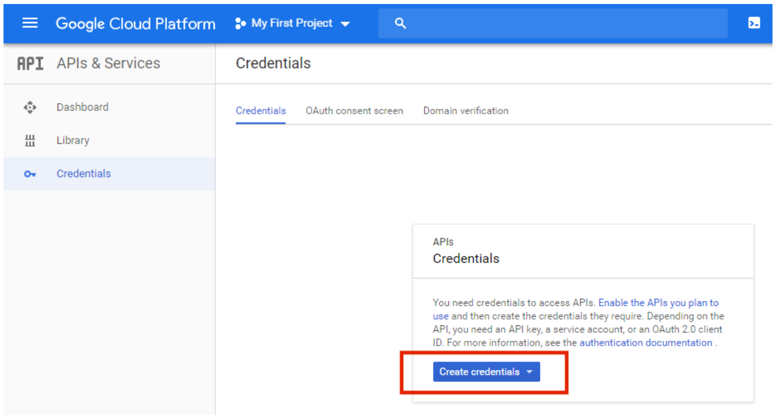
After you have enabled the Google Maps JavaScript API and opened the required Google Cloud Platform project, you can create the Google API key for the project.

To create a Google API key:

1. Access the **Dashboard** tab for your Google Cloud Platform account.
2. In the left menu, click **APIs & Services** and then click **Credentials**.

   The **APIs & Services Credentials** page appears. For example:

   FIGURE 282 Google Cloud Credentials

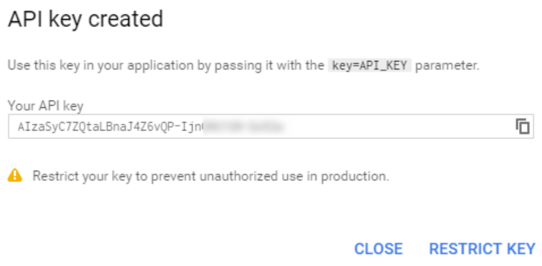
   

   You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. For more information, see the authentication documentation .

   In this example, there are no existing API keys in the current project.
3. Click the **Create credentials** pull-down menu and then select **API Key**.

   The **API key created** dialog appears. For example:

   FIGURE 283 Google Cloud API Key Created

   API key created

   Use this key in your application by passing it with the `key=API_KEY` parameter.

   Your API key
   AIzaSyC7ZQtaLBnaJ4Z6vQP-Ijn[redacted]

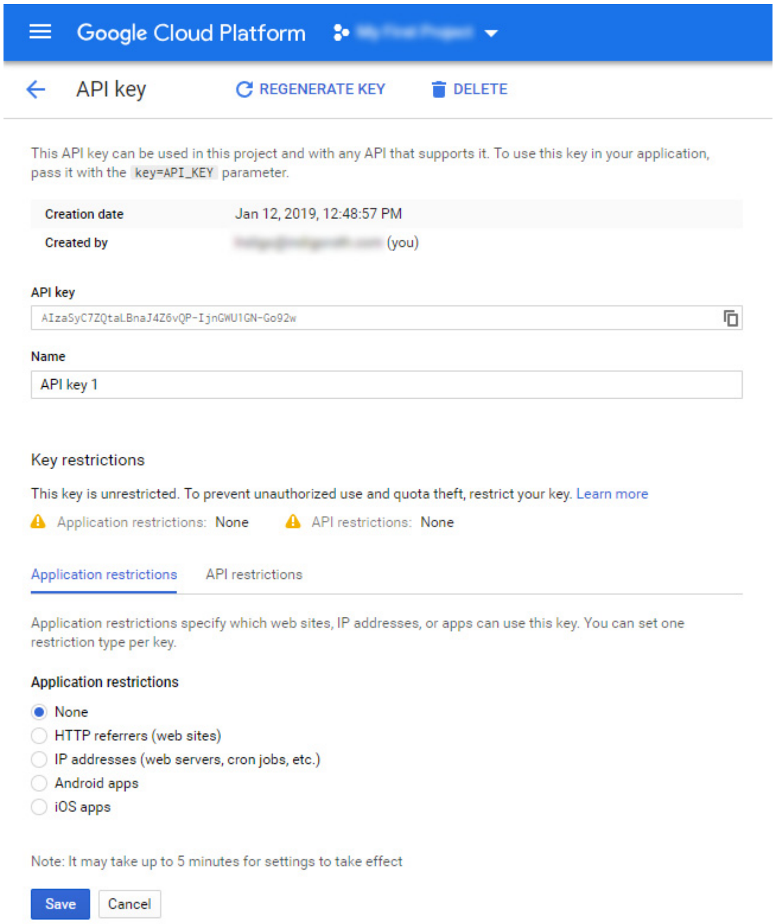
   ⚠ Restrict your key to prevent unauthorized use in production.

   CLOSE RESTRICT KEY
4. (Optional) Record **Your API key** and click **Close**.

   You can click **Copy** (⧉) to put the key into your browser clipboard for recording purposes.
5. (Optional) To restrict your API key to prevent unauthorized use and potential quota theft, click **Restrict Key**.

The **API key** page appears. For example:

FIGURE 284 Google Cloud API Key



This API key can be used in this project and with any API that supports it. To use this key in your application, pass it with the `key=API_KEY` parameter.

Creation date	Jan 12, 2019, 12:48:57 PM
Created by	[redacted] (you)

API key

AIzaSyC7ZQtaLBnaJ4Z6vQP-IjnGWU1GN-Go92w

Name

API key 1

Key restrictions

This key is unrestricted. To prevent unauthorized use and quota theft, restrict your key. Learn more

Application restrictions: None   API restrictions: None

Application restrictions specify which web sites, IP addresses, or apps can use this key. You can set one restriction type per key.

Application restrictions

- ● None
- ○ HTTP referrers (web sites)
- ○ IP addresses (web servers, cron jobs, etc.)
- ○ Android apps
- ○ iOS apps

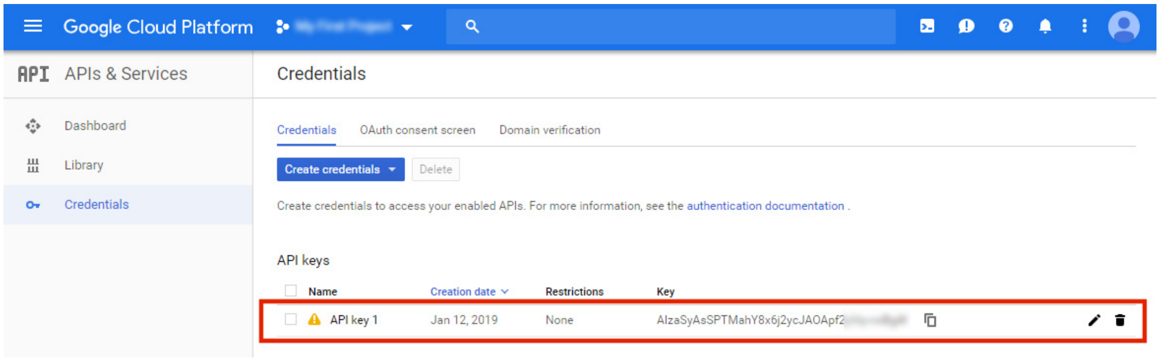
Note: It may take up to 5 minutes for settings to take effect

On this page, you can optionally perform any of the following:

- Specify a different **Name** for the API key.
- Click **Copy** (⧉) to put the key into your browser clipboard for recording purposes.
- Limit the use of the API at the application level by selecting the **Application restrictions** tab and specifying any required limitations.
- Limit the APIs that can be called using the key by selecting the **API restrictions** tab and specifying any required limitations. For example, if you want the API key to only be able to access the Map JavaScript API and no others, you can configure this requirement here.
- Click **Regenerate Key** to replace the current key, based on current criteria.
- Click **Delete** to remove the current key and close the dialog.
- Click **Save** to save the settings and close the dialog.

After you have created your API key, it is listed on the **Credentials** page. For example:

FIGURE 285 Google Cloud Credentials New API Key



Create credentials to access your enabled APIs. For more information, see the authentication documentation .

API keys

	Name	Creation date	Restrictions	Key
□	API key 1	Jan 12, 2019	None	AIzaSyAsSPTMahY8x6j2ycJAOApf2[redacted]

You can then use the API key to enable Pulse Workspace to render device locations using Google Maps, see **"Configuring Device Location" on page 242**.

Configuring Device Location

Perform the following steps to configure device location:

- **"Configuring Workspace Properties to Enable Device Location" on page 242**.
- **"Configuring a Policy to Support Device Location" on page 244**.
- **"Configuring a Device After Device Location is Enabled" on page 246**.

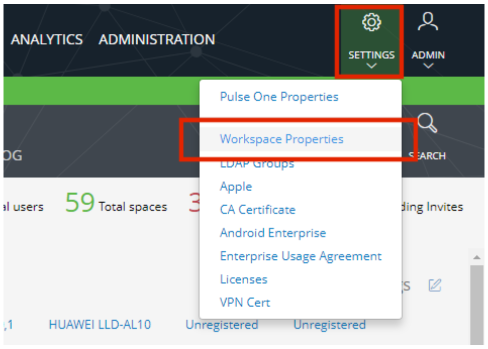
Note: Device location requires iOS v10 or later, or Android 8.0 or later.

Configuring Workspace Properties to Enable Device Location

To configure Pulse Workspace properties to support device location:

1. Start Pulse One.
2. Click the **Settings** icon on top-right corner of the page and select **Workspace Properties**.

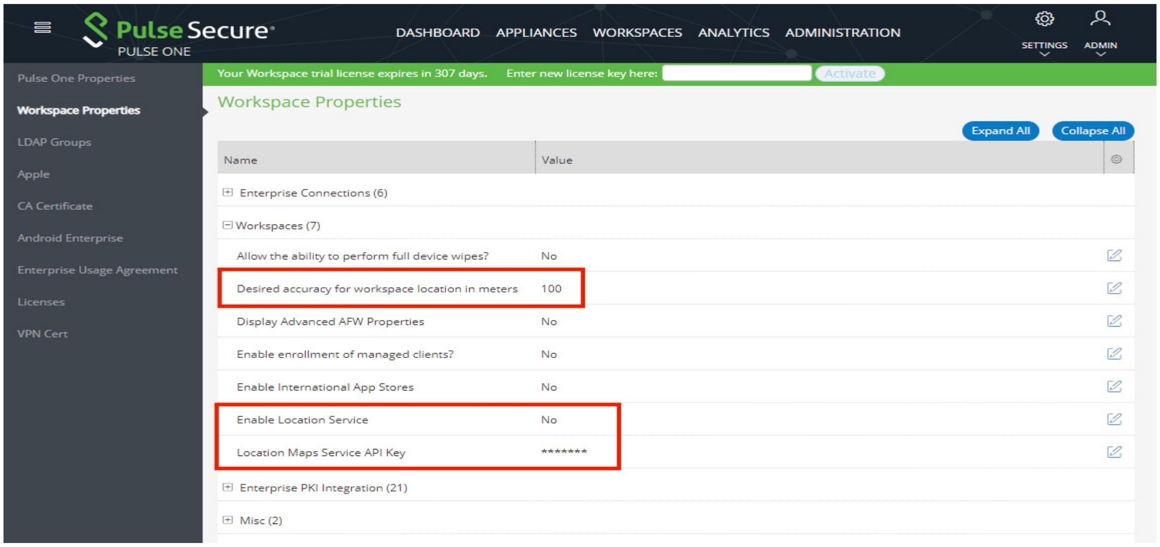
   FIGURE 286 Settings Menu

   The **Workspace Properties** page appears.

3. Expand the **Workspaces** group to view the **Enable Location Service** and **Location Maps Service API Key** properties. For example:

FIGURE 287 Workspace Properties



Your Workspace trial license expires in 307 days. Enter new license key here:

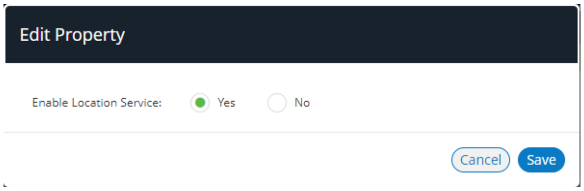
Workspace Properties

Name	Value
⊞ Enterprise Connections (6)	
⊟ Workspaces (7)	
Allow the ability to perform full device wipes?	No
Desired accuracy for workspace location in meters	100
Display Advanced AFW Properties	No
Enable enrollment of managed clients?	No
Enable International App Stores	No
Enable Location Service	No
Location Maps Service API Key	*******
⊞ Enterprise PKI Integration (21)	
⊞ Misc (2)	

4. Click the **Edit** button for the **Enable Location Service** property.

   The **Edit Property** dialog appears.

FIGURE 288 Enable Location Service Workspace Property



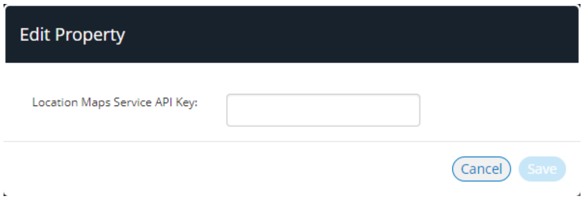
Enable Location Service: ● Yes ○ No

5. In the **Edit Property** dialog, set **Enable Location Service** to *Yes* and then click **Save**.

6. (Optional) If you have a Google API Key (see “Creating a Google API Key” on page 236, click the **Edit** button for the **Location Maps Service API Key** property.

   The **Edit Property** dialog appears.

FIGURE 289 Location Maps Service API Key Property



Location Maps Service API Key:

In this dialog, enter the **Location Maps Service API Key** and then click **Save**.

7. For iOS device location, ensure that the **Desired accuracy for workspace location in meters** workspace property is set to your required accuracy. The default is 100 meters. See **"Working with Policies" on page 164** and **"Workspaces" on page 182**.

   Note: This property is not used to locate Android devices. The location of Android devices is always the closest location using available network information.

The configuration of workspace properties to enable device location is now complete.

Next, you must configure the policy properties and push the policy to all devices that use it, see **"Configuring a Policy to Support Device Location" on page 244**.

Configuring a Policy to Support Device Location

After you have configured workspace properties to enable device location, you can request the location of any compatible device. The Pulse Client app on the device will prompt the user for permission to access the Location Service. The user will have the option to allow or deny access.

The following policy properties determine whether refusing the use of this service on a device makes the device non-compliant:

- **iOS Pulse Client Denied To Use Location Service**
- **Android Pulse Client Denied To Use Location Service**

For both of these properties, there are three supported compliance settings:

- *Allow*. If the user declines the location service, the device is flagged as non-compliant, but the user's access is not restricted.
- *Restrict VPN*. If the user declines the location service, the device is flagged as non-compliant, but access to the VPN from the device is restricted.
- *Wipe*. If the user declines the location service, the device is flagged as non-compliant, and the workspace will be wiped from the device.

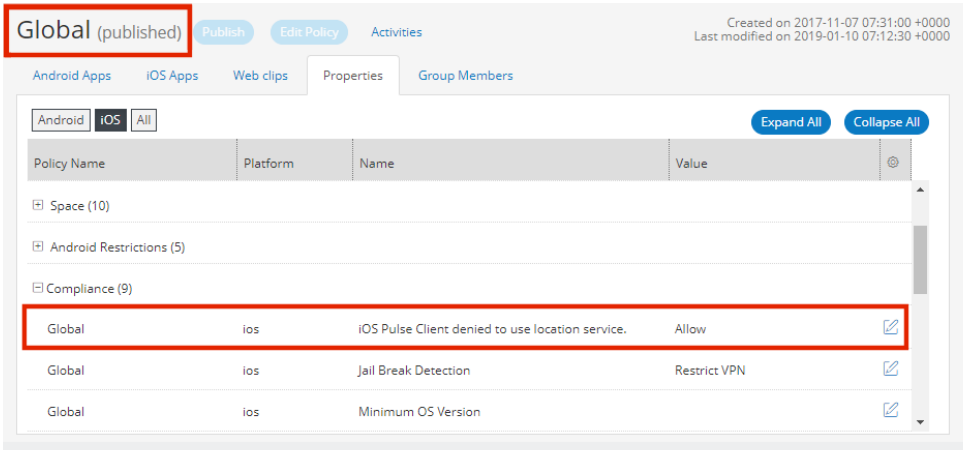
To set the required **Pulse Client Denied To Use Location Service** property for a policy:

1. Select the **Workspace** tab.
2. Select the **Policies** tab.
3. Select the required policy.
4. Click the **Properties** tab for the policy.
5. Expand the *Compliance* collection of policies.

6. Locate the required property. That is, either:
    - **iOS Pulse Client Denied To Use Location Service**, or
    - **Android Pulse Client Denied To Use Location Service**

    For example:

    FIGURE 290 iOS Denied To Use Location Service Property



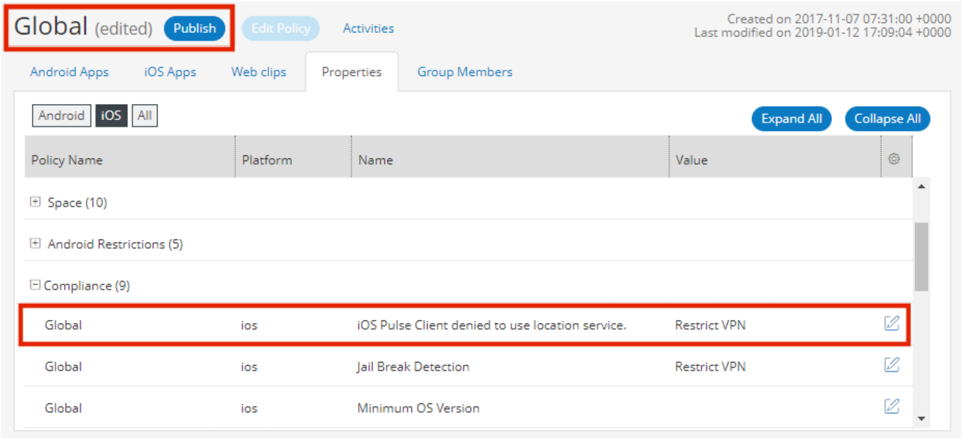
Created on 2017-11-07 07:31:00 +0000
Last modified on 2019-01-10 07:12:30 +0000

Policy Name	Platform	Name	Value
⊞ Space (10)			
⊞ Android Restrictions (5)			
⊟ Compliance (9)			
Global	ios	iOS Pulse Client denied to use location service.	Allow
Global	ios	Jail Break Detection	Restrict VPN
Global	ios	Minimum OS Version	

7. Click the **Edit** (✎) icon for the required property.
8. Make the required changes and click **Save**.

    The policy updates, and indicates that it has been edited. For example:

    FIGURE 291 Updated iOS Denied To Use Location Service Property



Created on 2017-11-07 07:31:00 +0000
Last modified on 2019-01-12 17:09:04 +0000

Policy Name	Platform	Name	Value
⊞ Space (10)			
⊞ Android Restrictions (5)			
⊟ Compliance (9)			
Global	ios	iOS Pulse Client denied to use location service.	Restrict VPN
Global	ios	Jail Break Detection	Restrict VPN
Global	ios	Minimum OS Version	

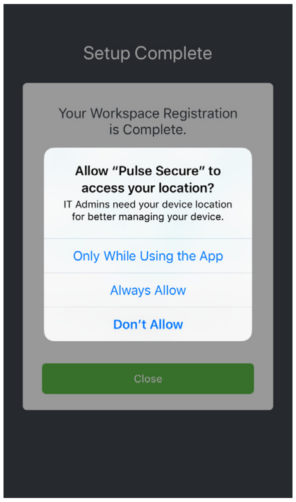
9. **Publish** the updated policy to implement it on all devices that use the policy.

The configuration of the policy is complete. The feature must then be enabled manually on each device that uses the policy, see **"Configuring a Device After Device Location is Enabled" on page 246**.

Configuring a Device After Device Location is Enabled

After you have updated a policy to support device location and published the policy to its devices, the Pulse Secure client on each device notifies the user about the device location feature. For example:

FIGURE 292 Pulse Secure Device Location



Setup Complete

Your Workspace Registration is Complete.

Allow "Pulse Secure" to access your location?

IT Admins need your device location for better managing your device.

The results of each choice depends on the **Android/iOS Pulse Client Denied To Use Location Service** policy property, see **"Configuring a Policy to Support Device Location" on page 244**.

- *Always Allow*. The location of the device can always be retrieved from the device by Pulse Workspace.

  The device is compliant for location policy.

- *Only While Using the App*. The location of the device can be retrieved by Pulse Workspace while the Pulse Secure client is running on the device.

  The device is always non-compliant for location policy.

- *Don't Allow*. The location of the device cannot be retrieved by Pulse Workspace.

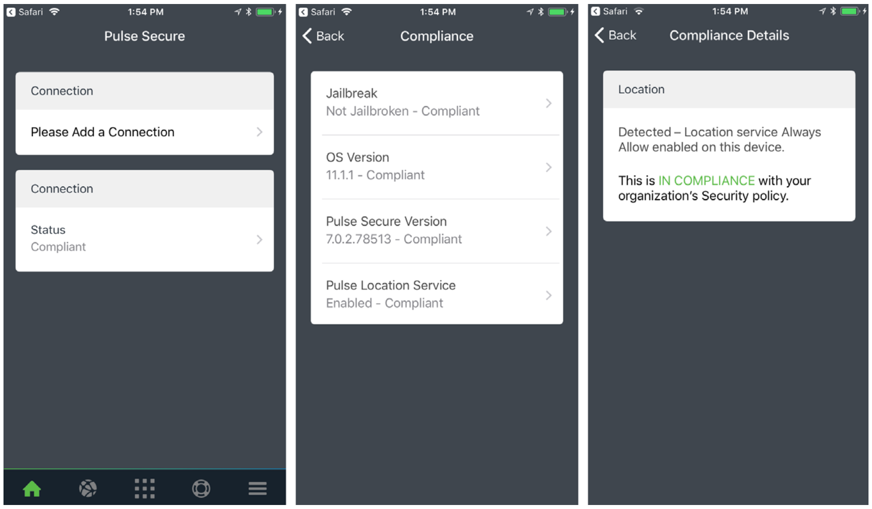
  The device is always non-compliant for location policy.

After a device user has confirmed that they allow the retrieval of their device location, Pulse Workspace can request the device location at any time, see **"Locating a Device" on page 249**.

The device location compliance status can be seen from the device:

- A compliant device (in this example, an iOS device) is shown below:

FIGURE 293 Pulse Secure Device Location Compliance



Pulse Secure

Connection

Please Add a Connection

Connection

Status
Compliant

Compliance

Jailbreak
Not Jailbroken - Compliant

OS Version
11.1.1 - Compliant

Pulse Secure Version
7.0.2.78513 - Compliant

Pulse Location Service
Enabled - Compliant

Compliance Details

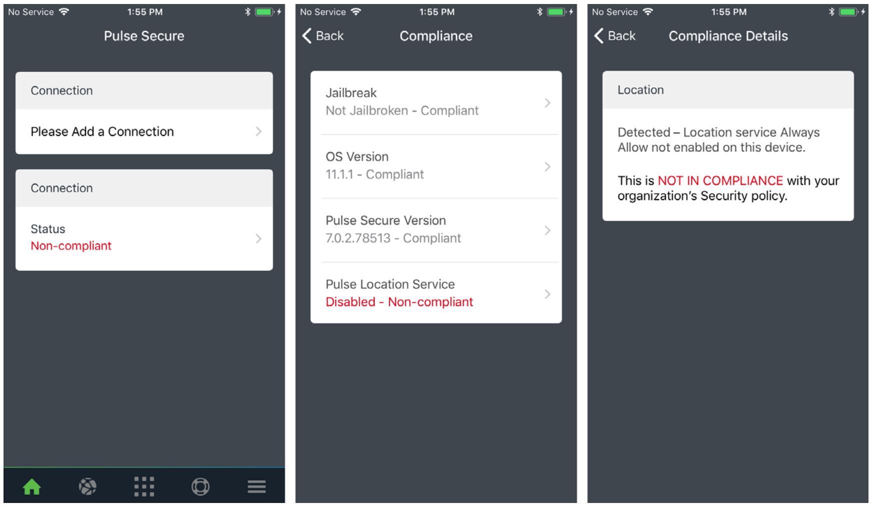
Location

Detected – Location service Always Allow enabled on this device.

This is IN COMPLIANCE with your organization's Security policy.

- A non-compliant device (in this example, an iOS device) is shown below:

FIGURE 294 Pulse Secure Device Location Non-Compliance



Pulse Secure

Connection

Please Add a Connection

Connection

Status
Non-compliant

Compliance

Jailbreak
Not Jailbroken - Compliant

OS Version
11.1.1 - Compliant

Pulse Secure Version
7.0.2.78513 - Compliant

Pulse Location Service
Disabled - Non-compliant

Compliance Details

Location

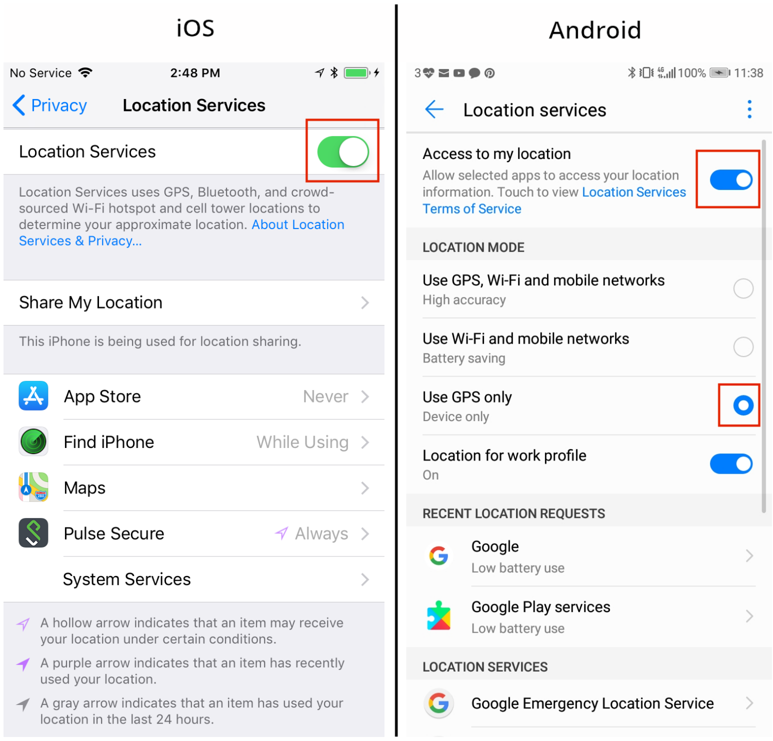
Detected – Location service Always Allow not enabled on this device.

This is NOT IN COMPLIANCE with your organization's Security policy.

To enable/disable the Device Location feature:

- For iOS devices, use the **Location Services** switch in the iOS Privacy Settings for Location Services.
- For Android devices, use the **Access to my location switch** in the Google > Location settings.

FIGURE 295 iOS and Android Device Location Services Switch



iOS

No Service 2:48 PM

Privacy Location Services

Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Share My Location

This iPhone is being used for location sharing.

App Store Never

Find iPhone While Using

Maps

Pulse Secure Always

System Services

A hollow arrow indicates that an item may receive your location under certain conditions.

A purple arrow indicates that an item has recently used your location.

A gray arrow indicates that an item has used your location in the last 24 hours.

Android

100% 11:38

Location services

Access to my location
Allow selected apps to access your location information. Touch to view Location Services Terms of Service

LOCATION MODE

Use GPS, Wi-Fi and mobile networks
High accuracy

Use Wi-Fi and mobile networks
Battery saving

Use GPS only
Device only

Location for work profile
On

RECENT LOCATION REQUESTS

Google
Low battery use

Google Play services
Low battery use

LOCATION SERVICES

Google Emergency Location Service

Once location services are enabled, you must also ensure that the location services are set to use GPS or (optionally) GPS with mobile networks. The location of a device cannot be determined using WiFi only. The device will be flagged as non-compliant unless GPS is enabled for device location.

Note: When **Location Services** is enabled, you can update the current **Allow Location Access** setting in the Pulse Secure Client App Location Services settings.

Locating a Device

After a device user has confirmed that they allow the retrieval of their device location, Pulse Workspace can request the device location at any time.

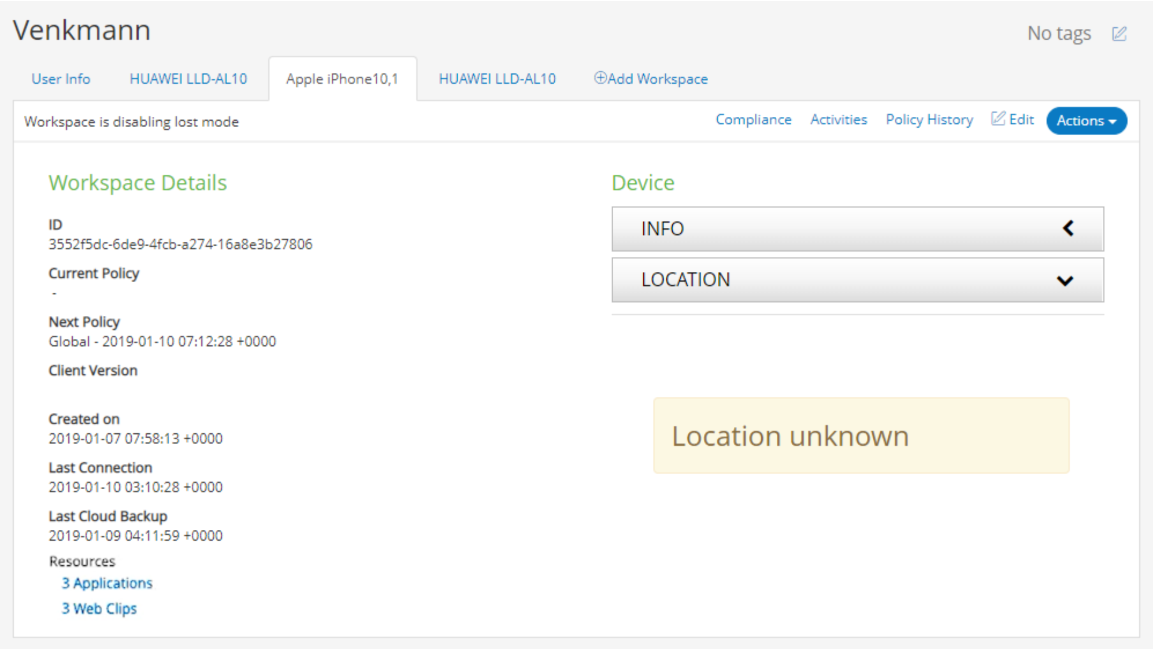
Note: Device location requires iOS v10 or later, or Android 8.0 or later.

To retrieve a device location:

1. Log into Pulse Workspace.
2. Select the **Workspaces** menu.
3. Select the **Devices** tab.
4. Select the required user and device.

   The **Workspace Details** for the device appears. For example:

   FIGURE 296 iOS Device Location Unknown



Workspace is disabling lost mode

Workspace Details

ID
3552f5dc-6de9-4fcb-a274-16a8e3b27806

Current Policy
-

Next Policy
Global - 2019-01-10 07:12:28 +0000

Client Version

Created on
2019-01-07 07:58:13 +0000

Last Connection
2019-01-10 03:10:28 +0000

Last Cloud Backup
2019-01-09 04:11:59 +0000

Resources
3 Applications
3 Web Clips

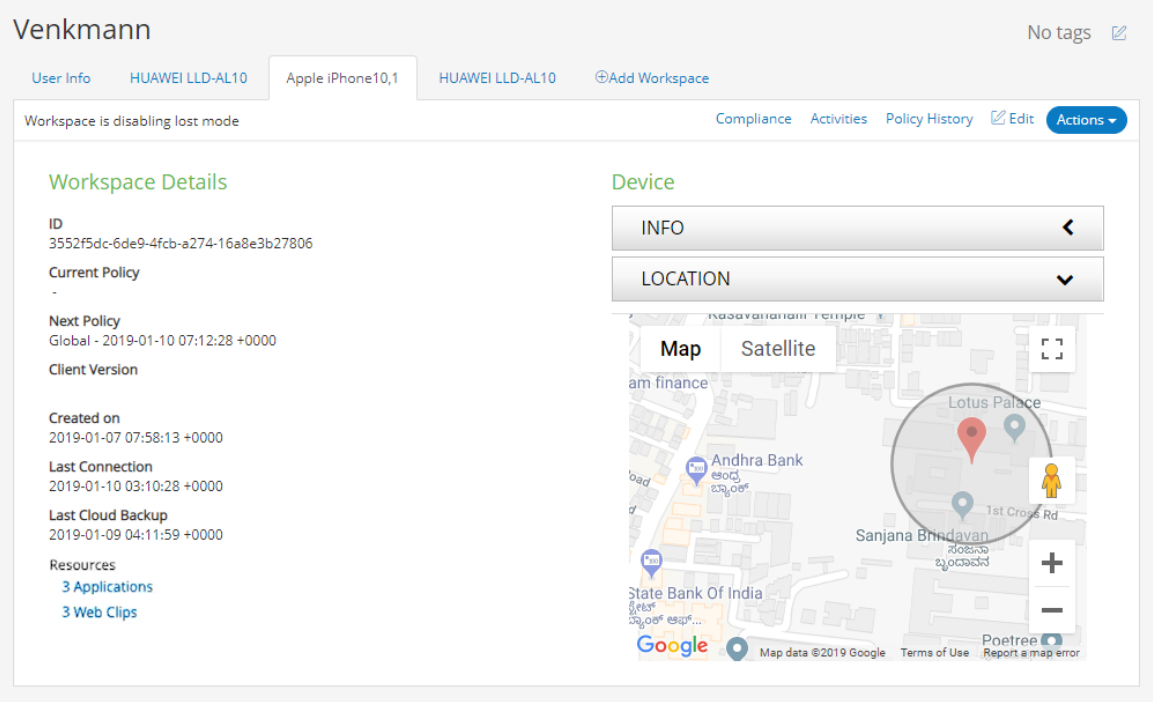
Location unknown

   In this example, no device location has yet been retrieved.

5. Click the **Actions** pull-down menu and select **Update Location**.

The device location request is sent. After it is retrieved, the device location appears. For example:

FIGURE 297 iOS Device Location Retrieved



Workspace is disabling lost mode

Workspace Details

ID
3552f5dc-6de9-4fcb-a274-16a8e3b27806

Current Policy
-

Next Policy
Global - 2019-01-10 07:12:28 +0000

Client Version

Created on
2019-01-07 07:58:13 +0000

Last Connection
2019-01-10 03:10:28 +0000

Last Cloud Backup
2019-01-09 04:11:59 +0000

Resources
3 Applications
3 Web Clips

Working with Lost Mode for a Device

Note: Lost Mode is only supported on Supervised iOS devices at version 10 or later.

In the event that a mobile device is lost, you can perform the following actions to secure the device and then assist with its recovery:

1. Enable Lost Mode for the device. This locks the device and displays a recovery message on the device.
2. Play a continuous loud tone on the lost device to assist in the search.
3. Request the geographical location of the lost device (where supported) to assist in the search.

After the owner has their device, Lost Mode can be canceled and the device can be used as usual.

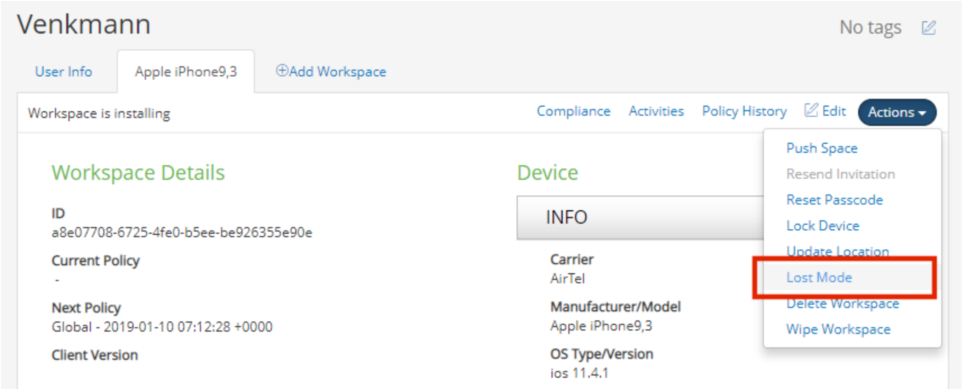
To enable Lost Mode for a device:

1. Log into Pulse Workspace.
2. Select the **Workspaces** menu.
3. Select the **Devices** tab.
4. Select the required user and device.

   The **Workspace Details** for the device appears.

5. In the **Actions** pull-down menu for the device, select **Lost Mode**:

FIGURE 298 iOS Device Actions Lost Mode



Venkmann

Workspace is installing

Workspace Details

ID
a8e07708-6725-4fe0-b5ee-be926355e90e

Current Policy
-

Next Policy
Global - 2019-01-10 07:12:28 +0000

Client Version

Device

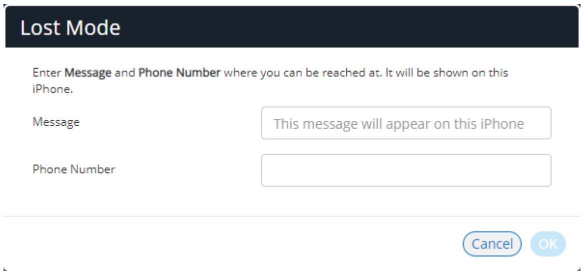
Carrier
AirTel

Manufacturer/Model
Apple iPhone9,3

OS Type/Version
ios 11.4.1

The **Lost Mode** dialog appears:

FIGURE 299 Lost Mode



Lost Mode

Enter **Message** and **Phone Number** where you can be reached at. It will be shown on this iPhone.

Message: This message will appear on this iPhone

Phone Number:

6. Enter a **Message** and a **Phone Number** to be displayed on the lost device, and click **OK**.

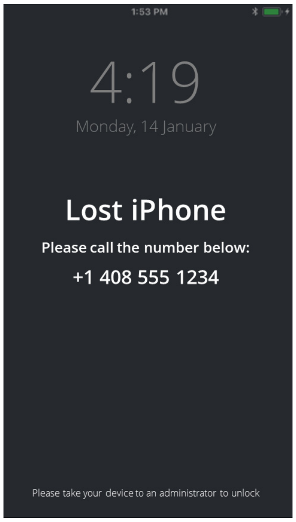
   A confirmation message appears.

7. Confirm the confirmation message.

   The device enters Lost Mode.

The lost device becomes locked, and displays the **Message** and **Phone Number**. For example:

FIGURE 300 Lost iPhone Message



1:53 PM

4:19

Monday, 14 January

Lost iPhone

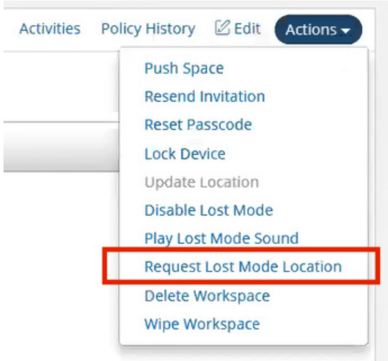
Please call the number below:

+1 408 555 1234

Please take your device to an administrator to unlock

8. (Optional) To request the location of a lost device, select the **Actions** pull-down menu for the device and then select **Request Lost Mode Location**.

FIGURE 301 Request Lost Mode Location



The **Devices Location** map updates when the device location is received.

9. (Optional) To play a loud continuous tone on the device to assist in its recovery, select the **Actions** pull-down menu for the device and then select **Play Lost Mode Sound**.

10. After the owner has their device, you can cancel Lost Mode. To do this, select the **Actions** pull-down menu for the device and then select **Disable Lost Mode**.

Viewing Analytics

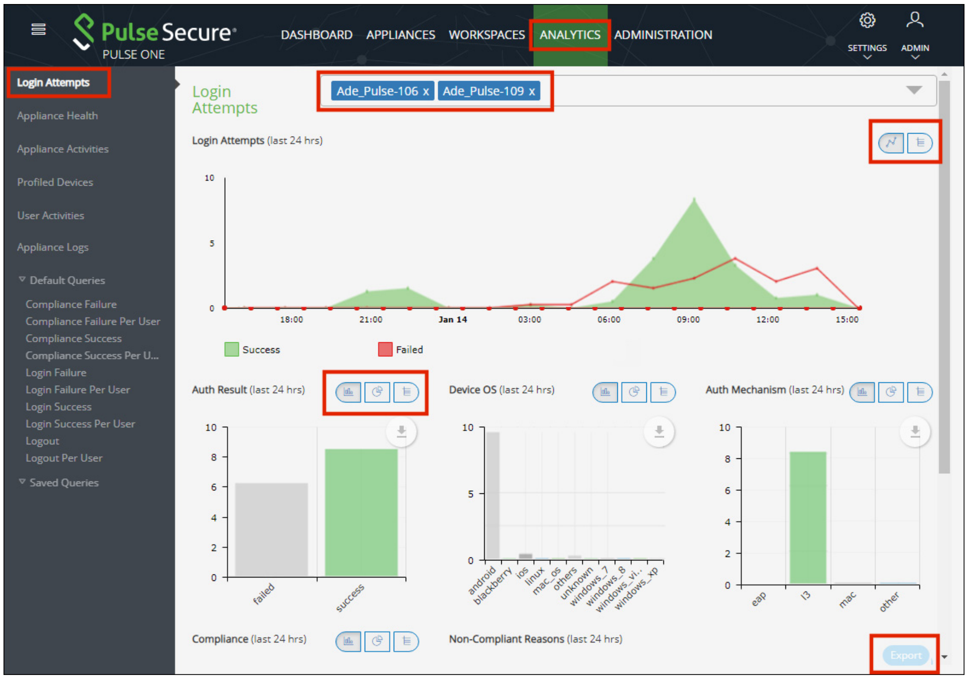
Viewing the Login Attempts Report

To view the **Login Attempts** report:

1. Select the **Analytics** menu.
2. Select **Login Attempts**.
3. From the **Login Attempts** drop-down, select one or more appliances for the report.
4. Select the graph type.

   The report shows the login attempts, authentication mechanism and result, and device OS in the last 24 hours.

   FIGURE 302 Login Attempts Report



5. (Optional) Choose bar chart, line graph, pie chart or table data for each graph.
6. (Optional) Click **Export** to download displayed information as a *.csv* format file.

Viewing the Appliance Health Report

To view the **Appliance Health** report:

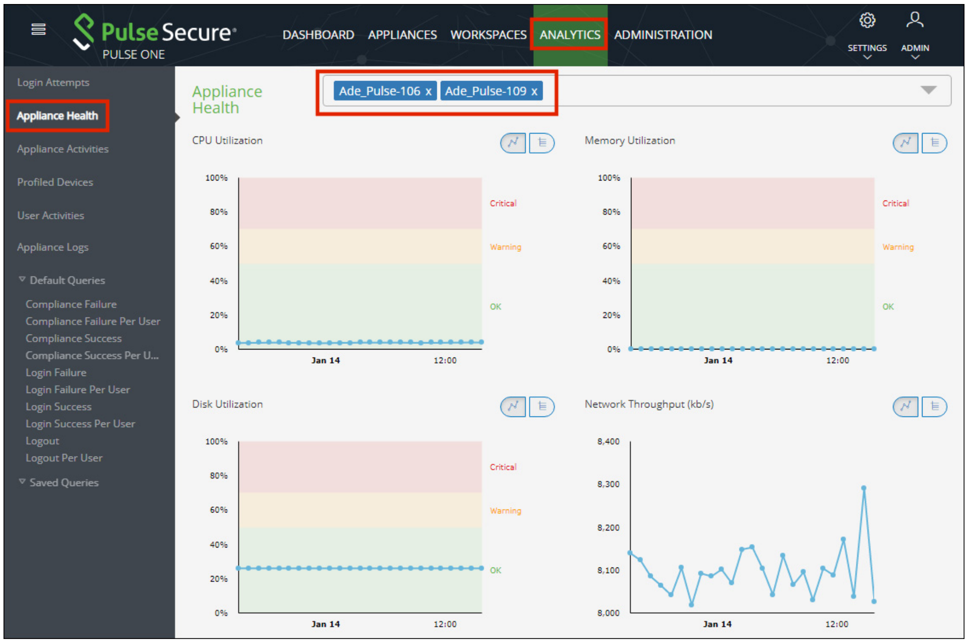
1. Select the **Analytics** menu.
2. Select **Appliance Health**.
3. From the **Appliance Health** drop-down, select one or more appliances for the report.

   The following reports for the selected appliance over the last 24 hours are displayed:

   - **CPU Utilization**
   - **Memory Utilization**
   - **Disk Utilization**
   - **Network Throughput (kb/s)**

   For example:

FIGURE 303 Appliance Health Report



Appliance Health: Ade_Pulse-106 x Ade_Pulse-109 x

Viewing the Appliance Activities Report

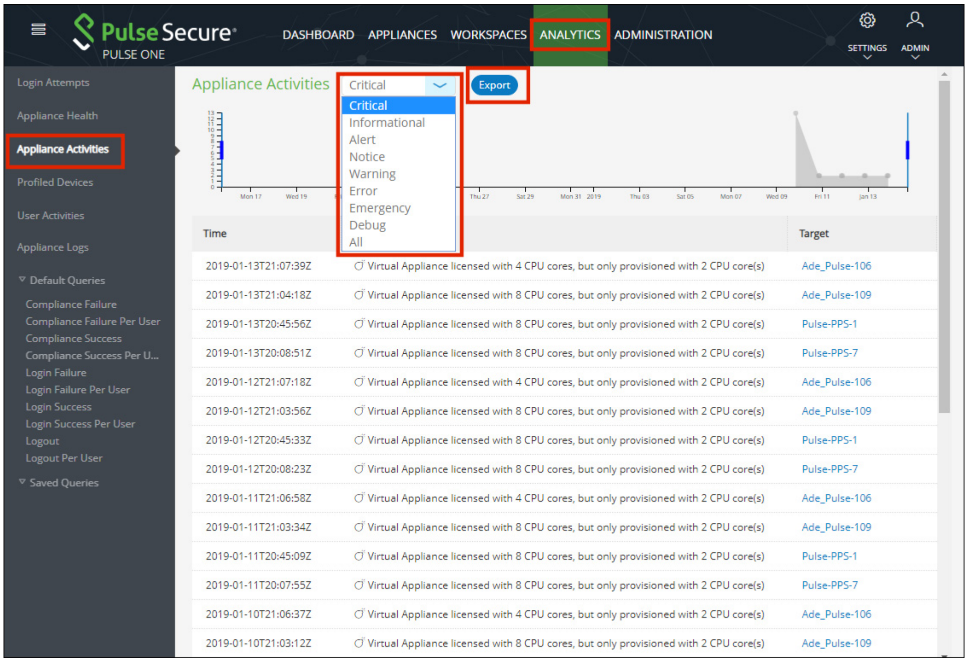
To view the **Appliance Activities** report:

1. Select the **Analytics** menu.

2. Select **Appliance Activities**.

3. From the **Appliance Activities** drop-down, select the filter (*Critical*, *Alert*, *Notice*, and so on) for the report.

FIGURE 304 Appliance Activities



Time		Target
2019-01-13T21:07:39Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106
2019-01-13T21:04:18Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-109
2019-01-13T20:45:56Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-1
2019-01-13T20:08:51Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-7
2019-01-12T21:07:18Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106
2019-01-12T21:03:56Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-109
2019-01-12T20:45:33Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-1
2019-01-12T20:08:23Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-7
2019-01-11T21:06:58Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106
2019-01-11T21:03:34Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-109
2019-01-11T20:45:09Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-1
2019-01-11T20:07:55Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-7
2019-01-10T21:06:37Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106
2019-01-10T21:03:12Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-109

4. (Optional) Click **Export** to download displayed information as a *.csv* format file.

Viewing the App Visibility Report

To view the **App Visibility** report:

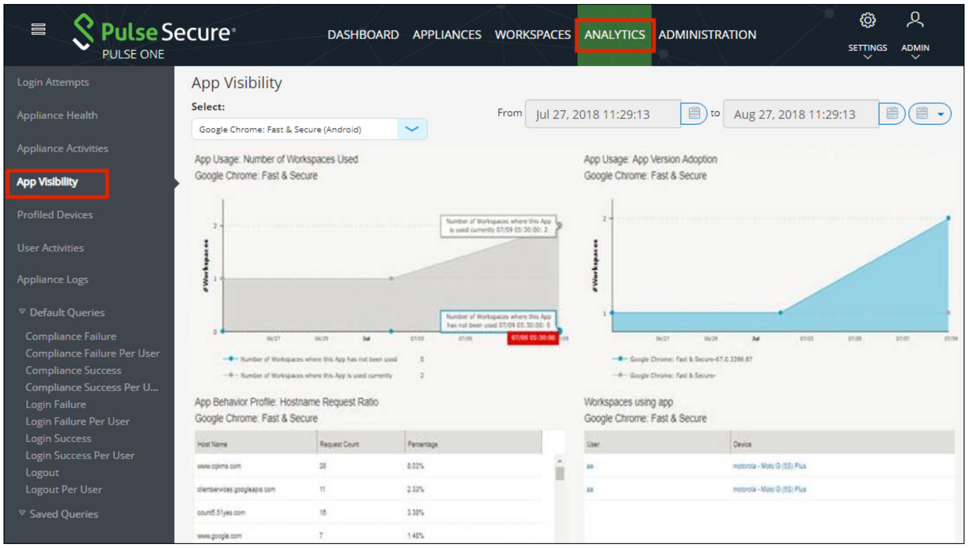
1. Select the **Analytics** menu.
2. Select **App Visibility**.
3. From the **App Visibility** drop-down, select an app.
4. Select a time range for the report. To do this, click the calendar (📅) and then either:
   - Select a fixed duration for the report by selecting *Last Day*, *Last 7 Days*, or *Last 30 Days*. OR
   - Select a range duration for the report by selecting *Custom Range*. Then, specify a **From** and **To** timestamp for the report.

   The following reports for the selected app and time range are displayed:

   - **App Usage: Number of Workspaces Used** – This displays the number of devices that have the app installed, and the number where the app is in use.
   - **App Usage: App Version Adoption** – This displays the number of devices that have the app installed at different version numbers.
   - **App Profile Behavior: Hostname Request Ratio** – This displays a pie chart that shows how the requests are divided among different hostnames.

   For example:

FIGURE 305 App Visibility Report


Pulse Secure
PULSE ONE
DASHBOARD
APPLIANCES
WORKSPACES
ANALYTICS
ADMINISTRATION
SETTINGS
ADMIN
Login Attempts
Appliance Health
Appliance Activities
App Visibility
Profiled Devices
User Activities
Appliance Logs
Default Queries
Compliance Failure
Compliance Failure Per User
Compliance Success
Compliance Success Per U...
Login Failure
Login Failure Per User
Login Success
Login Success Per User
Logout
Logout Per User
Saved Queries
App Usage: Number of Workspaces Used
Google Chrome: Fast & Secure
#Workspaces
Number of Workspaces where this App is used currently 07/09 05:30:00: 2
Number of Workspaces where this App has not been used 07/09 05:30:00: 0
07/09 05:30:00
Number of Workspaces where this App has not been used 0
Number of Workspaces where this App is used currently 2
App Usage: App Version Adoption
Google Chrome: Fast & Secure
#Workspaces
Google Chrome: Fast & Secure-67.0.3396.87
Google Chrome: Fast & Secure-

App Visibility

Select: Google Chrome: Fast & Secure (Android)

From Jul 27, 2018 11:29:13 to Aug 27, 2018 11:29:13

App Behavior Profile: Hostname Request Ratio
Google Chrome: Fast & Secure

Host Name	Request Count	Percentage
www.cqkms.com	38	8.03%
clientservices.googleapis.com	11	2.33%
count5.51yes.com	16	3.38%
www.google.com	7	1.48%

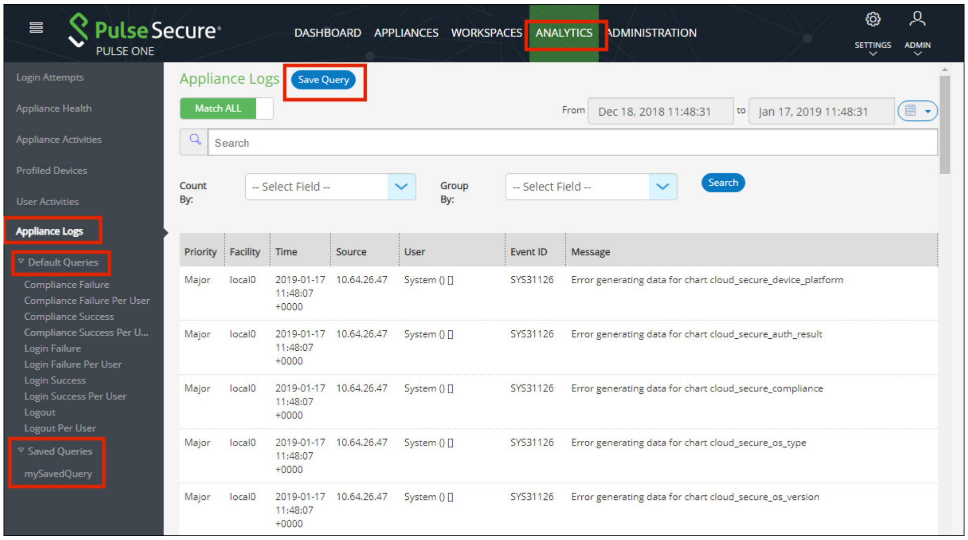
Workspaces using app
Google Chrome: Fast & Secure

User	Device
aa	motorola - Moto G (5S) Plus
aa	motorola - Moto G (5S) Plus

Viewing Log Aggregation and Analysis

The syslog forwarded from the configured PCS/PPS appliances can be viewed in Appliance Logs. Here, users have a consolidated view of logs generated by every PPS/PCS appliance that is configured to forward its syslogs to the Pulse One server.

FIGURE 306 Appliance Logs



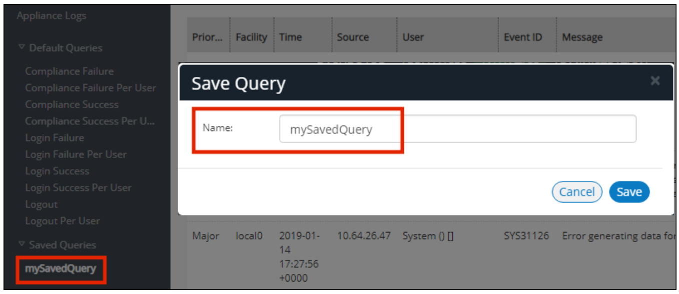
From Dec 18, 2018 11:48:31 to Jan 17, 2019 11:48:31

Priority	Facility	Time	Source	User	Event ID	Message
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_device_platform
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_auth_result
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_compliance
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_type
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_version

The system provides a set of Default Queries below the Appliance Logs menu in the navigation panel. Administrator can also customize the queries and save them for future use. These customized queries are listed below **Saved Queries**.

The Appliance Logs page allows searching by a string token by typing in the token in the search bar or double-clicking a string in the logs details. The view is then filtered to display all messages with the token that is being searched for. Users can enter multiple tokens separated by space. This customized query can then be saved using the **Save Query** feature.

FIGURE 307 Save Query



Name: mySavedQuery

Prior...	Facility	Time	Source	User	Event ID	Message
Major	local0	2019-01-14 17:27:56 +0000	10.64.26.47	System () []	SYS31126	Error generating data fo

To view logs from any of the system default queries, expand **Default Queries** and click on the query.

To view logs from the customized queries, expand **Saved Queries** and click on the query.

It is also possible to filter the logs by timestamp. This can be done by choosing a **From date** and **To date** in the date fields on the top right.

Users can also choose to filter search results by **Match All** (will display search results that have all tokens searched for) or **Match Any** (will display search results that include any of the tokens searched for).

The number of search results to be displayed on the screen can be 50, 100, 250, 500 by making a choice on the bottom left corner of the page. Finally, the search results can span over multiple pages and navigated using the buttons on the bottom right corner of the page.

Note: Only the saved queries can be deleted using the **Delete Query** feature.

User Administration

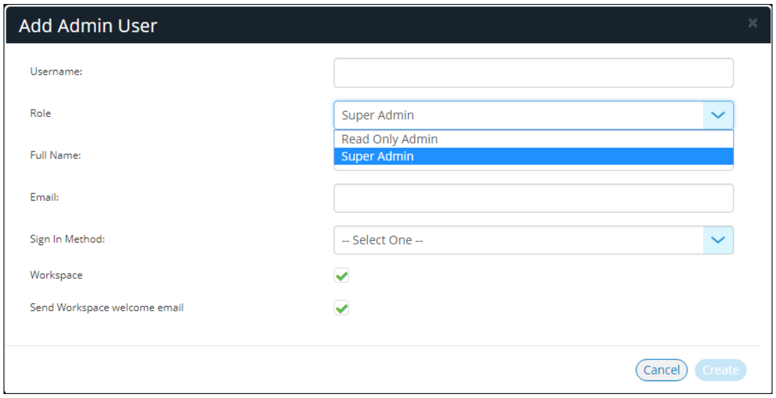
Adding an Admin User

To add an admin user:

1. Select the **Administration** menu.
2. Select **User Management**.

   A list of existing admin users is displayed.
3. Click **Add User** to add an admin user.
4. In the **Add Admin User** window, enter the user details.
5. Select the required **Role** from the drop-down list – *Super Admin*, *Read Only Admin.*
6. Select the **Workspace** check box to provide the link to user's workspace.
7. Select the **Send Workspace welcome email** check box to send an email confirmation to the user about the creation of Workspace.
8. Click **Create**. The new user will be displayed in the User's list.

FIGURE 308 Add Admin User



Add Admin User

Username:

Role: Super Admin

Full Name:

Email:

Sign In Method: -- Select One --

Workspace ☑

Send Workspace welcome email ☑

Note: If Role is set to **Read Only Admin**, then the user will not be given the permissions to create/update/delete functions.

Modifying User Details

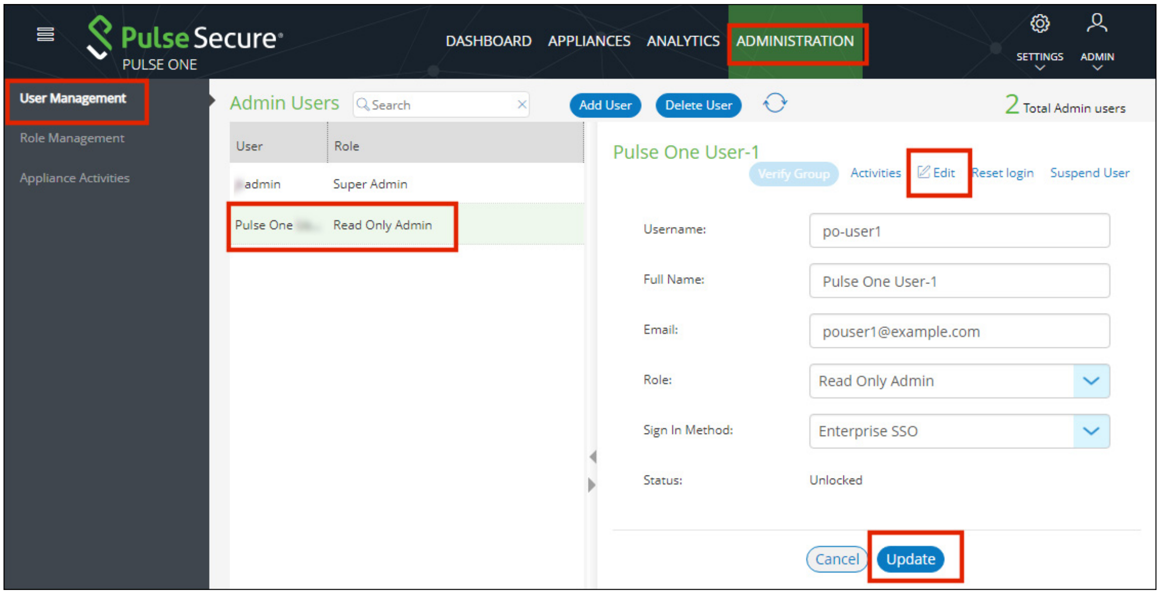
To modify an admin user's details:

1. Select the **Administration** menu.
2. Select **User Management**.

   A list of existing admin users is displayed.
3. Select the user from the list.
4. Click **Edit** and make the required changes.
5. Click **Update**.

For example:

FIGURE 309 Edit User Details



Username: po-user1

Full Name: Pulse One User-1

Email: pouser1@example.com

Role: Read Only Admin

Sign In Method: Enterprise SSO

Status: Unlocked

Removing an Admin User

To remove an admin user:

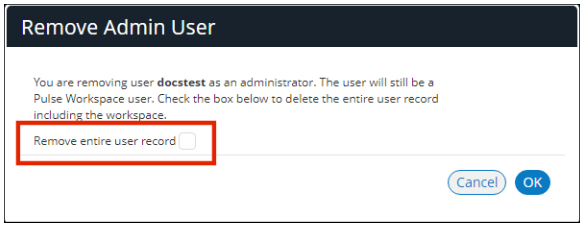
1. Select the **Administration** menu.
2. Select **User Management**.

   A list of existing admin users is displayed.
3. Select the user from the list and click **Delete User**.

   The **Remove Admin User** dialog appears. By default, this dialog will enable you to remove a user from the list of admin users.

4. (Optional) In order to remove the user from Pulse Workspace completely, select the **Remove entire user record** check box.

FIGURE 310 Remove Admin User



Remove Admin User

You are removing user **docstest** as an administrator. The user will still be a Pulse Workspace user. Check the box below to delete the entire user record including the workspace.

Remove entire user record □

5. Click **OK.**

Resetting a User Password

To reset a user's password:

1. Select the user from the list and click the **Reset login** link in the user details panel. An email that contains the **Set new password** link will be sent to your registered mail id.

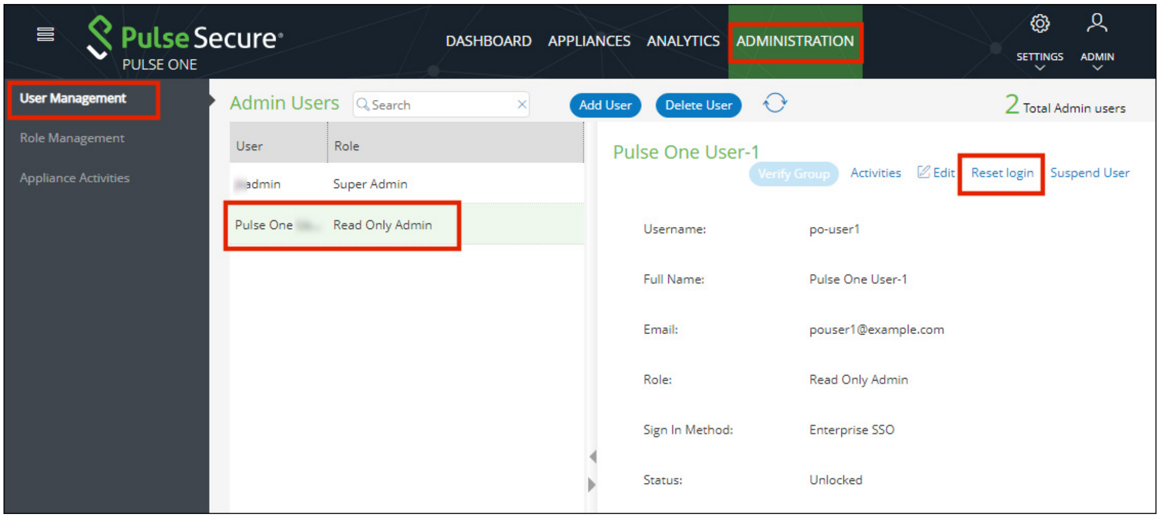
2. Click the **Set new password** link in the mail.

3. In the Pulse One page that appears, provide the new password and confirm the new password. The new password will be saved in the database.

4. Then log in to Pulse One with the new password.

   Note: The **Set new password** link that you received in the email has an expiration time of 1 hour. Beyond this time, you will have to make a new request for setting new password.

FIGURE 311 Reset Login



User	Role
admin	Super Admin
Pulse One	Read Only Admin

Pulse One User-1

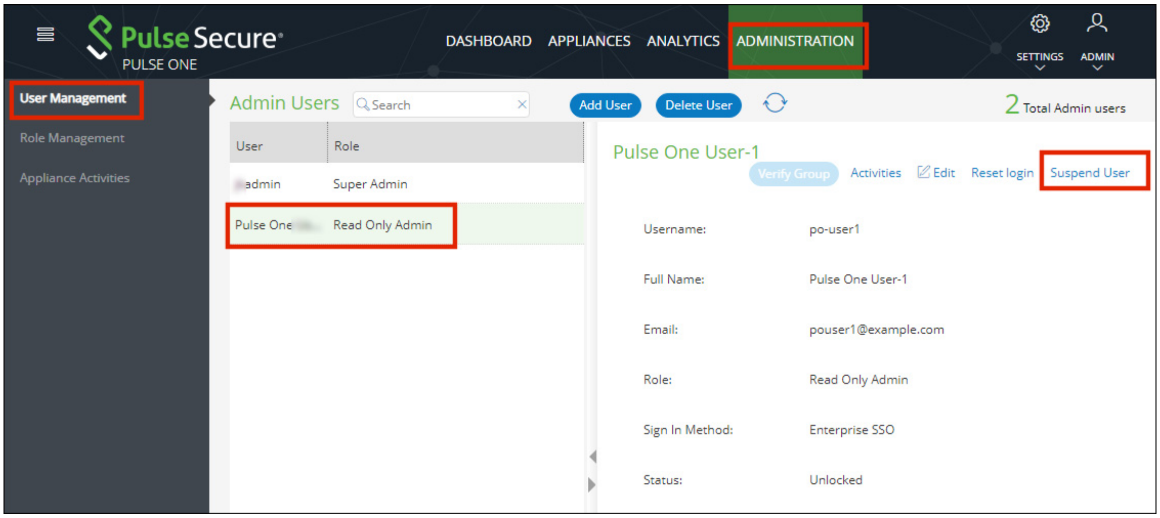
Username:	po-user1
Full Name:	Pulse One User-1
Email:	pouser1@example.com
Role:	Read Only Admin
Sign In Method:	Enterprise SSO
Status:	Unlocked

Suspending a User

To suspend a user, select the user from the list and click **Suspend User**. The user will be locked and will not be able to log into admin console. The Forgot Password option in the Login page will not send mail to reset password.

To unlock the suspended user, select the user and click **Reset Login**. This will send a mail to the user with a set new password link.

FIGURE 312 Suspend User



User	Role
[redacted]admin	Super Admin
Pulse One [redacted]	Read Only Admin

Pulse One User-1

Username:	po-user1
Full Name:	Pulse One User-1
Email:	pouser1@example.com
Role:	Read Only Admin
Sign In Method:	Enterprise SSO
Status:	Unlocked

Role Management

Adding Admin-Defined Roles

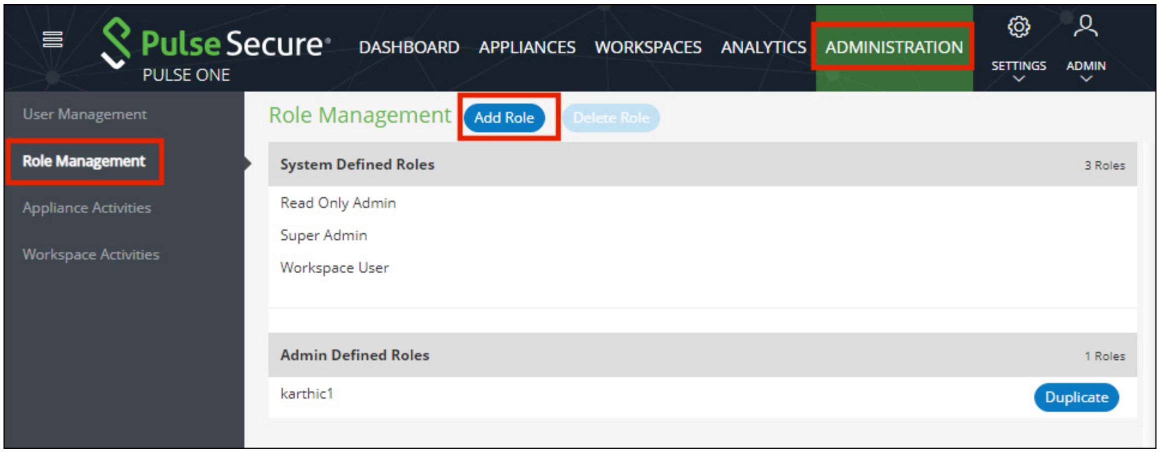
An admin-defined role can be created manually, or by duplicating an existing role.

To add a new role:

1. Select the **Administration** menu.
2. Select **Role Management**.

   A list of system defined roles appears.
3. Click **Add Role** to add a new admin defined role.

   FIGURE 313 Add Role

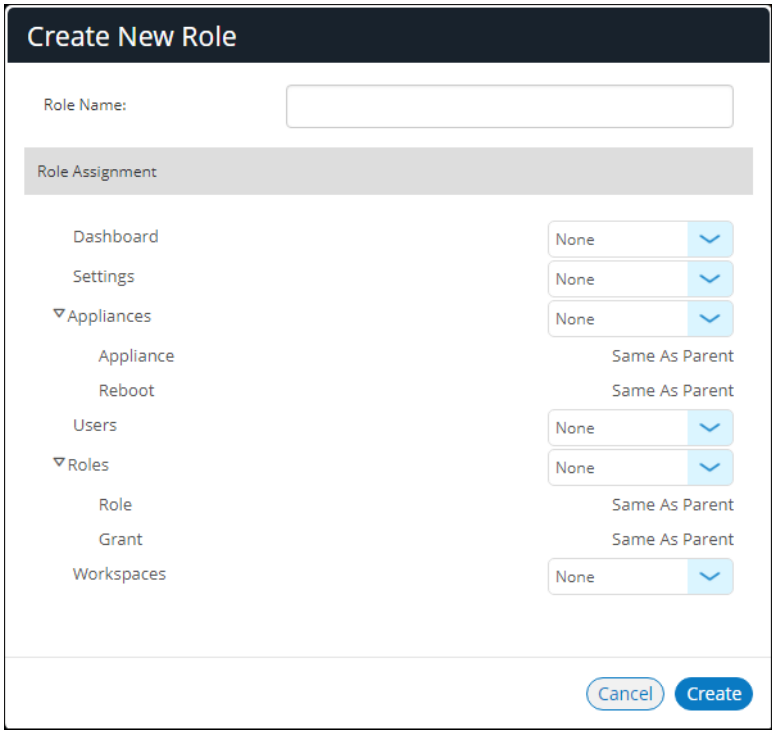


System Defined Roles	3 Roles
Read Only Admin	
Super Admin	
Workspace User	

Admin Defined Roles	1 Roles
karthic1	

The **Create New Role** dialog appears.

FIGURE 314 Create New Role



Create New Role

Role Name:

Role Assignment

Dashboard	None
Settings	None
▽Appliances	None
Appliance	Same As Parent
Reboot	Same As Parent
Users	None
▽Roles	None
Role	Same As Parent
Grant	Same As Parent
Workspaces	None

4. Enter the **Role Name**.
5. In the Role Assignment section, select the permissions for Dashboard, Appliances, Settings, Users, and Roles from the drop-down list. Supported permission are:
    - *None* – This permission will disable the assigned feature. For example, if **Appliances** permission is set to *None*, then **Appliances** page will not be visible in Pulse One console for this role.
    - *Read Only* – This permission will disable create/edit/delete options for the assigned feature.
    - *Edit* – This permission allows create/view/edit operations.
    - *Delete* – This permission allows all operations.
6. Click **Create**.

   The duplicated admin role is added to the list of admin roles.

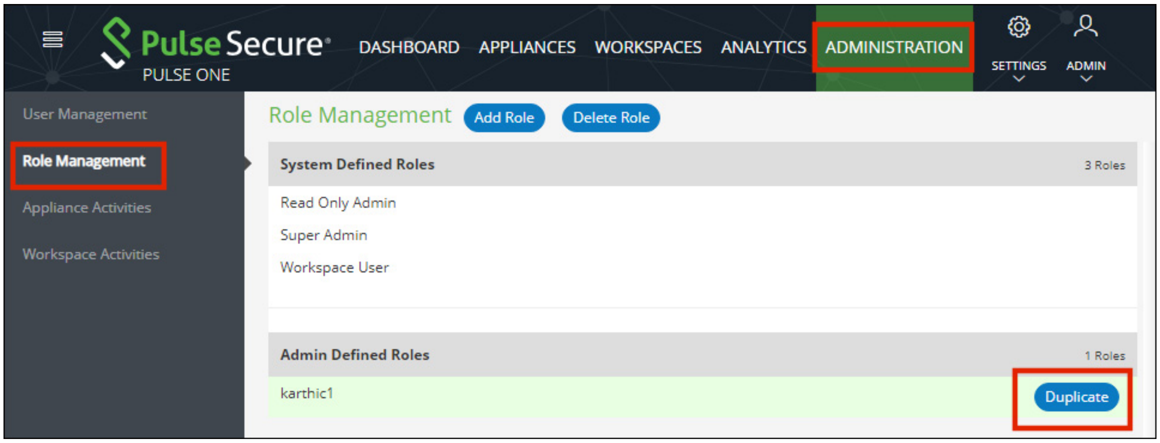
To duplicate an existing role:

1. Select the **Administration** menu.
2. Select **Role Management**.

   A list of system defined roles appears.

3. Click **Add Role** to add a new admin defined role.
4. Click **Duplicate Role** to add a new admin defined role.

FIGURE 315 Duplicate a Role



Role Management

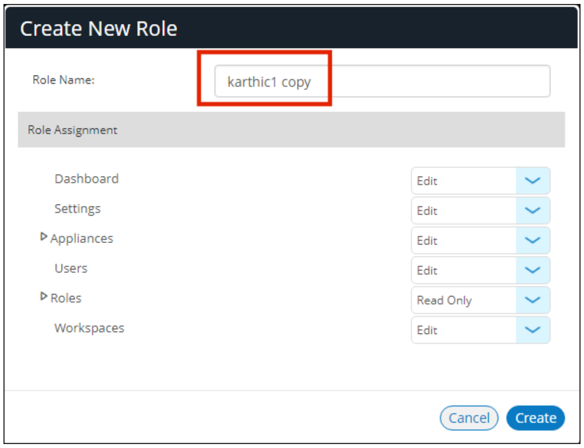
System Defined Roles	3 Roles
Read Only Admin	
Super Admin	
Workspace User	

Admin Defined Roles	1 Roles
karthic1	Duplicate

The **Create New Role** dialog appears. In this dialog:

- A duplicate name is used.
- All permissions match the original admin role.

FIGURE 316 Create Duplicate Role



Create New Role

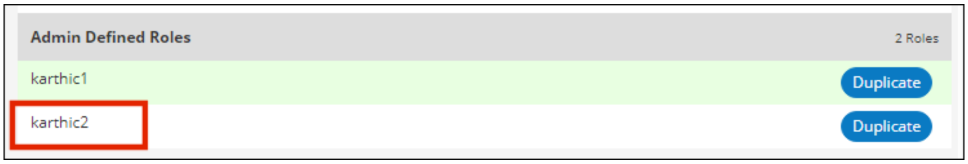
Role Name: karthic1 copy

Role Assignment	
Dashboard	Edit
Settings	Edit
▷ Appliances	Edit
Users	Edit
▷ Roles	Read Only
Workspaces	Edit

5. Make any required changes and click **Create**.

The duplicated admin role is added to the list of admin roles.

FIGURE 317 Duplicated Role



Admin Defined Roles	2 Roles
karthic1	Duplicate
karthic2	Duplicate

Modifying Admin-Defined Roles

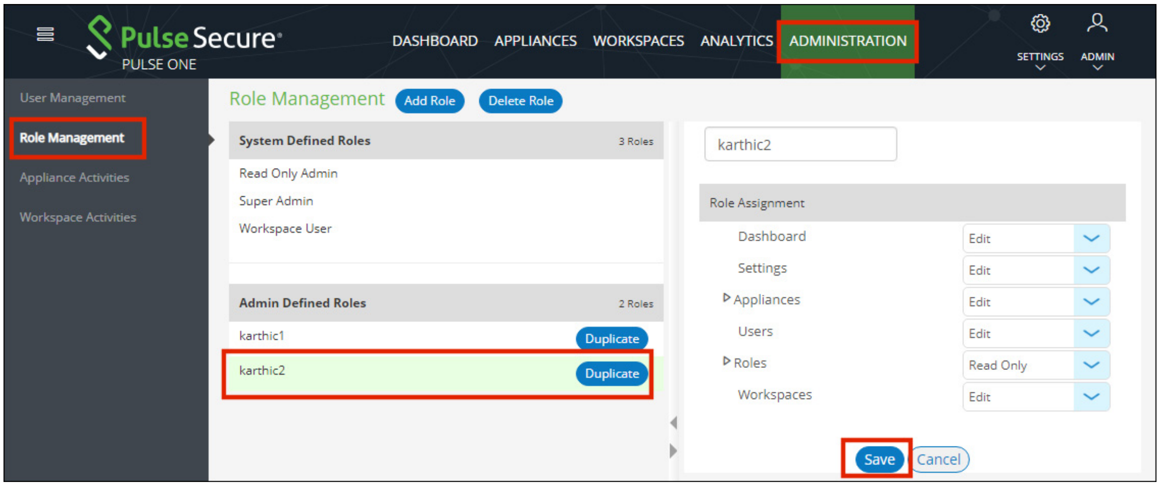
You can modify only the admin defined roles.

To modify a role's permissions:

1. Select the **Administration** menu.
2. Select **Role Management**.

   A list of system defined roles appears.
3. Select the role from the list.
4. In the **Role Assignment** panel, make the required changes and click **Save**.

FIGURE 318 Modify Role



System Defined Roles 3 Roles

Read Only Admin
Super Admin
Workspace User

Admin Defined Roles 2 Roles

karthic1
karthic2

karthic2

Role Assignment

Dashboard	Edit
Settings	Edit
Appliances	Edit
Users	Edit
Roles	Read Only
Workspaces	Edit

Removing Admin-Defined Roles

You can remove only the admin defined roles.

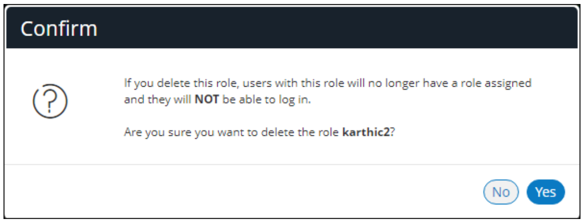
To remove an admin defined role:

1. Select the **Administration** menu.
2. Select **Role Management**.

   A list of system defined roles appears.
3. Select the role from the list and click **Delete Role**.

4. In the Confirmation message box, click **Yes** to remove the selected role.

FIGURE 319 Confirm Delete Role



Confirm

If you delete this role, users with this role will no longer have a role assigned and they will **NOT** be able to log in.

Are you sure you want to delete the role **karthic2**?

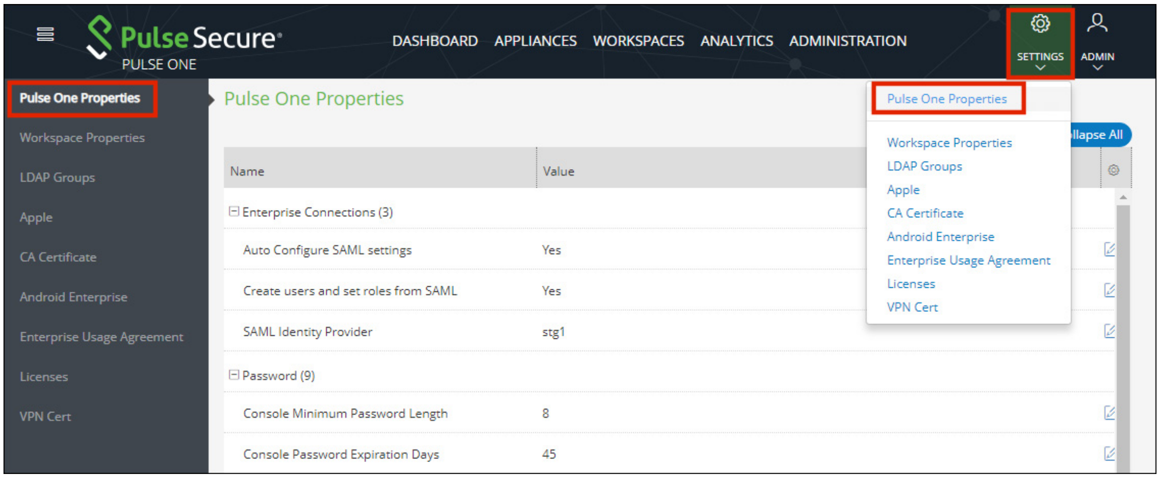
Managing Pulse One Properties

To open the **Pulse One Properties** page:

1. Click the **Settings** icon on top-right-corner of the page.
2. Select **Pulse One Properties**.

   The **Pulse One Properties** page appears.

FIGURE 320 Pulse One Properties

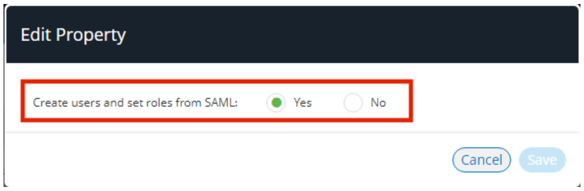


Name	Value
⊟ Enterprise Connections (3)	
Auto Configure SAML settings	Yes
Create users and set roles from SAML	Yes
SAML Identity Provider	stg1
⊟ Password (9)	
Console Minimum Password Length	8
Console Password Expiration Days	45

To edit a Pulse One property:

3. Click the **Edit** button corresponding to the field you want to edit.
4. Change the value and then click **Save**.

FIGURE 321 Edit Property



Edit Property

Create users and set roles from SAML: ● Yes ○ No

Enterprise Connections

- **Auto Configure SAML Settings** – Boolean. If *True*, Pulse One automates the SAML Metadata configuration flow for both Appliance and Pulse One SAML settings.
- **Create Users and Roles from SAML** – Boolean. If *True*, a Pulse One user is created automatically whenever a user from a linked SAML idP (PCS) authentication server logs into Pulse One for the first time using Enterprise SSO.
- **SAML Identity Provider** – The Pulse Connect Secure appliance that is configured for Pulse One server SAML auto-provisioning.
- **SAML Identity Provider Metadata** – Required metadata for the SAML identity provider.
- **SAML Service Provider Metadata**– Required metadata for the SAML service provider.

Password

The **Password** settings are described below:

- **Console Minimum Password Length** – The minimum length of a console password.
- **Console Password Expiration Days** – The number of days after which an Administrator must change their console password.
- **Console Password Require Lowercase** – Boolean. If *True*, the console password must contain at least one lowercase letter.
- **Console Password Require Number** – Boolean. If *True*, the console password must contain at least one number.
- **Console Password Require Special** – Boolean. If *True*, the console password must contain at least one special character.
- **Console Password Require Uppercase** – Boolean. If *True*, the console password must contain at least one uppercase letter.
- **Console Password Reset Timeout Hours** – The number of hours a console password reset email link is valid.
- **Domain Allowed Password Attempts** – The number of login attempts until a console account is locked.
- **Welcome Timeout Hours** –The number of hours a registration token in a welcome email is valid.

Misc

The miscellaneous (**Misc**) settings are described below:

- **Created On** – The date on which the management console was created.
- **Locale** – The console language code.
- **Page Footer** – The footer information that will be displayed at the bottom of the admin console.
- **Server Version** – The current Management Server version that will be displayed at the bottom of the admin console.

Note: You cannot edit the **Created On** and **Server Version** properties.

Working with the MSSP Management Console

Introduction

Using a PSA7k Platform, you can provision a management console for Managed Security Service Provider (MSSP) operations.

From the MSSP management console, you can create multiple customer domains on the appliance. Each domain contains Pulse One, which can be operated by one of your customers. This enables you to operate as an independent provider of Enterprise Mobility Management (EMM) services.

Preparing to Provision an MSSP Management Console

Before you start to create an MSSP management console, ensure that you have the following items:

- Certificate - the MSSP management console requires a wildcard certificate instead of a Subject Alternative Name (SAN) certificate.
- Licenses – the following Pulse One licenses are required:
  - A Pulse One MSSP license - This is required to enable MSSP mode and the creation of an MSSP management console. It takes the form: *P1-MSSP-xxxxxxxx-xxxxxxxx*.
  - Pulse Workspace MSSP licenses – (Optional) This is required to enable Workspaces on the customer domains. It takes the form: *P1-WS-MSSP-xxxxxxxx-xxxxxxxx*.

  The following licenses are *not* supported by MSSP, and cannot be entered after MSSP mode is enabled:

  - PWS licenses for regular on-premise operations.
  - Log-aggregator licenses.

  Standard licenses types can be added to individual customer domains in the MSSP management console, to enable the corresponding features on that domain, see **"Licensing a Customer Domain" on page 280**.

- DNS – ensure that the following additional DNS records are prepared:
  - There is a new ‘msspreserved’ sub-domain that must be resolved to the appliance external IP address.
  - The sub-domains for MGMT domain and customer domains should also resolve to the appliance external IP address.

Creating an MSSP Management Console

The process of provisioning an MSSP Management Console is similar to the CLI-based process that provisions a Pulse One appliance, see the *Pulse One Appliance Getting Started Guide*.

There are some key differences:

- Licenses and certificates are different, see **“Preparing to Provision an MSSP Management Console” on page 271**.
- After you have installed a valid Pulse One MSSP license, you can provision an MSSP management console from the Pulse One Appliance. This uses an MSSP-specific command:

  ```
  p1 mssp provision
  ```

  For example:

  ```
  p1 mssp provision demo.customer.com --admin-username admin123
  --admin-email admin@demo.net
  ```

  In this example:

  - The FQDN URL (*demo.customer.com*) is the URL for the management console. You can choose this URL; it does not have to start with ‘mgmt’.
  - The admin username (*admin123*) will be the username that is used to log into the MSSP management console.

  The command will also prompt the customer to enter the password for the admin user.

- Credentials for AFW services - there will be multiple customer domains running on the appliance. Do not manually generate separate ESA credentials for each customer domain and send them to the customer. Instead, contact Pulse Secure about new MSA and ESA credentials. All the customer domains will share the same ESA credentials to enroll with AFW services.

  The following commands are used to configure the MSA and ESA:

  ```
  pws config set msa
  pws config set esa
  ```

  These commands require a valid PWS license. For the first command to set MSA, a valid MSSP license as also required.

- The following commands are disabled in MSSP mode. Where required, equivalent functionality is supported in the MSSP management console:

```
p1 domain provision
p1 domain group
pws email-domain
```

Accessing the MSSP Management Console

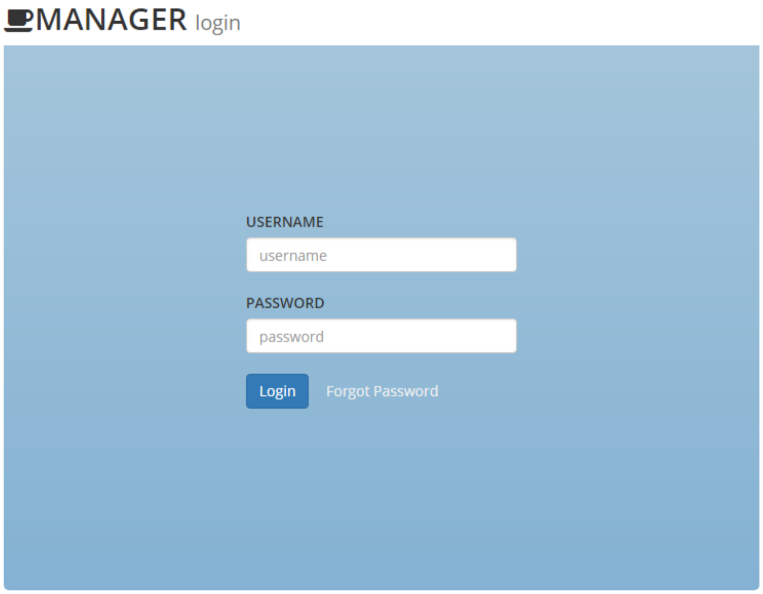
To access the MSSP management console:

1. Open a browser and enter the URL for the management console. For example:

   demo.customer.com

   The login page appears. For example:

   FIGURE 322 MSSP Management Console Login

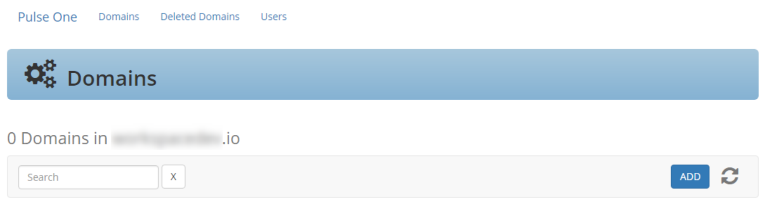
   

2. Log in using the administration user declared when the MSSP management console was provisioned. For example:

   admin123

The default home page (Domains) appears:

FIGURE 323 MSSP Management Console Home Page



0 Domains in [redacted].io

From this page, you can:

- (Optional) Create additional users to the MSSP management console, see **"Managing Users of the MSSP Management Console" on page 274**.
- Create customer domains, see **"Managing Customer Domains on the MSSP Management Console" on page 278**.

Managing Users of the MSSP Management Console

After you have logged into the MSSP management console, you can optionally perform the following tasks:

- **"Adding an MSSP Management Console User" on page 274**.
- **"Editing an MSSP Management Console User" on page 276**.
- **"Deleting an MSSP Management Console User" on page 277**.

Adding an MSSP Management Console User

By adding a user to the MSSP management console, the user can log in and use the features of the console. This user is able to access customer domains using a browser, see **"Accessing a Customer Domain" on page 290**.

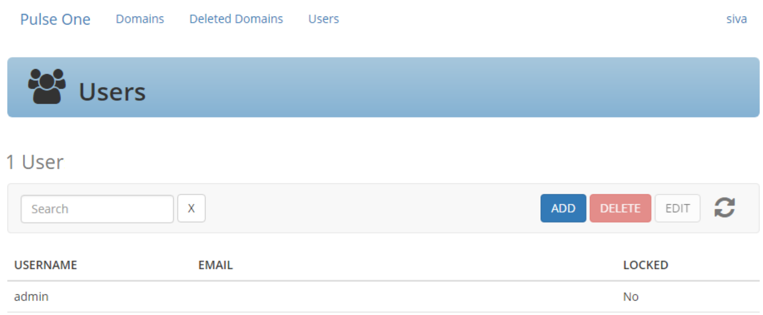
To add a user to the MSSP management console:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 273**.
2. Click the **Users** tab.

   The **Users** page appears.

   Note: When the MSSP management console is started for the first time, only the defined administrator user is present.

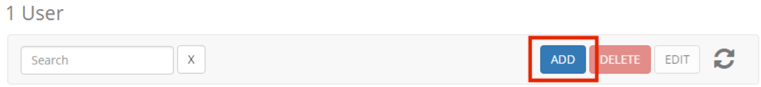
FIGURE 324 Users Page



USERNAME	EMAIL	LOCKED
admin		No

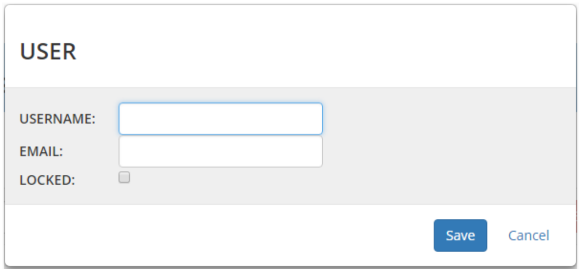
3. Above the table of users, click **Add**.

FIGURE 325 Adding a User



The **User** dialog appears.

FIGURE 326 User Dialog



4. Enter a **Username** for the user.

5. Enter an **Email address** for the user.

6. (Optional) select the **Locked** check box to lock the user account.

   Note: This is an unlikely action during the creation of a user. It is more likely performed when editing an existing user, see **"Editing an MSSP Management Console User" on page 276**.

7. Click **Save**.

   The new user is added to the **Users** page. For example:

   FIGURE 327 Users Page Addition

   The console sends an email to the declared **Email address**. This provides the user with a link to access the console and change their password.

8. Repeat this process for each required user.

Editing an MSSP Management Console User

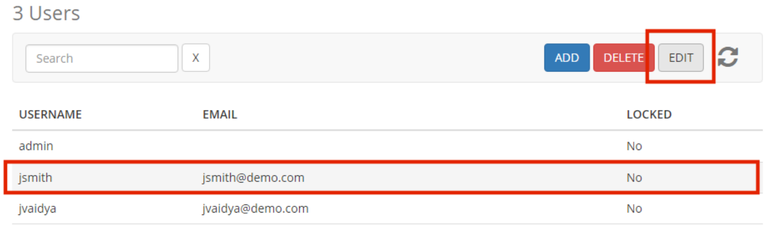
You can edit an existing user, either to change their declared details, or to lock the account.

To edit an existing user:

1. Log into the MSSP management console as an administrator, see **“Accessing the MSSP Management Console” on page 273**.
2. Click the **Users** tab.

   The **Users** page appears.
3. Select the required user in the table of users, and then click **Edit** above the table.

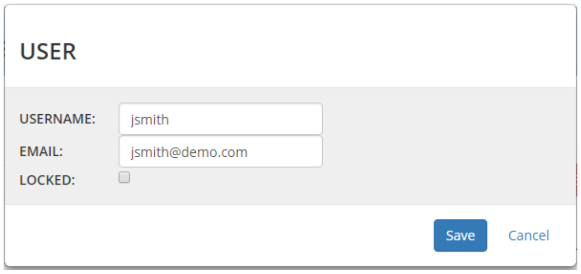
   FIGURE 328 Edit a User

USERNAME	EMAIL	LOCKED
admin		No
jsmith	jsmith@demo.com	No
jvaidya	jvaidya@demo.com	No

   The **User** dialog appears.

   FIGURE 329 Edit User

   USERNAME: jsmith
   EMAIL: jsmith@demo.com
   LOCKED: □

4. Make the required changes.
   - If you want to change the login name for the user, change the **Username**.
   - If you want the user’s email address, change the **Email**.
   - If you want to lock the user account, click **Lock**. This prevents the user from logging into the console.

   Note: If you want to permanently prevent a user from accessing the console, you can delete their account, see **“Deleting an MSSP Management Console User” on page 277**.
5. Click **Save**.
6. The table of users on the **Users** page updates.

Deleting an MSSP Management Console User

You can permanently delete an existing user from the MSSP management console.

After you delete a user, they will no longer be able to access the console.

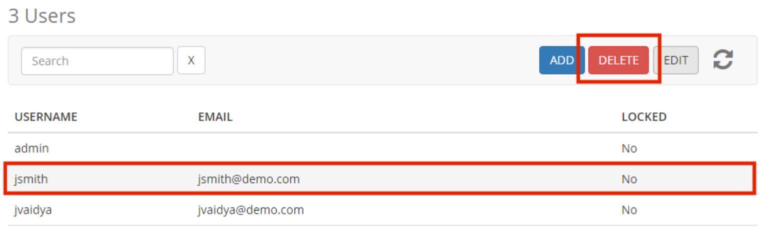
Note: If you want to temporarily prevent a user from accessing the console, you can edit the user to lock the account, see **"Editing an MSSP Management Console User" on page 276**.

To delete a user:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 273**.
2. Click the **Users** tab.

   The **Users** page appears.
3. Select the required user in the table of users, and then click **Delete** above the table.

   FIGURE 330 Delete User

   3 Users

USERNAME	EMAIL	LOCKED
admin		No
jsmith	jsmith@demo.com	No
jvaidya	jvaidya@demo.com	No

   A confirmation dialog appears.
4. Click **OK** to confirm the deletion.

   The user is removed from the table of users.

Managing Customer Domains on the MSSP Management Console

After you have created an MSSP management console and (optionally) created users, you can create individual customer domains. You can then apply one or more licenses to each customer domain, so it can be logged into and used as a standalone Pulse One Appliance.

This section describes the following activities:

- "Adding a Customer Domain" on page 278.
- "Licensing a Customer Domain" on page 280.
- "Adding an Email Domain to a Customer Domain" on page 285.
- "Editing a Customer Domain" on page 286.
- "Managing Customer Domains" on page 287.

Adding a Customer Domain

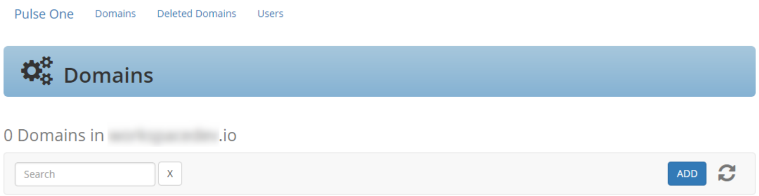
Each of your customers will use a single customer domain. Each domain has its Pulse One appliance, with licenses and one or more email domains.

To add a customer domain:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 273**.
2. Click the **Domains** tab.

   The **Domains** page appears.

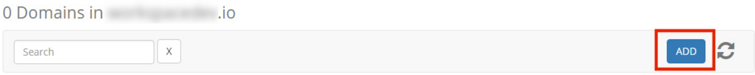
   FIGURE 331 Zero Customer Domains

   Note: When the MSSP management console is started for the first time, there are no customer domains.

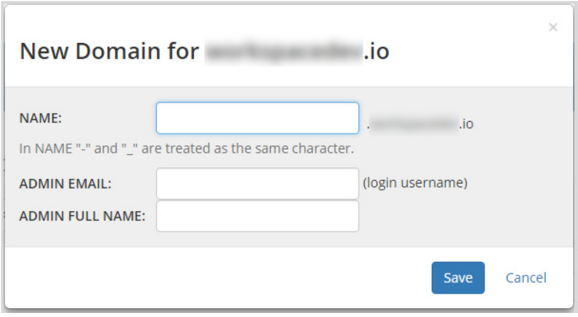
3. Above the table of domains, click **Add**.

   FIGURE 332 Add Customer Domain

The **Domain** dialog appears.

FIGURE 333 New Domain Dialog



New Domain for [redacted].io

NAME: [ ] .[redacted].io

In NAME "-" and "_" are treated as the same character.

ADMIN EMAIL: [ ] (login username)

ADMIN FULL NAME: [ ]

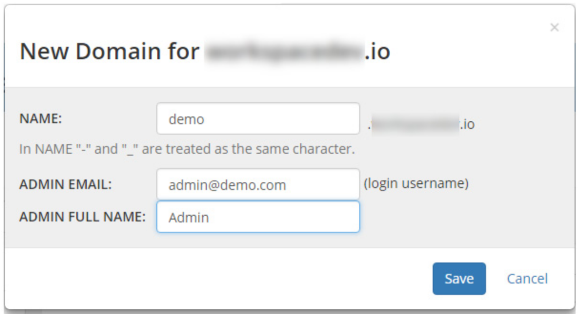
4. Enter a **Name** for the domain. This will be used in the URL for the domain.

   Note: For this property, typing either the hyphen ("-") or underscore ("_") characters will result in a hyphen being used in the domain name. That is, both "one-two" and "one_two" will result in a domain name of "one-two".

5. Enter an **Admin Email** address for the domain. This will be used as the login username for the domain.

6. Enter the administrator name under **Admin Full Name**. For example:

   FIGURE 334 New Domain Dialog



New Domain for [redacted].io

NAME: demo .[redacted].io

In NAME "-" and "_" are treated as the same character.

ADMIN EMAIL: admin@demo.com (login username)

ADMIN FULL NAME: Admin

   In this example, the URL is constructed as follows:

   - The customer domain **Name** is *demo*.
   - The management console is *consoledemo.io*.
   - The **Admin Email** is *admin@demo.com*.

   Then the resulting login URL for the customer domain is *http://demo.consoledemo.io/admin*.

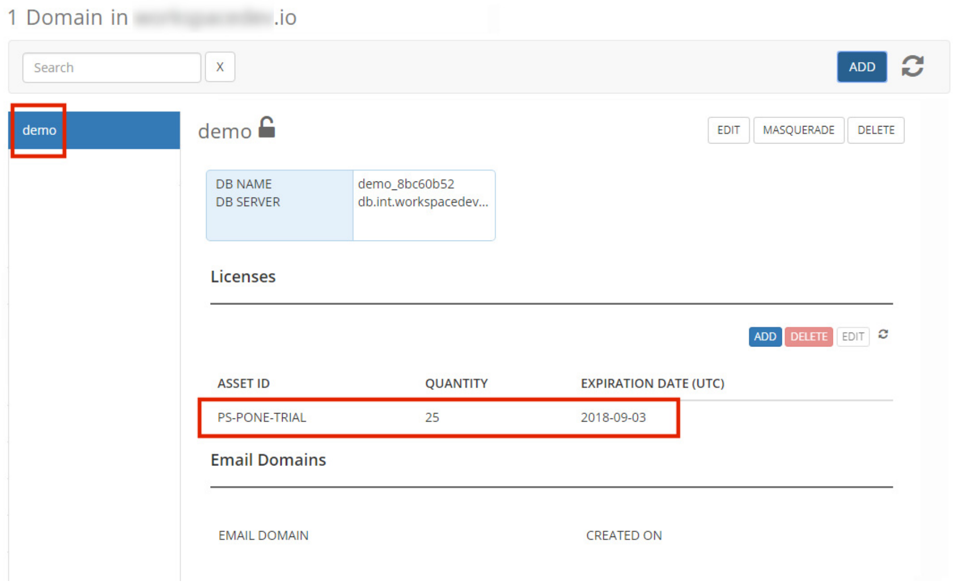
7. Click **Save**.

   The new domain is added to the **Domains** page.

   The console sends an email to the declared **Admin Email** address. This provides the user with a link to access the console and change their password.

When this domain is accessed for the first time, a *PS-ONE-TRIAL license* is applied automatically. For example:

FIGURE 335 Domains Page Addition



1 Domain in [redacted].io

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

Licenses

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PS-PONE-TRIAL	25	2018-09-03

Email Domains

EMAIL DOMAIN	CREATED ON

8. Repeat this process for each required customer domain.

After a customer domain exists, you can apply licenses, see **“Licensing a Customer Domain” on page 280**.

Licensing a Customer Domain

One you have created a customer domain, you can add Pulse One and Pulse Workspace licenses to it. This enables you to configure the customer’s Pulse One appliance with trial licenses, or to enter the licenses already purchased by the customer.

Note: These licenses are not MSSP-related licenses; MSSP licenses are only used to enable the MSSP management console itself.

This section describes the following activities:

- **“Understanding License Types for Customer Domains” on page 281**.
- **“Adding Customer Domain Licenses” on page 281**.
- **“Editing a License for a Customer Domain” on page 284**.
- **“Deleting a License from a Customer Domain” on page 284**.

Understanding License Types for Customer Domains

The following licenses types can be entered for individual customer domains in the MSSP management console, to enable the corresponding features on that domain. These licenses will be applied to the Pulse One appliance in the customer domain.

- *PS-PONE-TRIAL* – The default trial license for Pulse One. This is applied automatically to a customer domain when it is accessed for the first time.
- *PONE-BASIC* - A Pulse One license to enable all out-of-the-box functionality.
- *PWS-TRIAL* – A Pulse Workspace trial license.
- *PWS* – A standard Pulse Workspace license. This is required to enable the Workspace menu in Pulse One, and to enable all workspace-related functions.

Note: Where the Pulse One in an MSSP customer domain has Pulse Workspaces enabled, a single PCS appliance or PCS cluster must be registered, see the *Pulse One Admin Guide*.

Adding Customer Domain Licenses

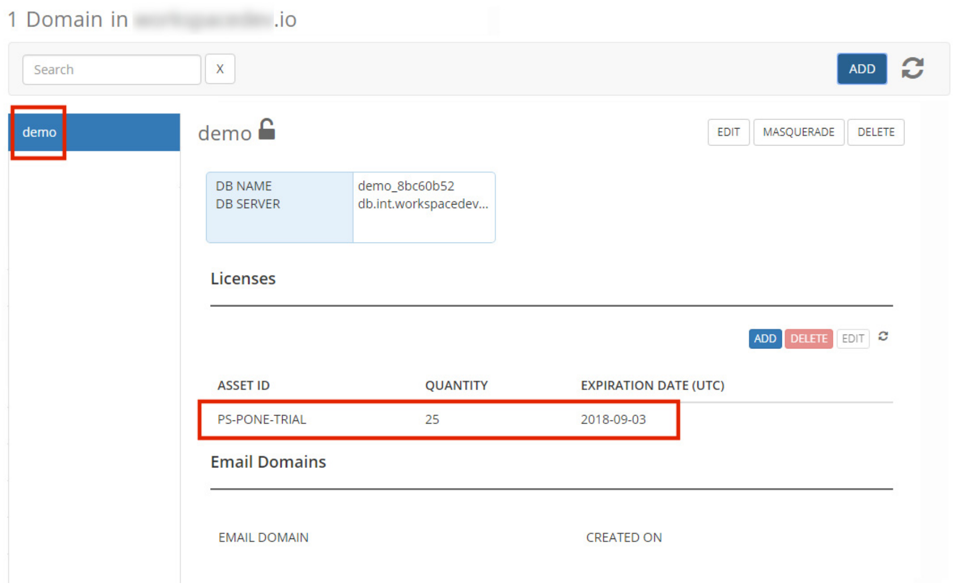
To add a license to a customer domain:

1. Log into the MSSP management console as an administrator, see **“Accessing the MSSP Management Console” on page 273**.
2. Click the **Domains** tab.

   The **Domains** page appears.
3. Select the required customer domain.

The **Domains** page updates to show details of the selection, including any default trial license that are in place. For example:

FIGURE 336 Customer Domain Trial License



1 Domain in [redacted].io

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

Licenses

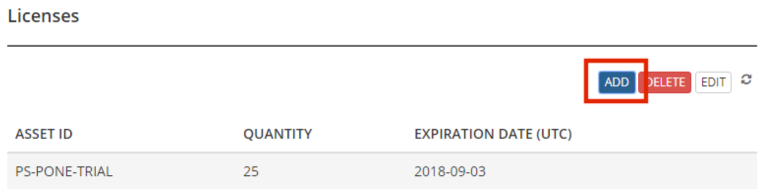
ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PS-PONE-TRIAL	25	2018-09-03

Email Domains

EMAIL DOMAIN	CREATED ON

4. Above the table of licenses, click **Add**.

FIGURE 337 Add Customer Domain License

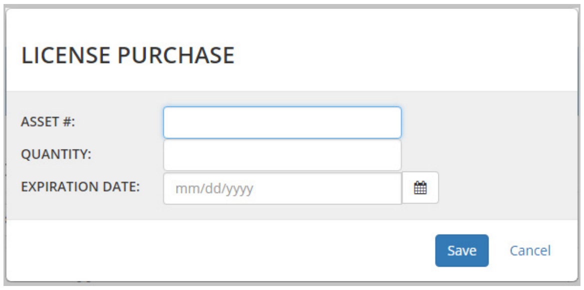


Licenses

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PS-PONE-TRIAL	25	2018-09-03

The **License** dialog appears.

FIGURE 338 License Purchase



LICENSE PURCHASE

ASSET #:

QUANTITY:

EXPIRATION DATE: mm/dd/yyyy

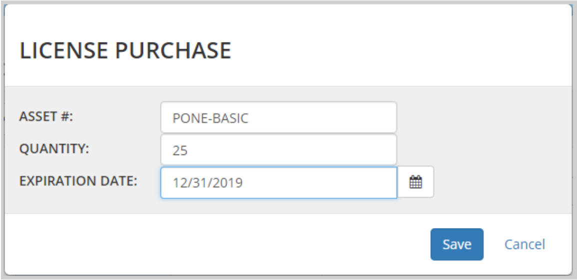
5. Enter the required license type as the **Asset #**. For example: *PONE-BASIC* or *PWS-TRIAL*.

6. Enter the required **Quantity** of this license.

7. Enter the required **Expiration Date** for this license.

   For example:

   FIGURE 339 Required License Details



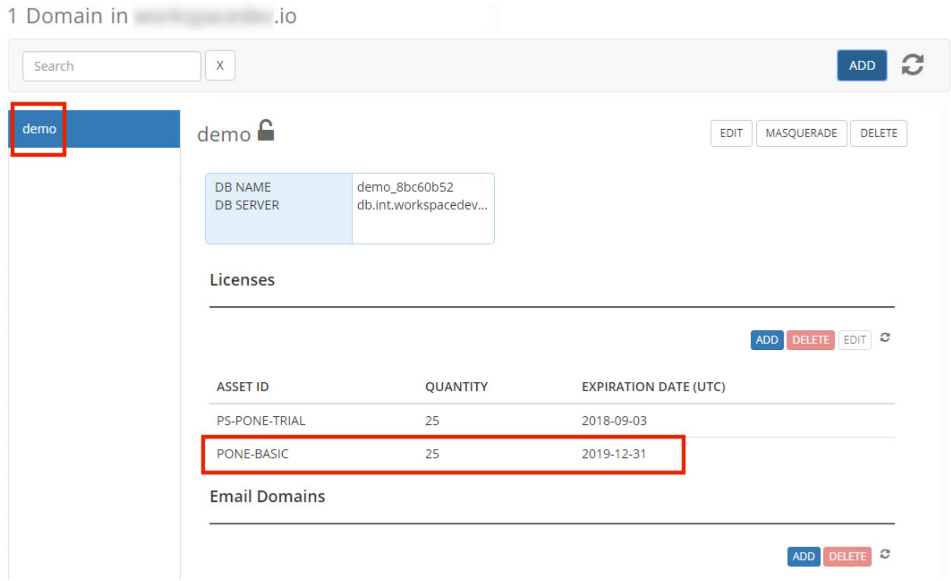
LICENSE PURCHASE

ASSET #:	PONE-BASIC
QUANTITY:	25
EXPIRATION DATE:	12/31/2019

8. Click **Save**.

   The license is added to the customer domain details.

   FIGURE 340 License Added



1 Domain in [redacted].io

demo

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

Licenses

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PS-PONE-TRIAL	25	2018-09-03
PONE-BASIC	25	2019-12-31

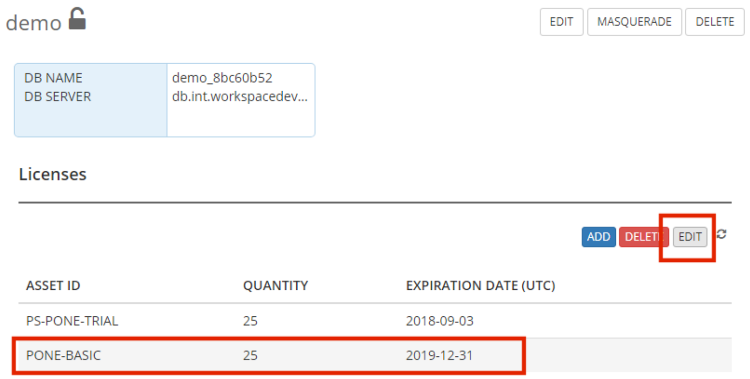
Email Domains

Editing a License for a Customer Domain

To edit a license for a customer domain:

1. Select the license in the table of licenses for the customer domain.
2. Above the table, click **Edit**.

   FIGURE 341 Edit a License

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

   Licenses

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PS-PONE-TRIAL	25	2018-09-03
PONE-BASIC	25	2019-12-31

   The **License Purchase** dialog appears.

3. Update the required details for the license.
4. Click **Save**.

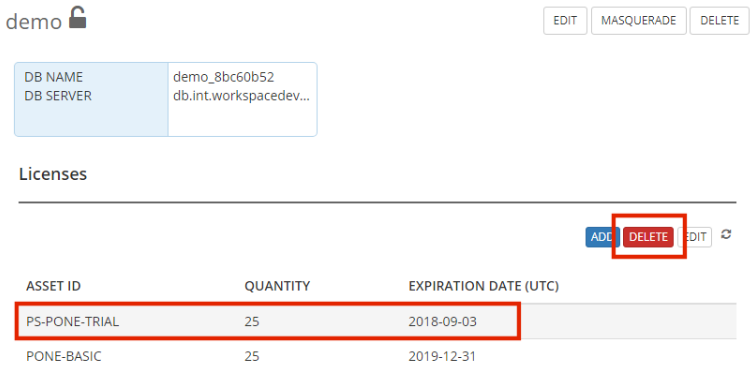
   The license details are updated.

Deleting a License from a Customer Domain

To delete a license from a customer domain:

1. Select the license in the table of licenses for the customer domain.
2. Above the table, click **Delete**.

   FIGURE 342 Delete a License

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

   Licenses

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PS-PONE-TRIAL	25	2018-09-03
PONE-BASIC	25	2019-12-31

   A confirmation dialog appears.

3. Click **OK** to confirm the deletion of the license from the customer domain.

   The license is removed from the table of licenses for the customer domain.

Adding an Email Domain to a Customer Domain

After you create a customer domain, you can add one or more email domains to it.

Each listed email domain permits registrations from users on that domain.

If a request for registration is received from an unlisted domain, it is prevented.

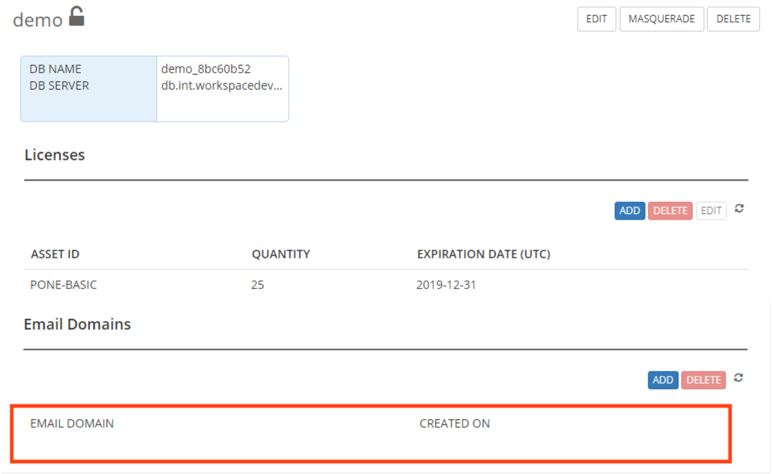
To add an email domain to a customer domain:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 273**.
2. Click the **Domains** tab.

   The **Domains** page appears.
3. Select the required customer domain.

   The **Domains** page updates to show details of the selection. For example:

   FIGURE 343 Customer Domain



demo

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

Licenses

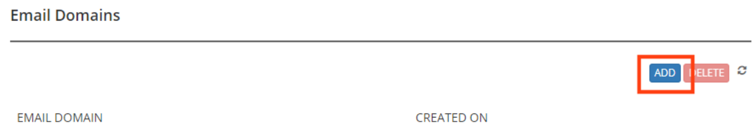
ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PONE-BASIC	25	2019-12-31

Email Domains

EMAIL DOMAIN	CREATED ON

   In this example, there is no defined email domain for the demo customer domain.
4. Above the (initially empty) table of email domains, click **Add**.

   FIGURE 344 Add Email Domain

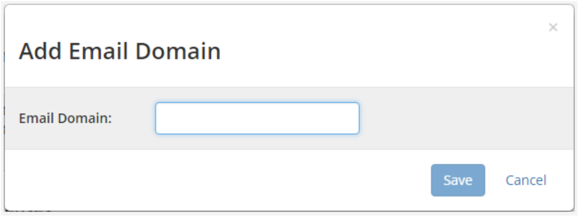


Email Domains

EMAIL DOMAIN	CREATED ON

The **Email** dialog appears.

FIGURE 345 Add Email Domain Dialog



Add Email Domain

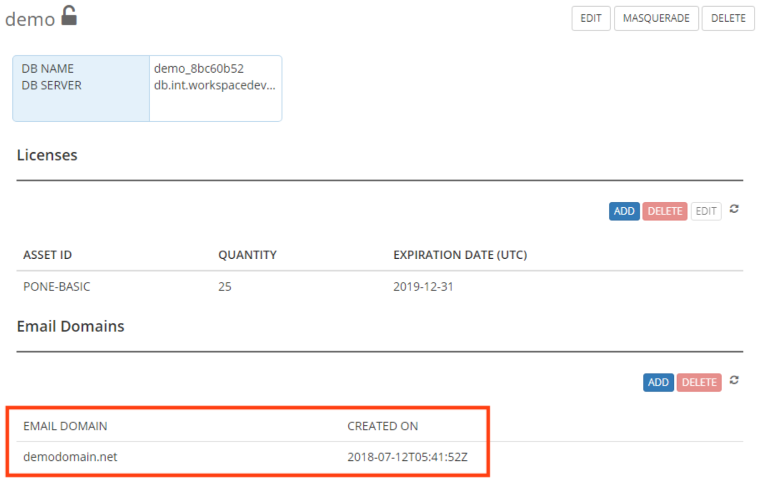
Email Domain:

5. Enter the required **Email Domain**. For example: *demodomain.net*.

6. Click **Save**.

   The email domain is added to the customer domain details.

FIGURE 346 Email Domain Added



demo

DB NAME	demo_8bc60b52
DB SERVER	db.int.workspacedev...

Licenses

ASSET ID	QUANTITY	EXPIRATION DATE (UTC)
PONE-BASIC	25	2019-12-31

Email Domains

EMAIL DOMAIN	CREATED ON
demodomain.net	2018-07-12T05:41:52Z

Editing a Customer Domain

You can edit the name of a customer domain at any time. When you do this:

- The URL of the customer domain changes, though all configuration is retained.
- The sessions of logged in users are closed.

To edit a customer domain:

1. Log into the MSSP management console as an administrator, see **“Accessing the MSSP Management Console” on page 273**.

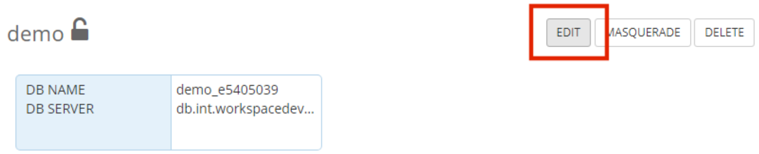
2. Click the **Domains** tab.

   The **Domains** page appears.

3. In the table of domains, select the required customer domain.

4. Above the table, click **Edit**.

FIGURE 347 Edit a Customer Domain

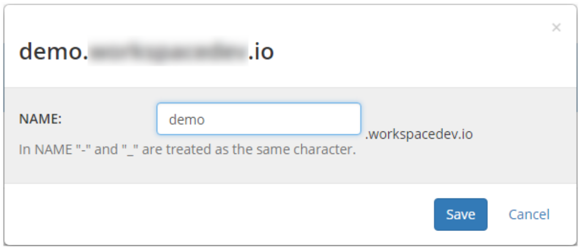


demo

DB NAME	demo_e5405039
DB SERVER	db.int.workspacedev...

A customer domain dialog appears. For example:

FIGURE 348 Customer Domain



demo.[redacted].io

NAME: demo .workspacedev.io

In NAME "-" and "_" are treated as the same character.

5. Update the **Name** of the domain.

Note: For this property, typing either the hyphen ("-") or underscore ("_") characters will result in a hyphen being used in the domain name. That is, both "one-two" and "one_two" will result in a domain name of "one-two".

6. Click **Save**.

The **Domains** page updates.

If the **Admin Email** address has changed, the console sends an email to the Admin Email address. This provides the user with a link to access the console and change their password.

Managing Customer Domains

This section describes the following processes:

- "Deleting a Customer Domain" on page 287.
- "Viewing Deleted Customer Domains" on page 288.
- "Recovering a Deleted Customer Domain" on page 289.

Deleting a Customer Domain

You can delete a customer domain at any time.

Any deleted customer domain can be viewed in the **Deleted Domains** tab, where it remains for a retention period, see "Viewing Deleted Customer Domains" on page 288.

You can log into a deleted customer domain if required.

A deleted customer domain can be recovered if required, including the configuration and data for the domain. However, Android/iOS devices that were managed by the customer domain are not retrieved, and must be re-registered. See **"Recovering a Deleted Customer Domain" on page 289**.

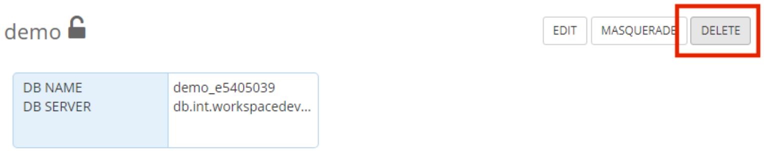
After the retention period, the deleted customer domain and all configuration and data is permanently deleted automatically.

To delete a customer domain:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 273**.
2. Click the **Domains** tab.

   The **Domains** page appears.
3. In the table of domains, select the required customer domain.
4. Above the table, click **Delete**.

   FIGURE 349 Delete a Customer Domain

DB NAME	demo_e5405039
DB SERVER	db.int.workspacedev...

   A confirmation dialog appears for the customer domain deletion.
5. Click **OK** to confirm the deletion.

   The domain is deleted from the **Domains** page, and moved to the **Deleted Domains** page, see **"Viewing Deleted Customer Domains" on page 288**.

Viewing Deleted Customer Domains

All customer domains that have been deleted can be viewed in the **Deleted Domains** tab for a retention period. This is two days for On-Prem appliances, and 30 for cloud appliances. During this time, the customer domain can be recovered. However, Android/iOS devices that were managed by the original customer domain are no longer accessible.

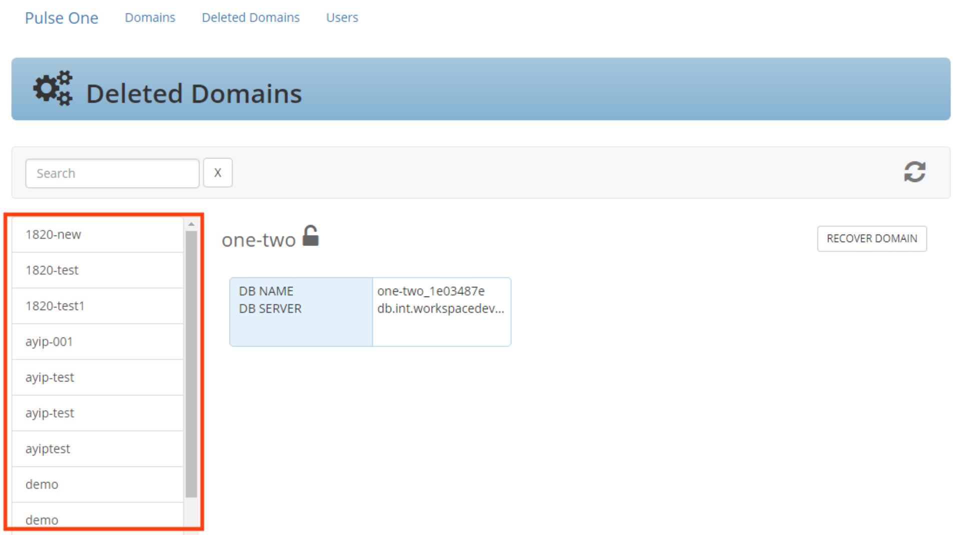
Note: After the retention period, the deleted domain is permanently deleted automatically, along with all configuration and data.

To view deleted customer domains:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 273**.
2. Click the **Deleted Domains** tab.

The **Deleted Domains** page appears. This includes a list of customer domains that have been deleted during the last 30 days.

FIGURE 350 Deleted Domains



1820-new
1820-test
1820-test1
ayip-001
ayip-test
ayip-test
ayiptest
demo
demo

one-two

DB NAME DB SERVER	one-two_1e03487e db.int.workspacedev...

You can recover a listed deleted customer domain if required, see **“Recovering a Deleted Customer Domain” on page 289**.

Recovering a Deleted Customer Domain

You can recover any customer domain that is listed in the **Deleted Domains** tab. This process retrieves the customer domain and its configuration and data. However, Android/iOS devices that were managed by the original customer domain are not retrieved, and must be re-registered.

Note: You cannot recover a domain if its name is in use by a current customer domain.

Note: After the retention period, the deleted domain is permanently deleted automatically.

To recover a deleted customer domain:

1. Log into the MSSP management console as an administrator, see **“Accessing the MSSP Management Console” on page 273**.

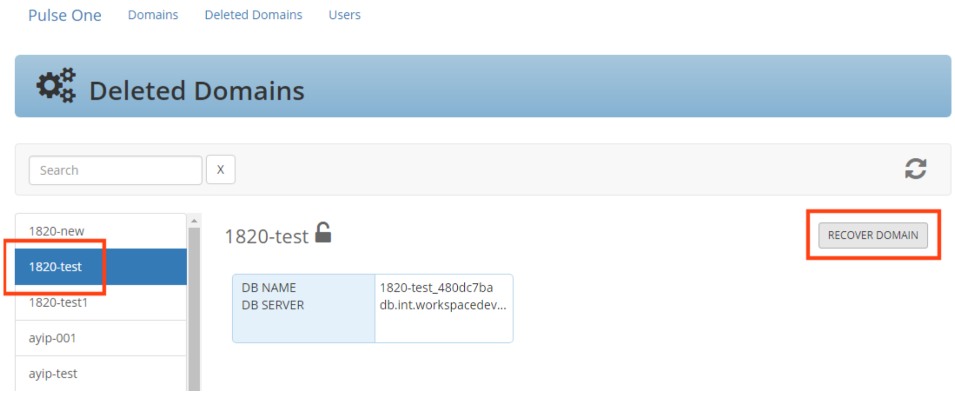
2. Click the **Deleted Domains** tab.

   The **Deleted Domains** page appears.

3. In the table of deleted domains, select the customer domain that you want to recover.

4. Above the table, click **Recover Domain**.

   FIGURE 351 Recover a Deleted Customer Domain

DB NAME DB SERVER	1820-test_480dc7ba db.int.workspacedev...

   A confirmation dialog appears for the customer domain recovery.

5. Click **OK** to confirm the recovery.

   The domain is removed from the **Deleted Domains** page, and moved to the **Domains** page, see “Accessing a Customer Domain” on page 290.

Accessing a Customer Domain

You can access a customer domain:

- From the management console, using a Masquerade session. To do this, select a customer domain on the **Domains** page and click **Masquerade**. You are logged into the customer domain in a separate tab using your current login on the management console.
- From a browser. This is how your customers will access their customer domain. To do this, enter the URL for the customer domain in the browser’s address bar. Log into the Pulse One appliance using admin credentials for the customer domain.

Note: You cannot access a customer domain while it is listed on the **Deleted Domains** page. To access it, you must first recover it to the **Domains** page.

Note: Where the Pulse One in an MSSP customer domain has Pulse Workspaces enabled, a single PCS appliance or PCS cluster must be registered, see the *Pulse One Admin Guide*.

Note: The Pulse One in an MSSP customer domain cannot be used as a syslog server.

Note: The Pulse One in an MSSP customer domain does not support configuration distribution.