Pulse Workspace Administration Guide

Supporting Pulse Workspace 2.0.1901

Product Release	**2.0.1901**
Published	**15 May 2019**
Document Version	**1.1**

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

www.pulsesecure.net

© 2019 by Pulse Secure, LLC. All rights reserved.

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

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

Pulse Workspace 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 1
Document conventions 1
Text formatting conventions 1
Command syntax conventions 1
Notes and Warnings 2
Requesting Technical Support 2
Self-Help Online Tools and Resources 2
Opening a Case with PSGSC 3

GETTING STARTED 5
Overview of Pulse One 5
Logging Into Pulse One 6
Adding a Pulse Workspace License 8
Changing the Password 9

VIEWING PULSE ONE DASHBOARDS 11
Viewing Overall System Health 11
Viewing Metrics for Appliances 12
Viewing Workspace Metrics 14

SYSTEM MANAGEMENT 17
Working with LDAP Groups 17
Adding an LDAP Group 17
Removing an LDAP Group 19
Configuring an LDAP Group 19
Adding an Apple MDM Certificate 21
Adding a CA Certificate 27
Configuring an External PKI Server 31
Configuring a VPN Certificate 32
Changing the Enterprise Usage Agreement 33
Viewing Activity Logs 33
Searching for an Activity 35
Filtering Activities 35
Viewing Activity Details 36
Licensing Pulse One and Pulse Workspace 36

© 2019 Pulse Secure, LLC.

PROVISIONING DEVICES 39
Features Supported on iOS and Android Devices 39
Features supported on iOS v10.0+ Devices 39
Features supported on Android v6.0.1+ devices 40
Features supported on Android v8.0+ devices 40
Understanding Managed Devices and Managed Clients 41
Onboarding iOS BYOD Devices 41
Understanding Your SAML-Based Authentication Email 42
Understanding Your PIN-Based Authentication Email 43
Registering an iOS BYOD Device 44
Onboarding Android BYOD Devices 51
Understanding Your SAML-Based Authentication Email 52
Understanding Your PIN-Based Authentication Email 53
Registering Your Android BYOD Device 54
Configuring Corporate-Owned iOS Devices 58
Configuring Corporate-Owned Android Devices 58
Registering a Corporate-Owned Android Device 59
Configuring Managed Clients 67
Enabling Managed Client Mode 67
Configuring VPN on Demand for Managed Clients 67
Enrolling a Personal Device as a Managed Client 78

CONFIGURING ANDROID ENTERPRISE 85
Overview 85
Adding an Android App to the App Catalog 85
Viewing the App Catalog 86
Adding an Android App to the App Catalog from Google Play 87
Adding an Android App to the App Catalog Manually 92
Uploading an Android App to the App Catalog from Pulse One 94
Uploading Your In-House or Enterprise Apps using Google Play Console 98
Logging into the Google Play Admin Console 98
Publishing a Private App on the Google Play Store 99
Approving a Private App for AFW Provisioning 101
Configuring Policy Settings 102
Adding an Android App to a Policy 102
Configuring Policy Properties 106
Setting a Password Policy 108
Locking a Work Profile 109

WORKSPACE MANAGEMENT 111
Managing Users 111

© 2019 Pulse Secure, LLC.

Adding a User 111
Deleting a User 114
Verifying an LDAP Group 115
Adding a Policy Tag to a Workspace User Account 116
Performing Workspace Actions 116
Understanding the Workspace Details Window 119
Working with the App Catalog 122
Working with the Apple Volume Purchase Program 122
Adding iOS Apps to the App Catalog 125
Adding iOS Apps to a Policy from the App Catalog 130
Managing Policies 132
Creating a Policy 132
Understanding Policy Properties 135
Configuring Workspace Properties 148
Enterprise Connections 149
Workspaces 149
Enterprise PKI Integration 150
Misc 152
Configuring Auto-Config of a VPN Provider on Mobile Devices 153
Ensuring that PCS has a CA Certificate Associated With its External Port 153
Ensuring that PCS is Synchronized with Pulse One 155
Configuring a VPN Provider in the Workspace Properties 156
Updating and Publishing a Policy to Use a Specified VPN Provider 158
Configuring Appliance ActiveSync 160
Configuring Certificate-Based ActiveSync 161
Working with ActiveSync Certificates via SCEP 161
Working with ActiveSync Certificates via Windows CAWE 162
Working with Device Location 165
Overview of Device Location 165
Creating a Google API Key 166
Configuring Device Location 172
Locating a Device 179
Working with Lost Mode for a Device 180

VIEWING ANALYTICS 183
Viewing the Login Attempts Report 183
Viewing the Appliance Health Report 184
Viewing the Appliance Activities Report 185
Viewing the App Visibility Report 186
Viewing Log Aggregation and Analysis 187

© 2019 Pulse Secure, LLC.

USER ADMINISTRATION 189
Adding an Admin User 189
Modifying User Details 190
Removing an Admin User 190
Resetting a User Password 191
Suspending a User 192

ROLE MANAGEMENT 193
Adding Admin-Defined Roles 193
Modifying Admin-Defined Roles 196
Removing Admin-Defined Roles 196
Managing Pulse One Properties 197
Enterprise Connections 198
Password 198
Misc 199

WORKING WITH THE MSSP MANAGEMENT CONSOLE 201
Introduction 201
Preparing to Provision an MSSP Management Console 201
Creating an MSSP Management Console 202
Accessing the MSSP Management Console 203
Managing Users of the MSSP Management Console 204
Adding an MSSP Management Console User 204
Editing an MSSP Management Console User 206
Deleting an MSSP Management Console User 207
Managing Customer Domains on the MSSP Management Console 208
Adding a Customer Domain 208
Licensing a Customer Domain 210
Adding an Email Domain to a Customer Domain 215
Editing a Customer Domain 216
Managing Customer Domains 217
Accessing a Customer Domain 220

© 2019 Pulse Secure, LLC.

Preface

- Document conventions 1
- Requesting Technical Support 2

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.

© 2019 Pulse Secure, LLC.

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**

© 2019 Pulse Secure, LLC.

- 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/**

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Getting Started

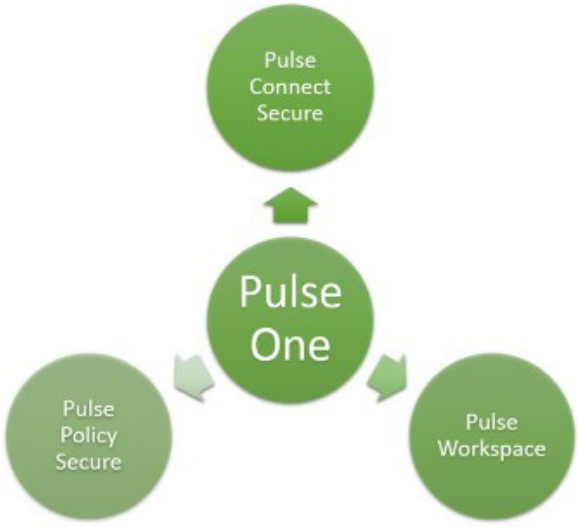
- Overview of Pulse One 5
- Logging Into Pulse One. 6
- Adding a Pulse Workspace License 8
- Changing the Password 10

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.

© 2019 Pulse Secure, LLC.

- **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

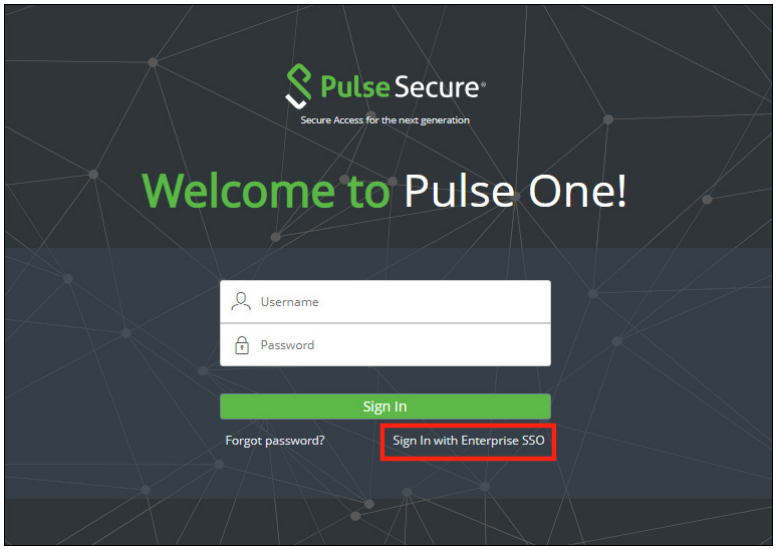
This section details the steps to log in to Pulse One administration.

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 148**.

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**.

© 2019 Pulse Secure, LLC.

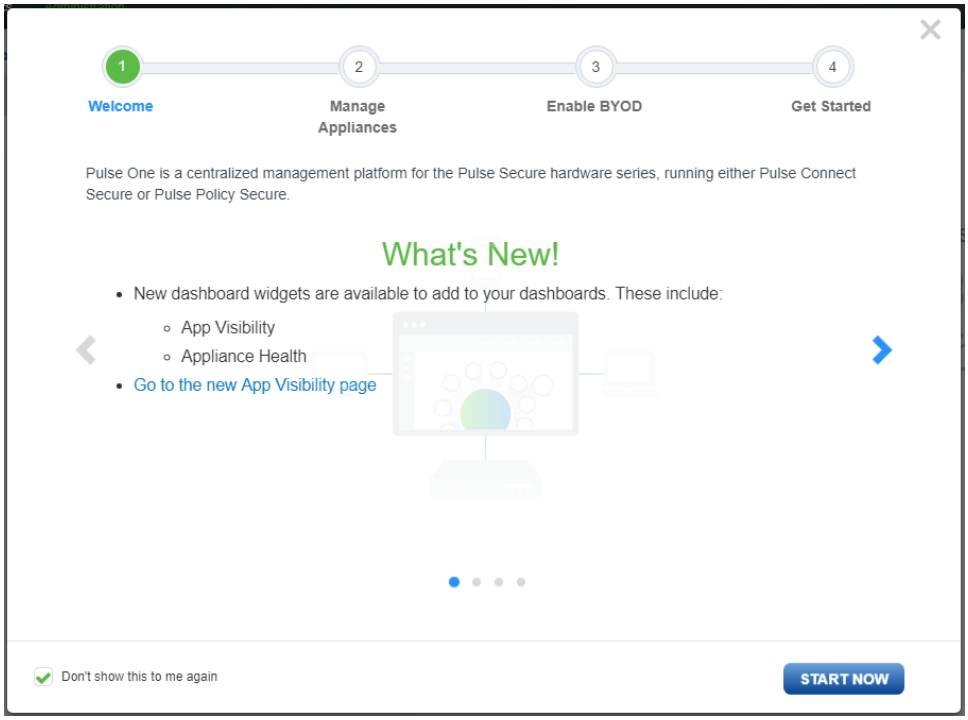
An email that contains **Reset your password** link will be sent to your registered mail id. Use this link to launch Pulse One and provide your new password and confirm the new password.

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

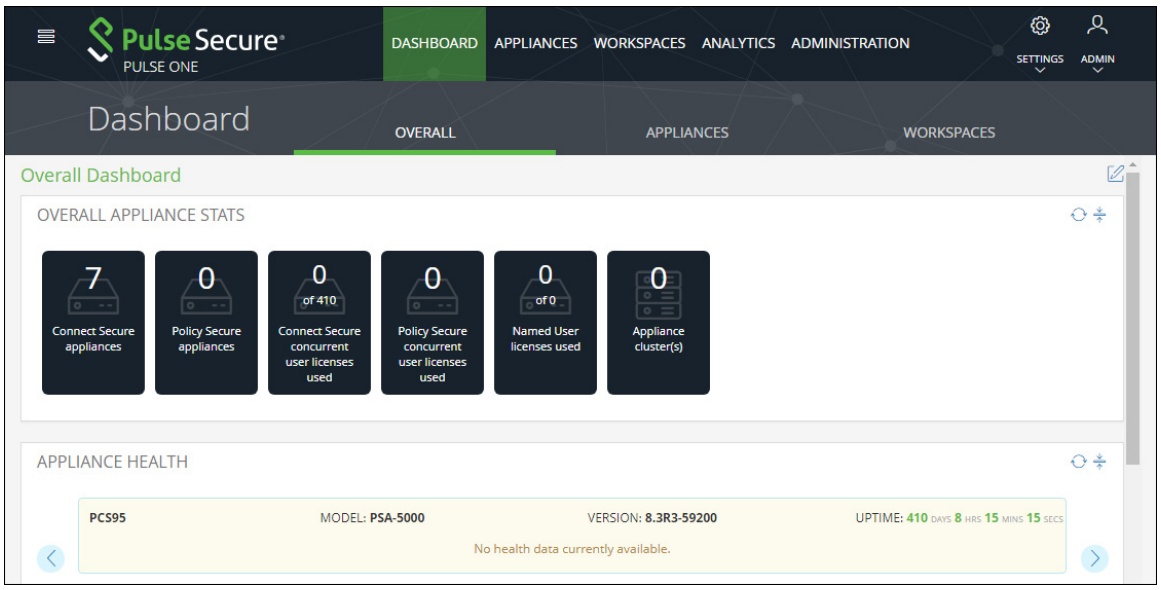


The Welcome wizard provides you a brief overview of Pulse One. Click the right-arrow button until the **Get Started** option appears. Optionally, select the **Don't show this to me again** check box and then click **Start Now**.

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**.

© 2019 Pulse Secure, LLC.

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.

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
```

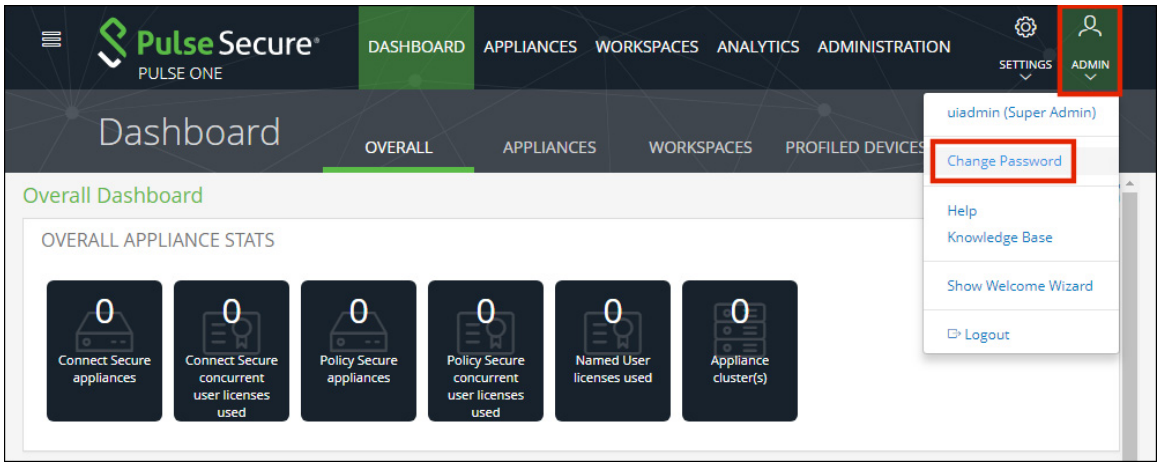

© 2019 Pulse Secure, LLC.

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**.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

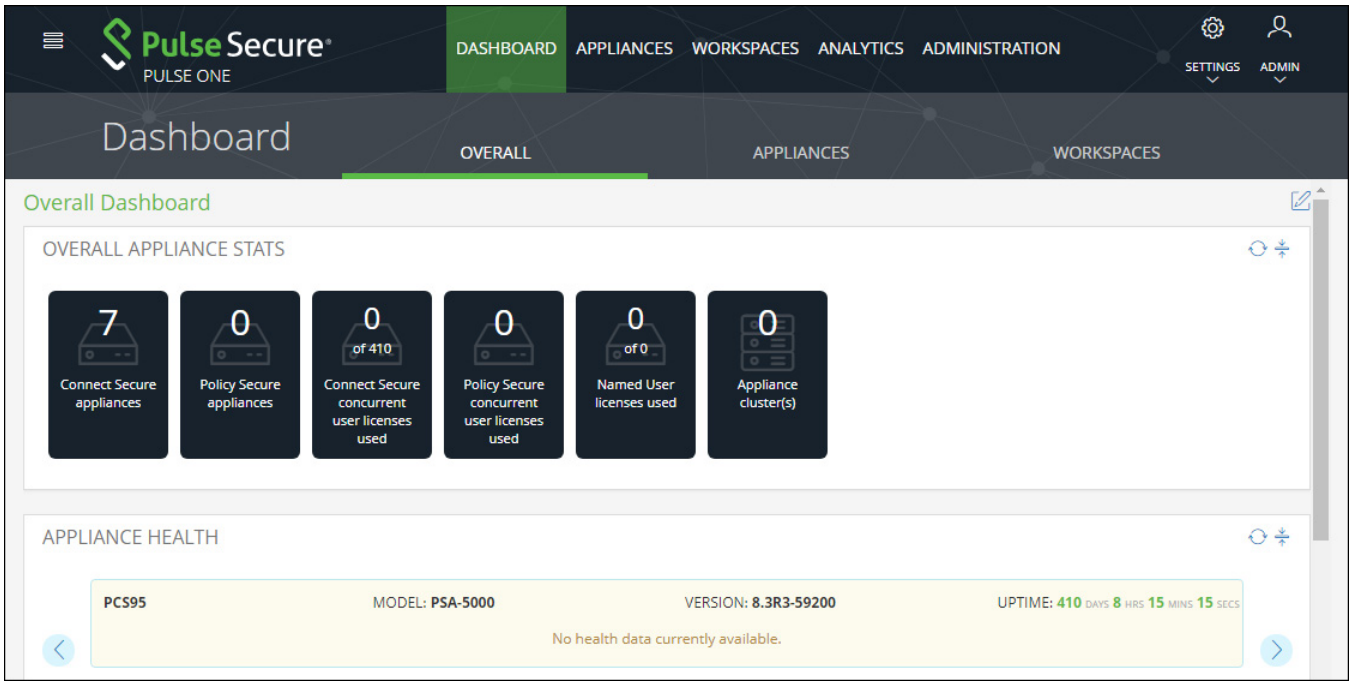
Viewing Pulse One Dashboards

- Viewing Overall System Health 11
- Viewing Metrics for Appliances 12
- Viewing Workspace Metrics 14

Viewing Overall System Health

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

FIGURE 6 Overall 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 in separate widgets in the **Overall** tab:

- Overall appliance statistics.
- Appliance health for individual appliances.
- VPN realm usage.
- Role usage.
- Frequent user logins.
- Logins in the past 24 hours.

© 2019 Pulse Secure, LLC.

- Critical appliance events with timestamps.
- Resource dial.
- Pulse Connect Secure versions.
- Pulse Policy Secure versions.

Viewing Metrics for Appliances

To view metrics for appliances, select the **Dashboard** tab, and then select the **Appliances** tab:

FIGURE 7 Appliances Dashboard

© 2019 Pulse Secure, LLC.

The administrator can view the following information in separate widgets in the **Appliances** tab:

- The total number of appliances. In this example, there are twenty appliances.
- Individual appliances are displayed as tabs around the central circle.
    - These are sorted into Pulse Connect Secure appliances and Pulse Policy Secure appliances.
    - The color of the individual tabs indicates the status of the appliance.
    - Hover over any tab to see its name.
- Details for each appliance can be viewed by clicking its tab. This includes:
    - The appliance **Version**.
    - The appliance **Model**. For example: PSA-300.
    - **Serial Number**.
    - **Last Config Upload**. A timestamp.
    - **IF-MAP Federation**. Boolean.
    - **Using License Server**. Boolean.
- Summary metrics are also displayed:
    - The number of Active Sync Connections for the appliances.
    - The number of concurrent users.
    - The number of authorization failures.
    - The throughput of data.
    - CPU utilization.
    - Disk utilization.
    - Memory utilization.

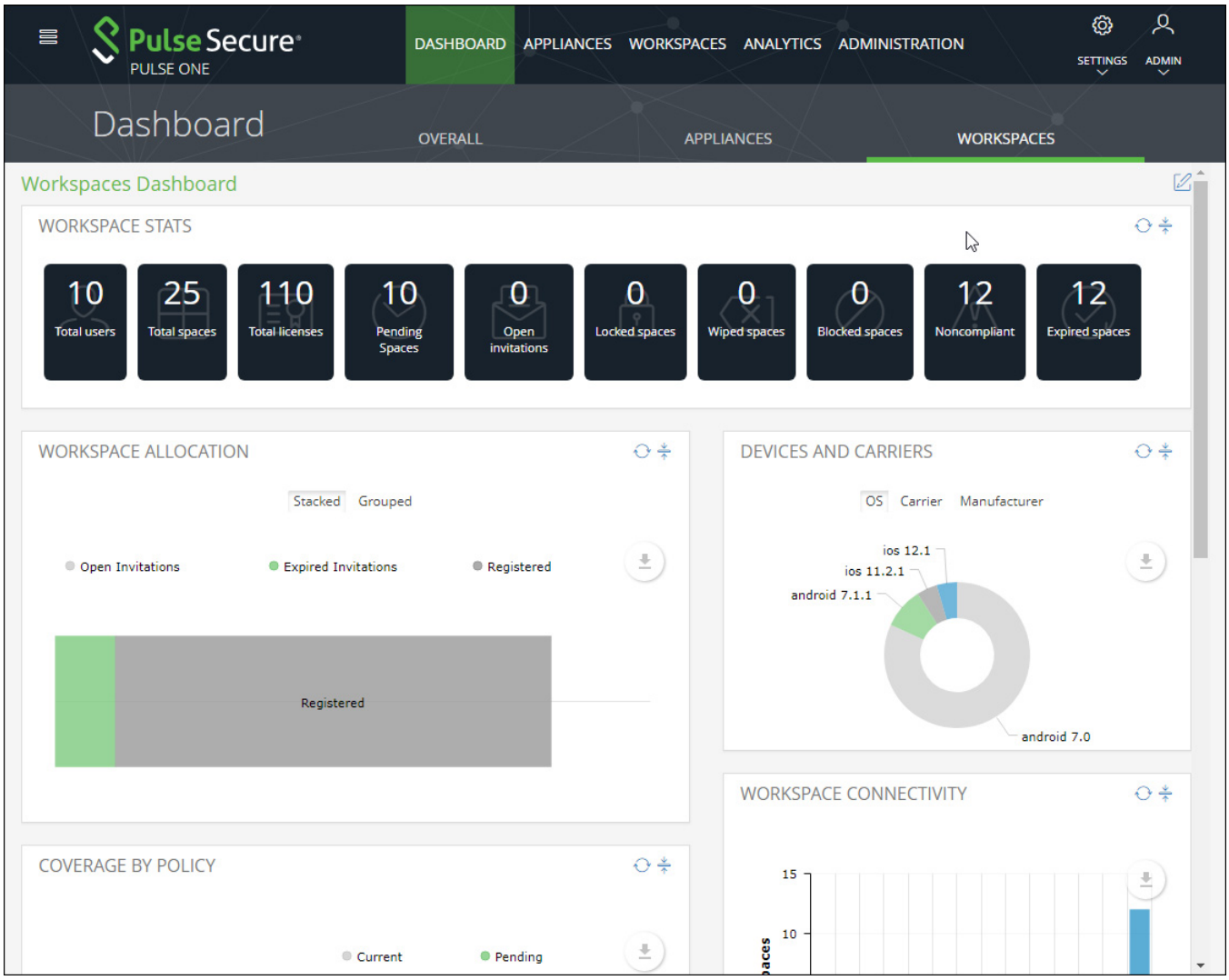
© 2019 Pulse Secure, LLC.

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 8 Workspaces Dashboard



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

© 2019 Pulse Secure, LLC.

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 (work)spaces.
    - The total number of wiped (work)spaces.
    - The total number of 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.

© 2019 Pulse Secure, LLC.

- Coverage by policy, in terms of individual current/pending policies.
- Workspace Connectivity.

© 2019 Pulse Secure, LLC.

System Management

- Working with LDAP Groups 17
- Adding an Apple MDM Certificate 21
- Adding a CA Certificate. 27
- Configuring a VPN Certificate 32
- Changing the Enterprise Usage Agreement 33
- Viewing Activity Logs 33
- Licensing Pulse One and Pulse Workspace. 36

Working with LDAP Groups

Enterprises would like to 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.

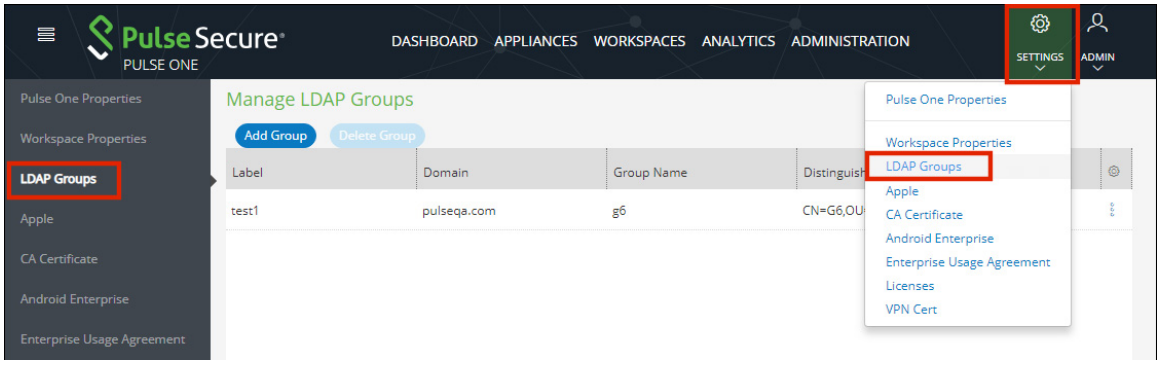
Adding an LDAP Group

To add an LDAP group:

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

   The **Manage LDAP Groups** page appears.

   FIGURE 9 Adding an LDAP Group



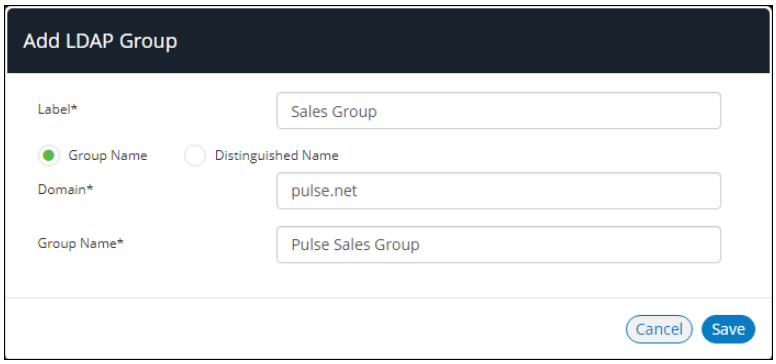
2. Click **Add Group**.

   The **Add LDAP Group** dialog appears.

© 2019 Pulse Secure, LLC.

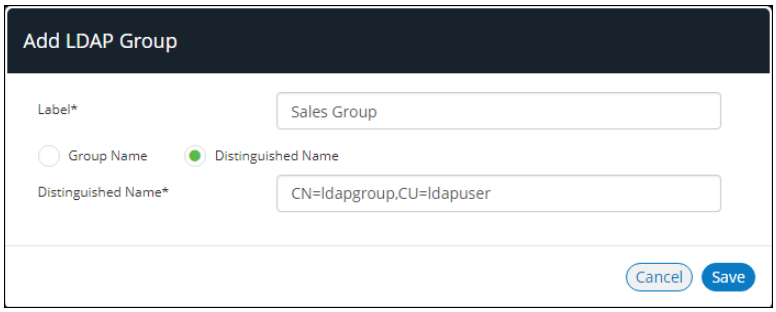
3. Enter a **Label** for the group.
4. Select either **Group Name** or **Distinguished Name** format. The dialog updates.
5. (Optional) If you selected **Group Name**:
    - Enter the **Domain** name to which the group belongs.
    - Specify a **Group Name**.
    - Click **Save** to add the group.

FIGURE 10 Add an LDAP Group using a Group Name



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 11 Provide LDAP Group details – using Distinguished Name



When an LDAP Group is added, it is unverified.

© 2019 Pulse Secure, LLC.

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**.

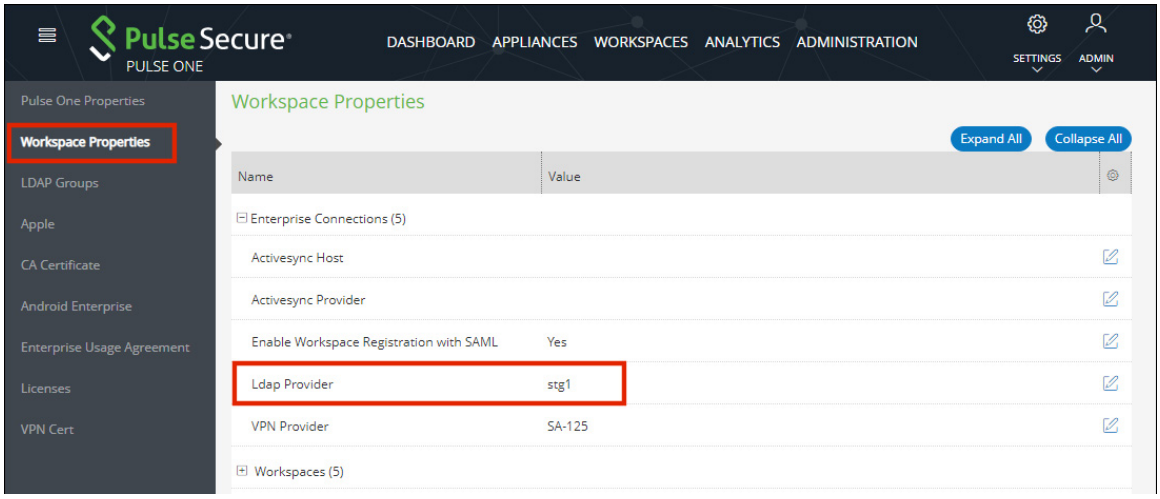
   The **Workspace Properties** page appears.

3. Expand **Enterprise Connections.**

© 2019 Pulse Secure, LLC.

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

FIGURE 12 Edit the LDAP Provider



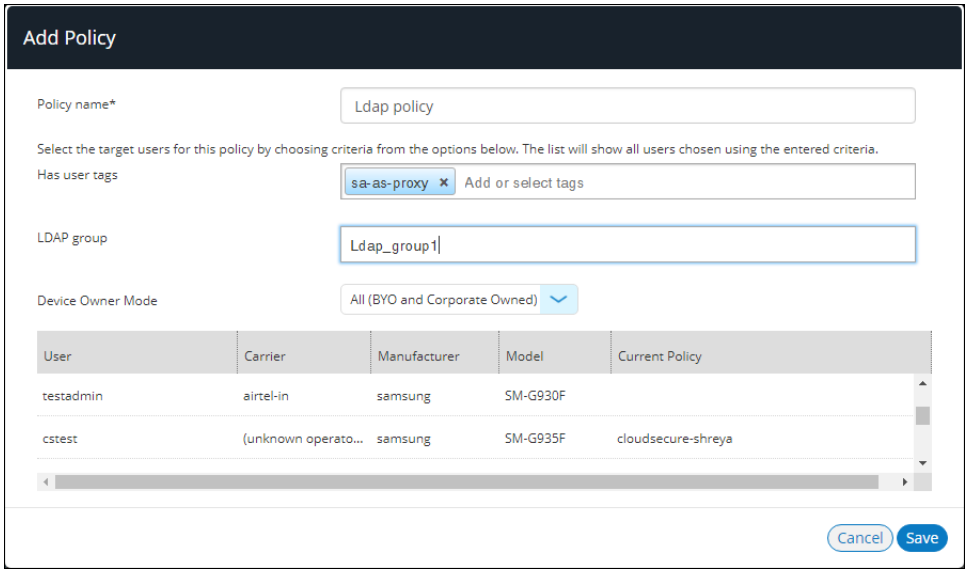
The **Edit Property** dialog appears.

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 13 Map Policy



9. Click **Save**.

© 2019 Pulse Secure, LLC.

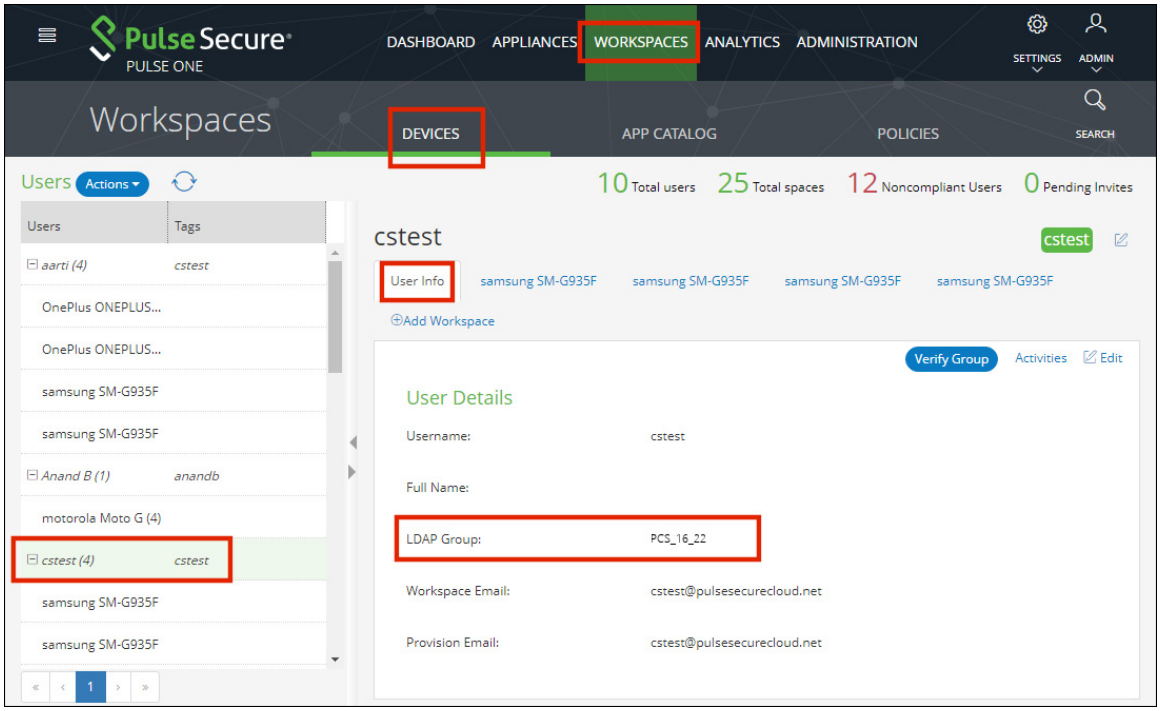
10. Select the **Workspaces** menu, and then the **Devices** tab.

    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 14 LDAP Group in User Details



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.

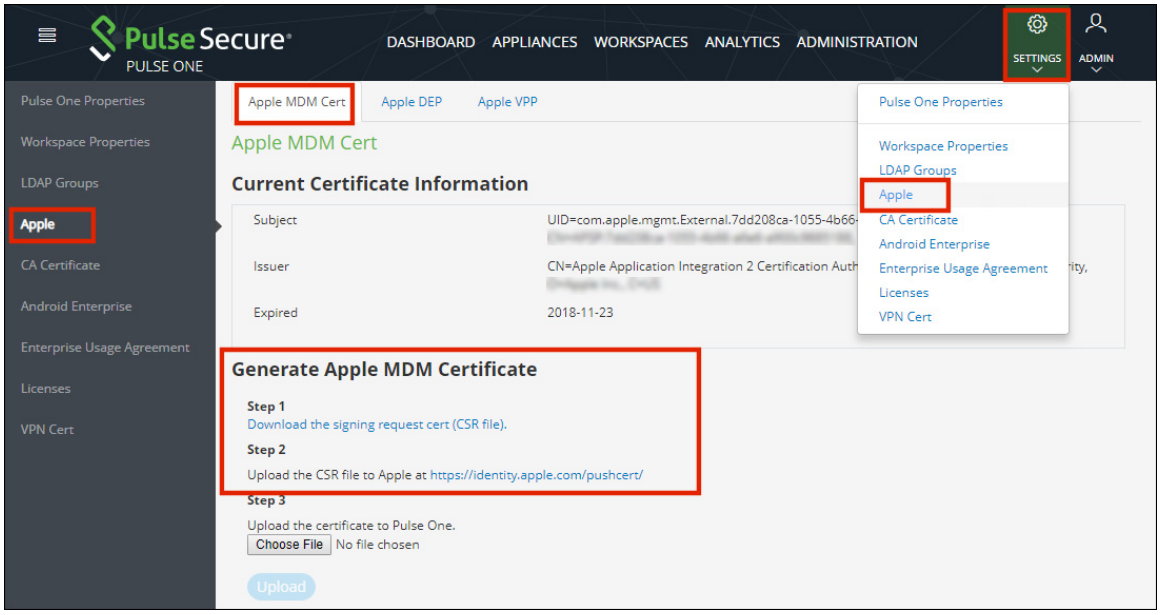
To add an iOS MDM certificate:

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

© 2019 Pulse Secure, LLC.

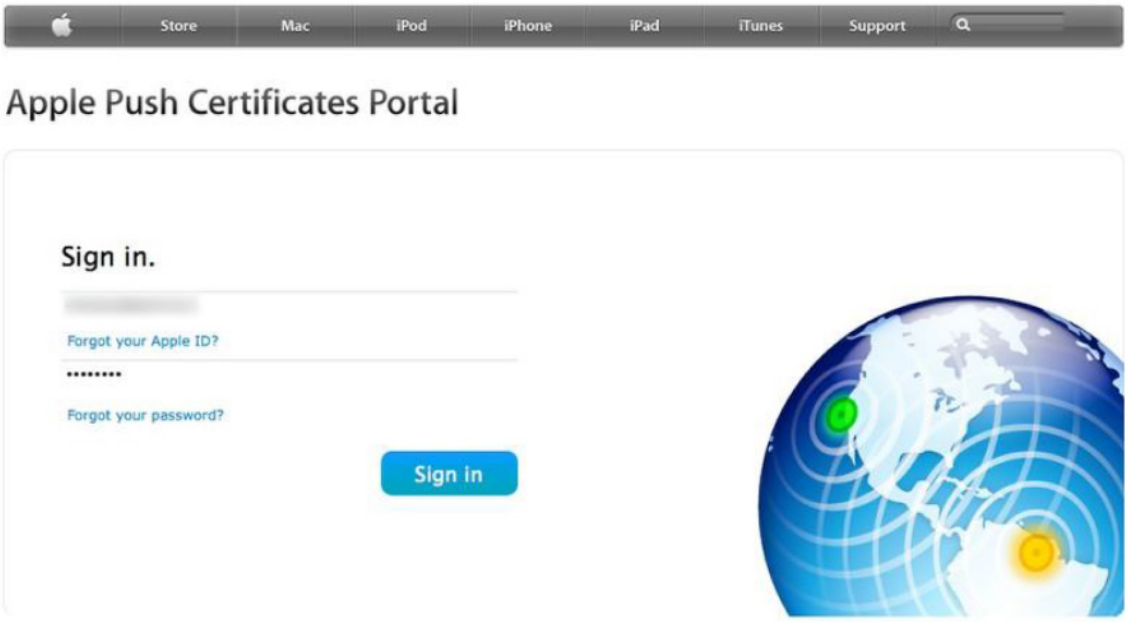
The **Apple MDM Cert** management page appears.

FIGURE 15 Apple MDM Cert page



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.

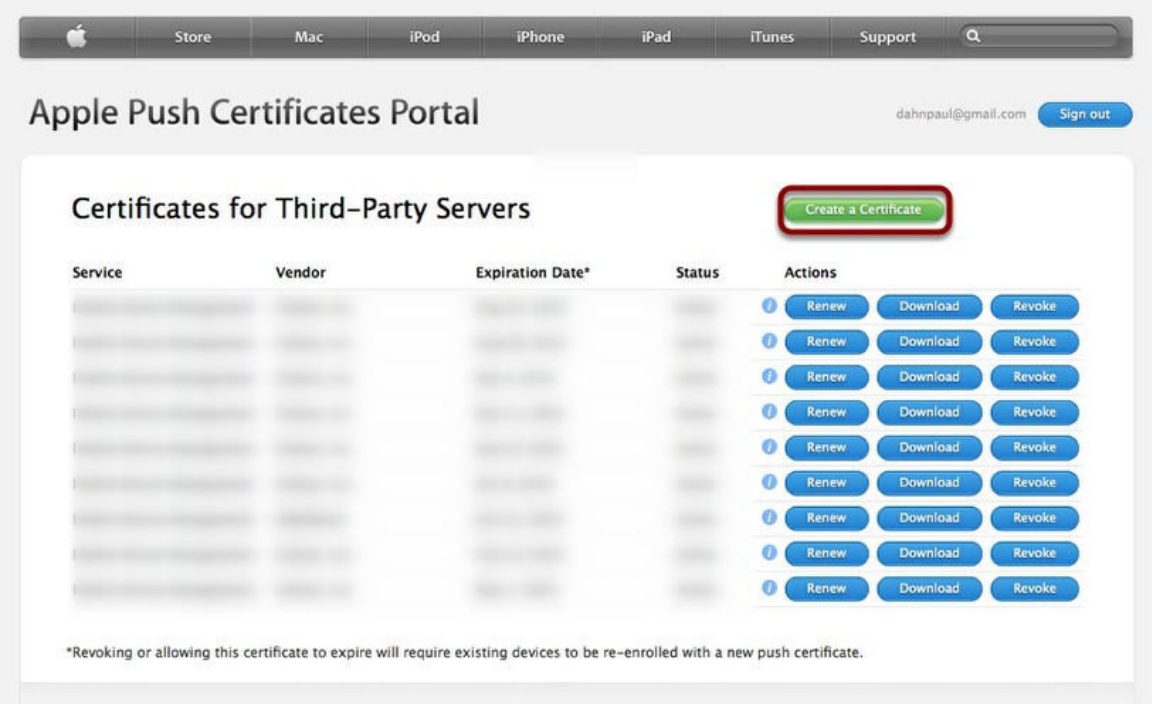
FIGURE 16 Log in to the Apple Push Certificates Portal



© 2019 Pulse Secure, LLC.

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

FIGURE 17 Create a New Certificate



7. Review and accept the terms of use.

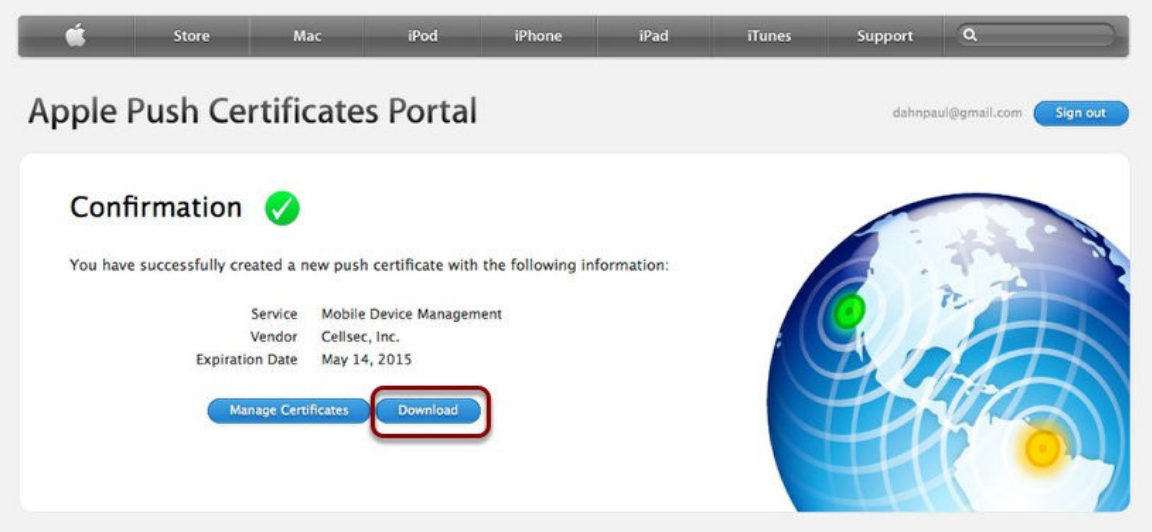
FIGURE 18 Accept Terms of Use

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

FIGURE 19 Upload Certificate Signing Request

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

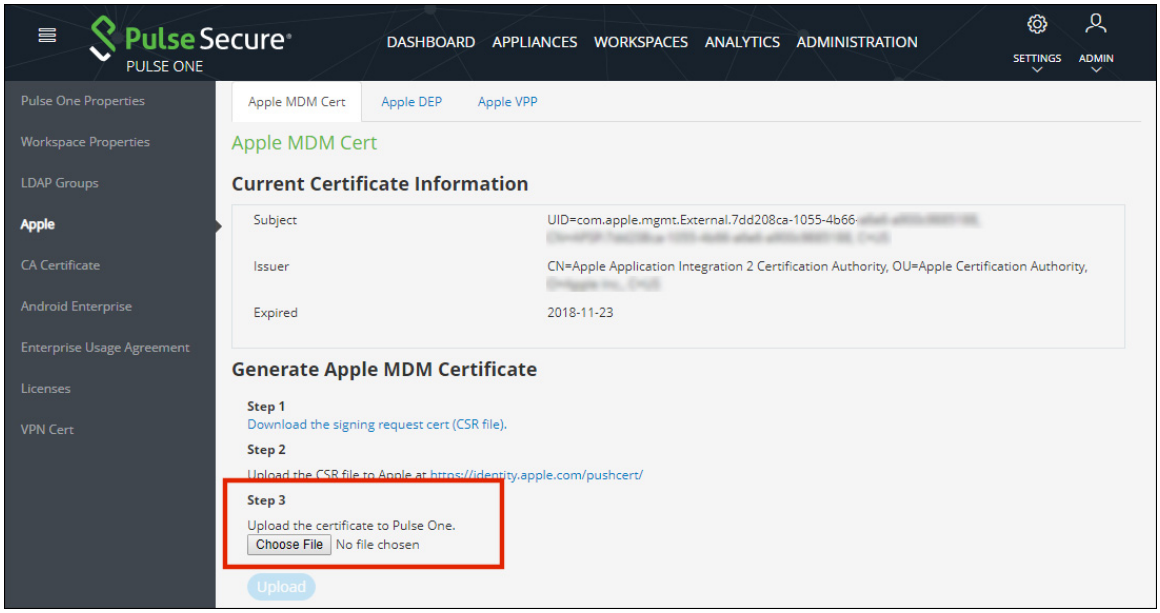
FIGURE 20 Download Signed Certificate



© 2019 Pulse Secure, LLC.

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

FIGURE 21 Upload Signed Certificate

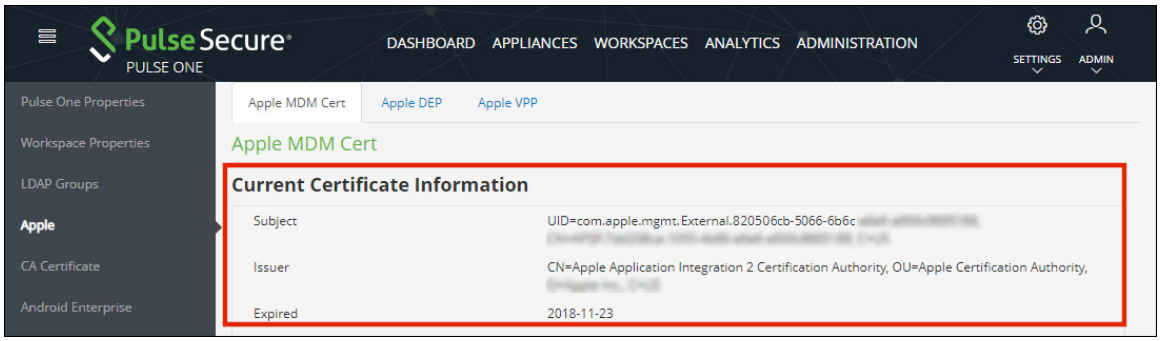


11. Click **Browse** and select the PEM file you downloaded from the Apple Push Certificates Portal.

12. Click **Upload**.

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

FIGURE 22 Review Certificate

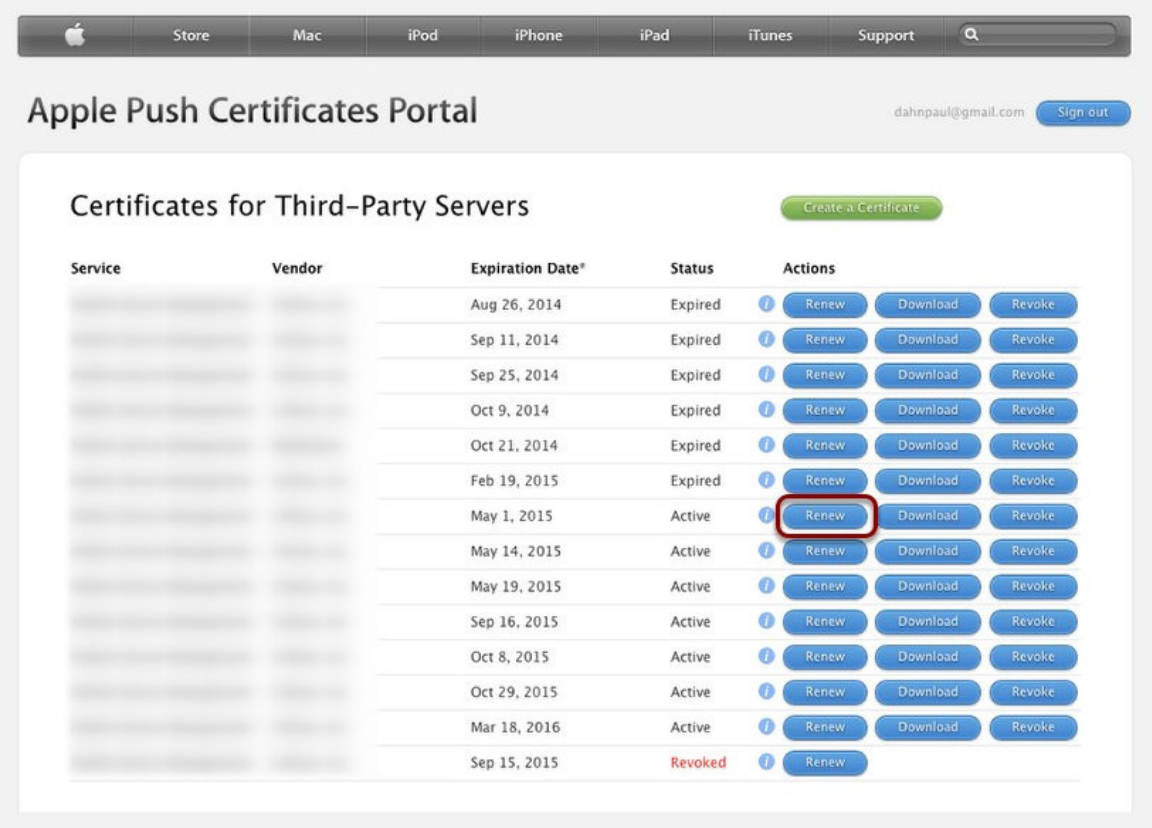


© 2019 Pulse Secure, LLC.

To renew a certificate:

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

FIGURE 23 Renew Certificate



© 2019 Pulse Secure, LLC.

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

FIGURE 24 Renew Push Certificate

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.

© 2019 Pulse Secure, LLC.

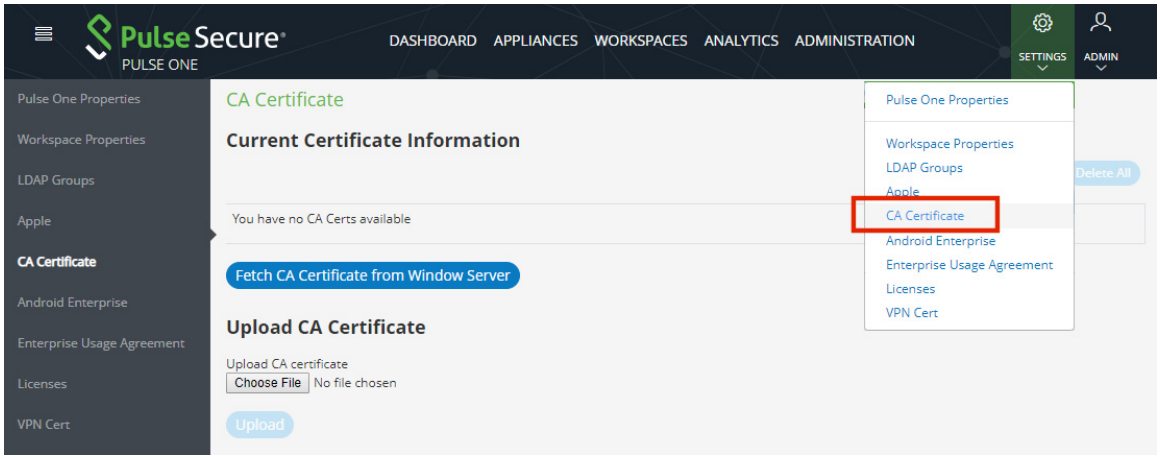
The **CA Certificate** page provides the following options to the Pulse One administrator:

- 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 25 CA Certificate Page



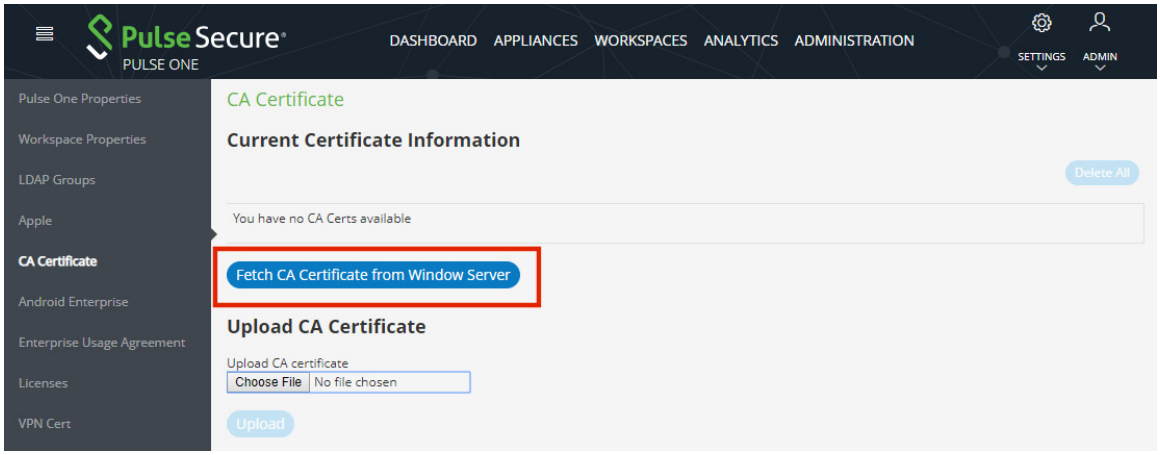
Note: The **Fetch CA Certificate from Windows Server** button is only displayed when you have an external PKI server configured, see **"Configuring an External PKI Server" on page 31**.

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

© 2019 Pulse Secure, LLC.

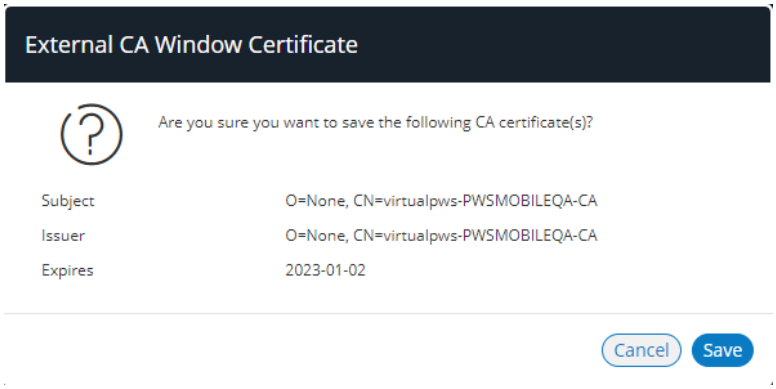
5. (Optional) If an external PKI server is configured, you can click **Fetch CA Certificate from Windows Server**. See **"Configuring an External PKI Server" on page 31** for details of the required configuration.

FIGURE 26 Fetch CA Certificate



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

FIGURE 27 Confirm CA Certificate



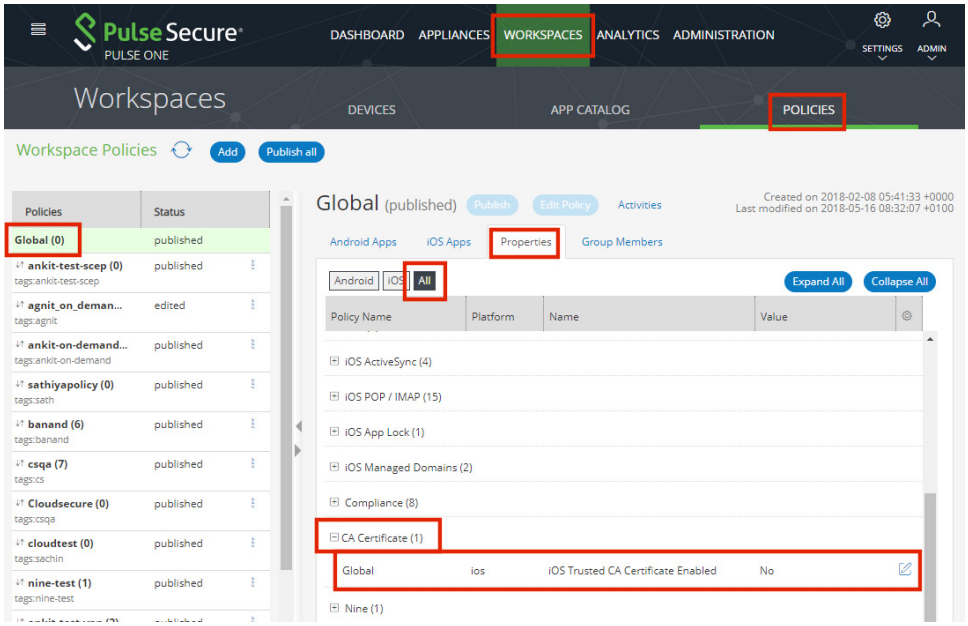
Click **Save** to add the CA certificate.

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

© 2019 Pulse Secure, LLC.

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

FIGURE 28 CA Certificate Settings



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

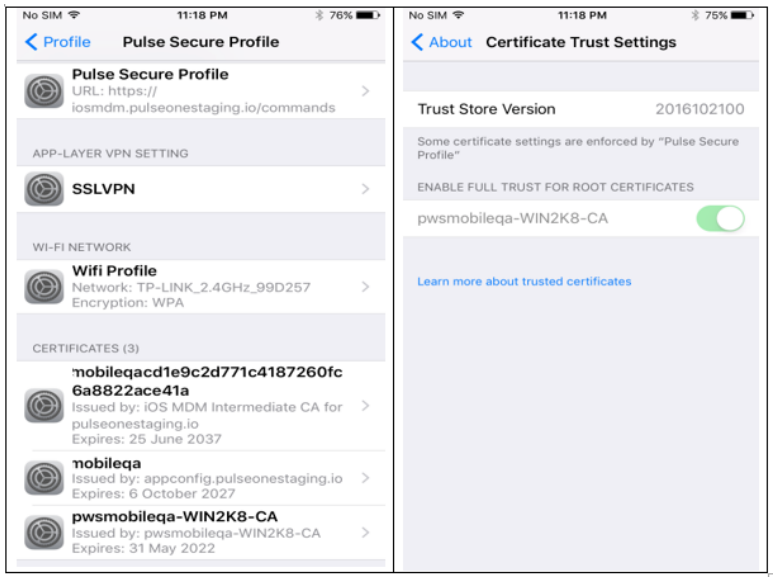
9. Click **Publish**.

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.

© 2019 Pulse Secure, LLC.

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

FIGURE 29 CA Certificate



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/*

© 2019 Pulse Secure, LLC.

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.

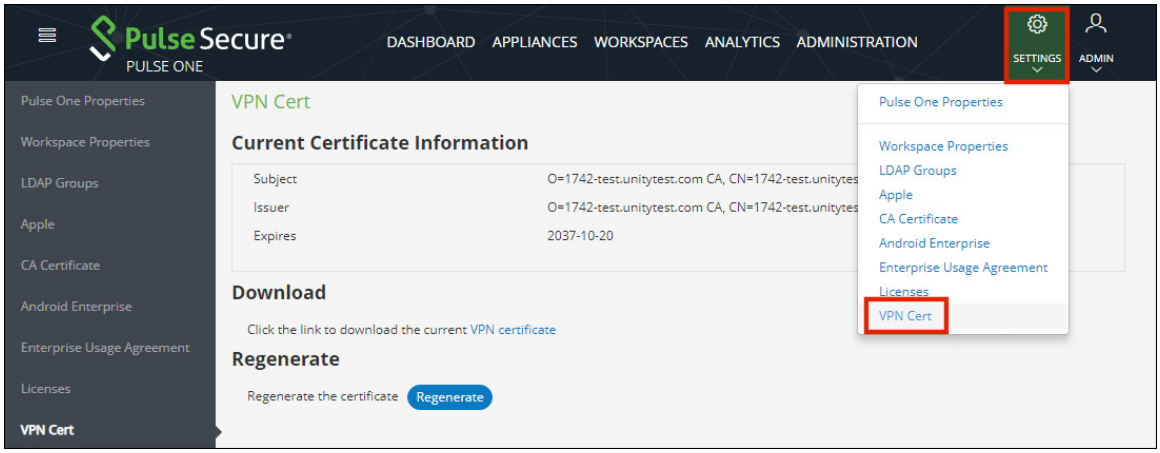
The configuration is complete.

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 30 Download VPN Root Certificate



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.

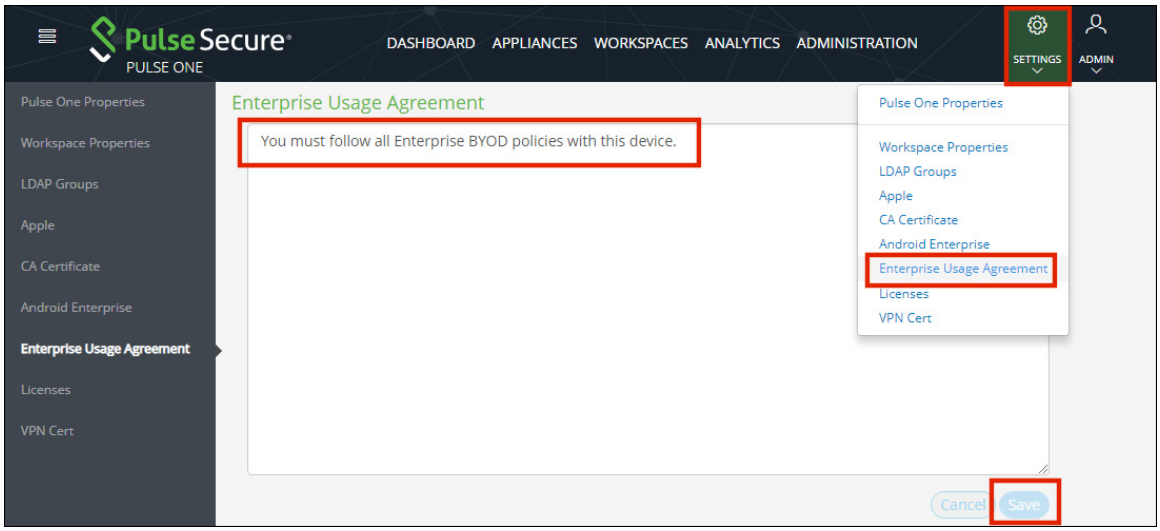
© 2019 Pulse Secure, LLC.

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 31 Navigate to Enterprise Usage Agreement



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

Viewing Activity Logs

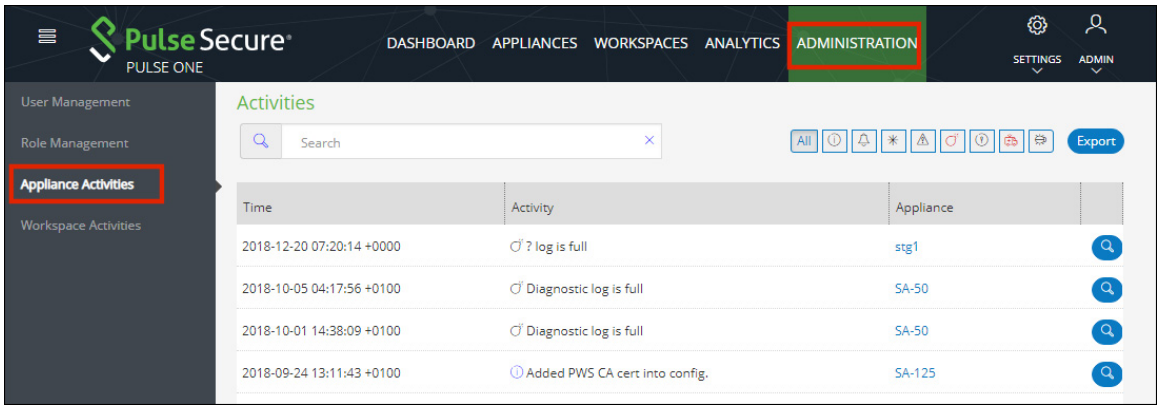
The Activity Logs display information about the events registered in the Management Server. These include Appliance and Workspace activities. You can view filtered Activities for Users, Workspaces or Policies.

To view Appliance activities:

© 2019 Pulse Secure, LLC.

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

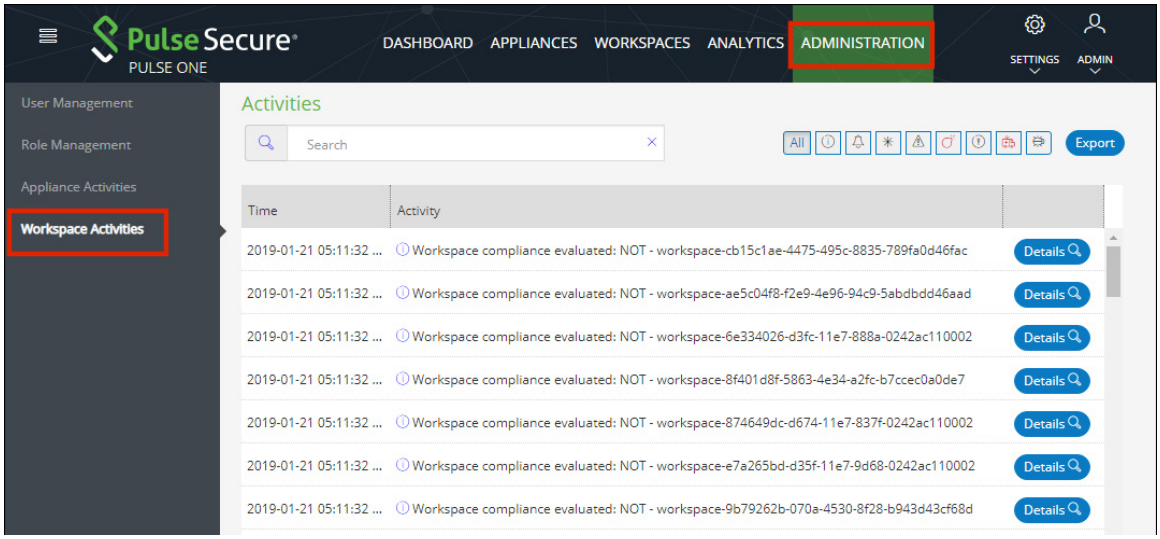
FIGURE 32 Appliance Activities



To view Workspace activities:

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

FIGURE 33 Workspace Activities



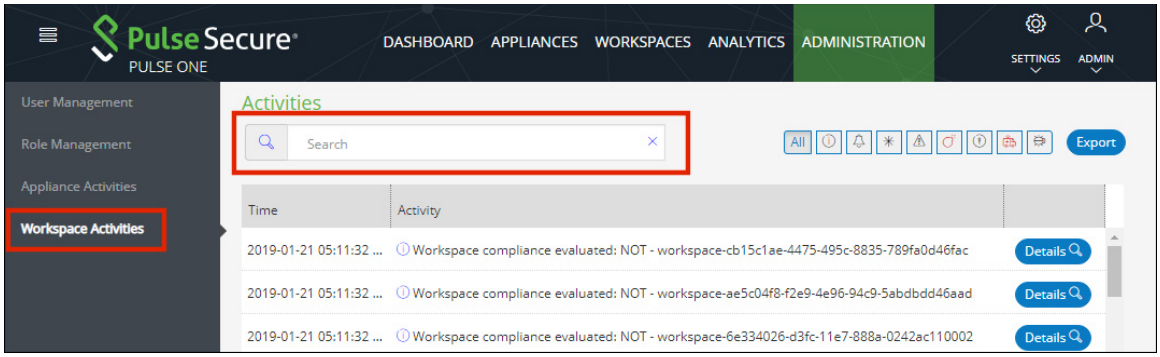
© 2019 Pulse Secure, LLC.

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:

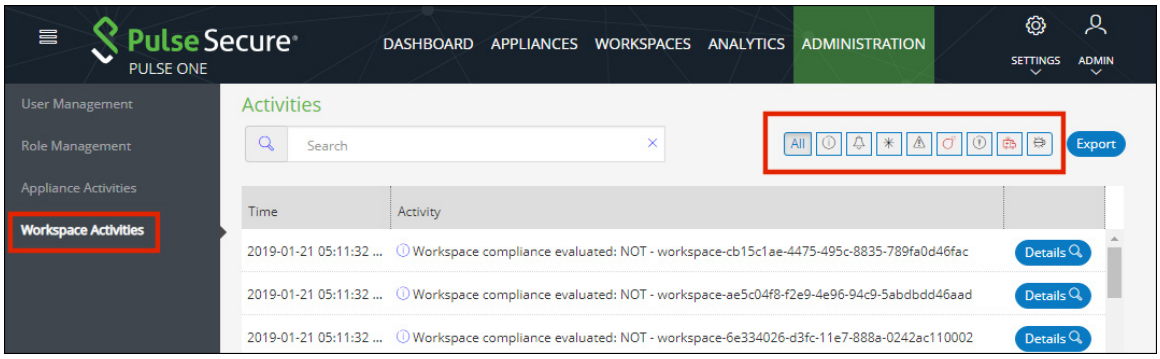
FIGURE 34 Search Activity



Filtering Activities

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

FIGURE 35 Filter Activities

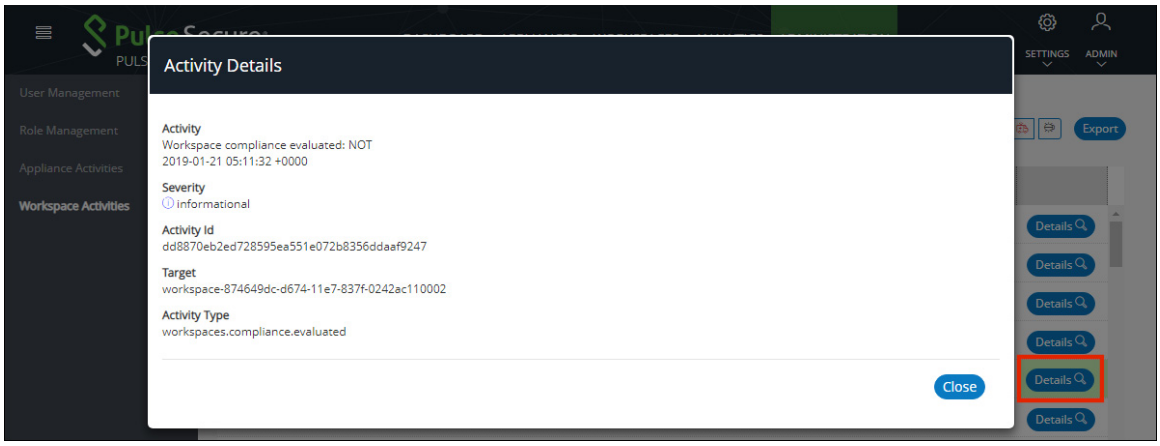


© 2019 Pulse Secure, LLC.

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 36 Activity Details



Licensing Pulse One and Pulse Workspace

The **Licenses** screen lists:

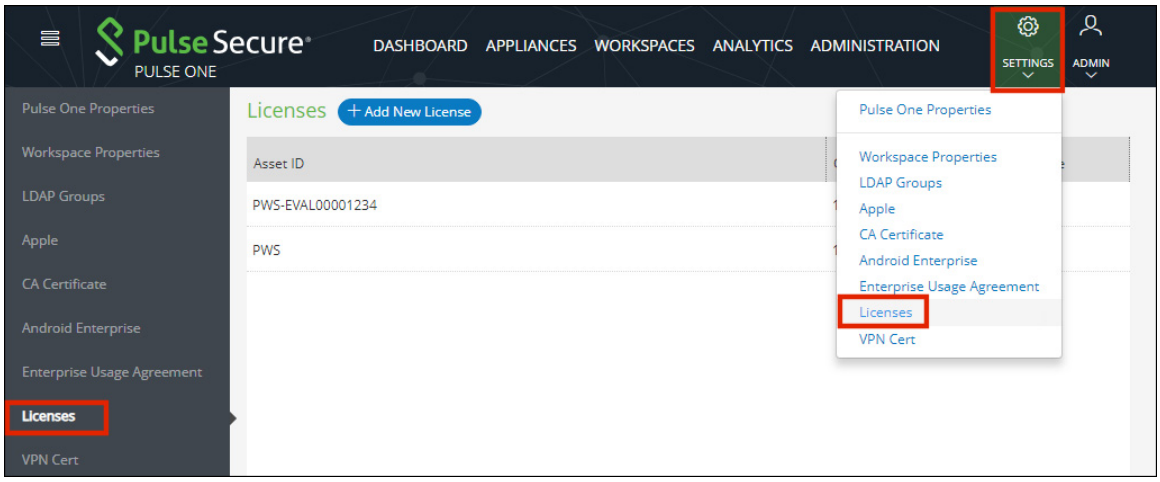
- Licenses, identified by their **Asset ID**.
- The **Quantity** of each license available.
- The license **Expiration Date**.

© 2019 Pulse Secure, LLC.

To view licenses:

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

FIGURE 37 License Details



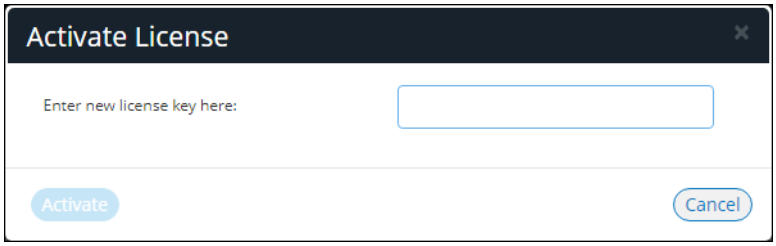
You can add one or more Pulse One and Pulse Workspace licenses on the **Licenses** page.

To add a new license:

1. Click **Add New License**.

   The **Activate License** dialog appears.

FIGURE 38 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.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Provisioning Devices

- Features Supported on iOS and Android Devices 39
- Understanding Managed Devices and Managed Clients 41
- Onboarding iOS BYOD Devices 41
- Onboarding Android BYOD Devices 51
- Configuring Corporate-Owned iOS Devices 58
- Configuring Corporate-Owned Android Devices 58
- Configuring Managed Clients 67

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.

© 2019 Pulse Secure, LLC.

- **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 165**.
- **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 Android v6.0.1+ 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**: The 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, such as whether the device is rooted. If the device is non- compliant, additional actions are provided to the end-user.

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 165**.

© 2019 Pulse Secure, LLC.

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 clients?** workspace property, see **"Workspaces" on page 149**.

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

For full details of managed clients, see **"Configuring Managed Clients" on page 67**.

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.

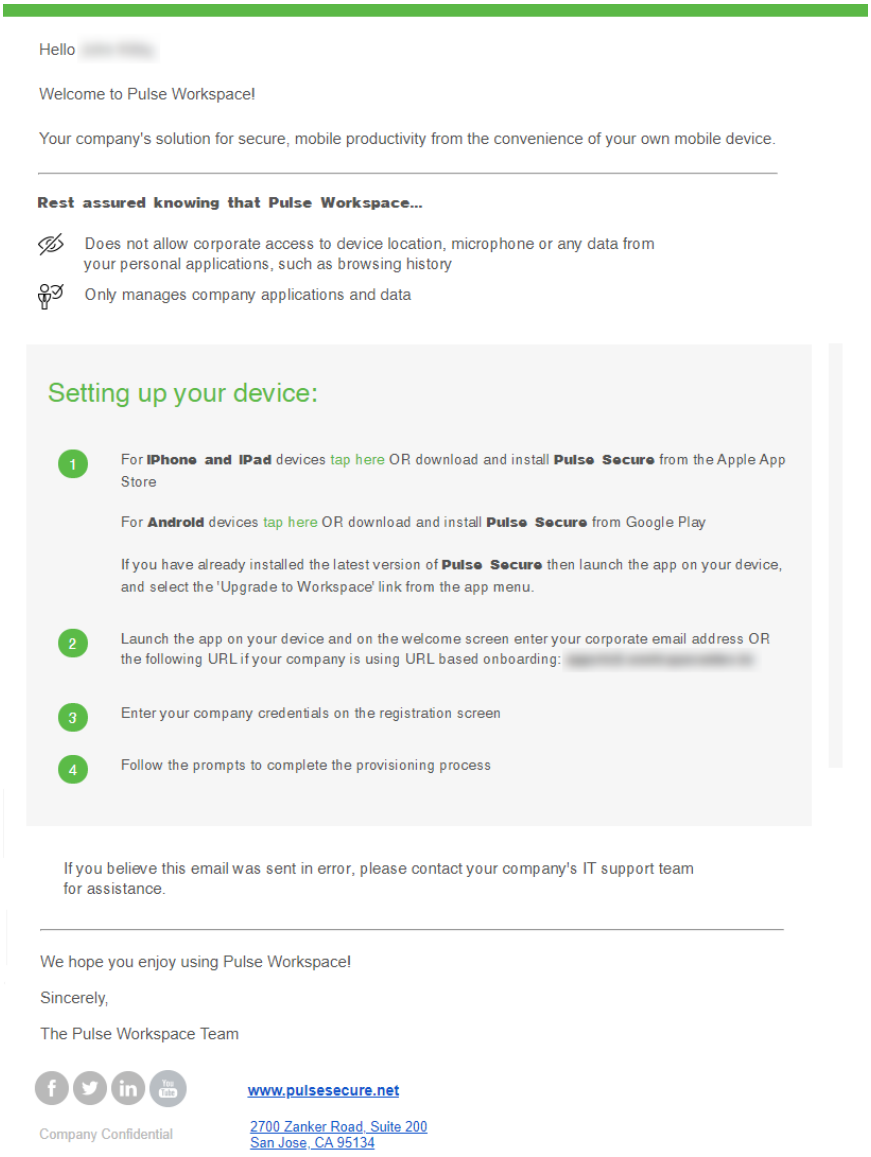
- **"Understanding Your SAML-Based Authentication Email" on page 42**.
- **"Understanding Your PIN-Based Authentication Email" on page 43**.
- **"Registering an iOS BYOD Device" on page 44**.

© 2019 Pulse Secure, LLC.

Understanding Your SAML-Based Authentication Email

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

FIGURE 39 Welcome Email: SAML Authentication



This email contains:

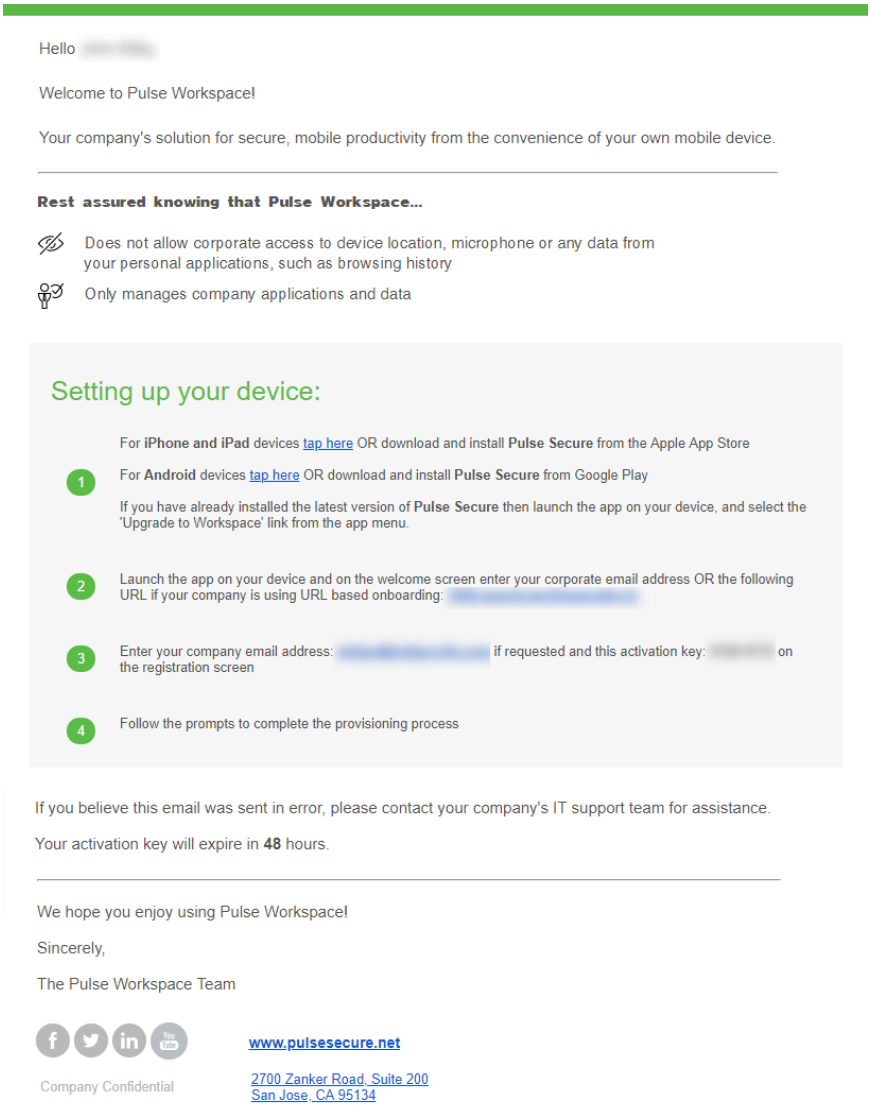
- A registration link to download and install Pulse Secure from Apple App Store for iPhone or iPad devices.
- An Enterprise URL.
- Instructions for completing the device registration.

© 2019 Pulse Secure, LLC.

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 40 Welcome Email: PIN Authentication



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.

© 2019 Pulse Secure, LLC.

Registering an iOS BYOD Device

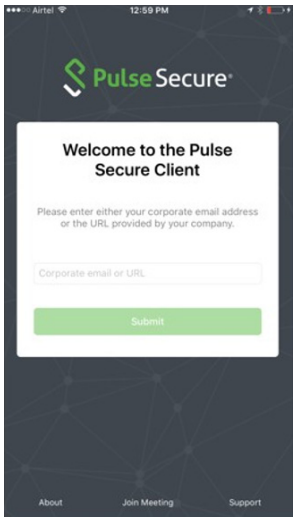
Note: Starting at iOS 12.2, Apple has changed the manual enrollment flow for Mobile Device Management (MDM), see **https://support.apple.com/en-us/HT209435**. As a result, installing the MDM profile involves some additional steps for end users who perform manual enrollment on their Apple device running 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 41 Welcome

   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.

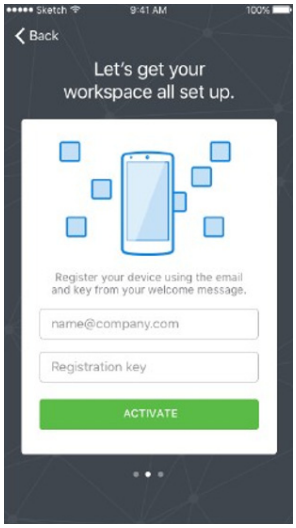
   On this screen, enter your corporate user name and password and click **Sign In**.

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

© 2019 Pulse Secure, LLC.

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

FIGURE 42 Entering your 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.

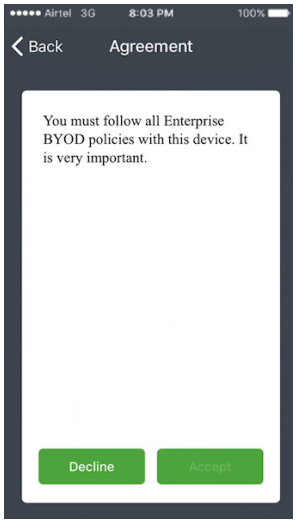
Note: To set up the Auto-Discovery experience, you will need to contact Pulse Secure Technical support through a DevOps ticket. After the needed information is provided (and validated), Technical Support will enable the Auto-Discovery experience for your Email Domain.

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

© 2019 Pulse Secure, LLC.

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

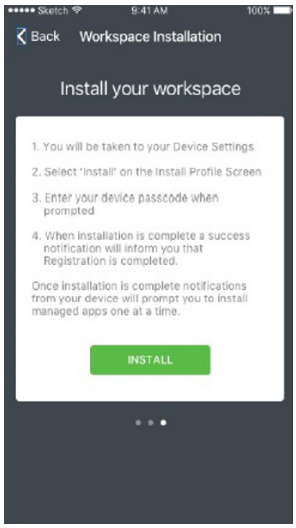
FIGURE 43 Enterprise BYOD Policies



The **Install Your Workspace** page appears.

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

FIGURE 44 Workspace Installation



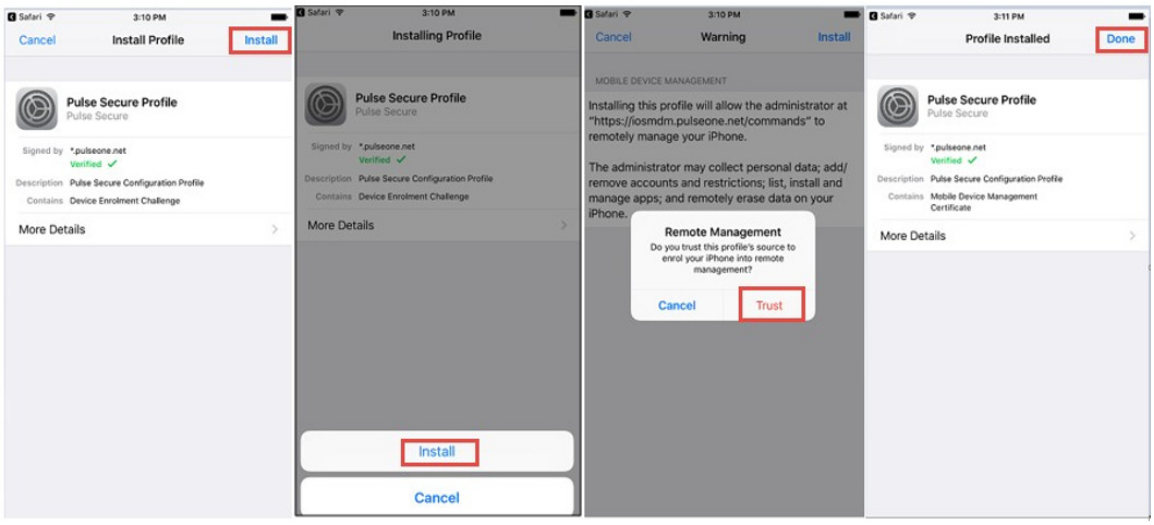
© 2019 Pulse Secure, LLC.

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:

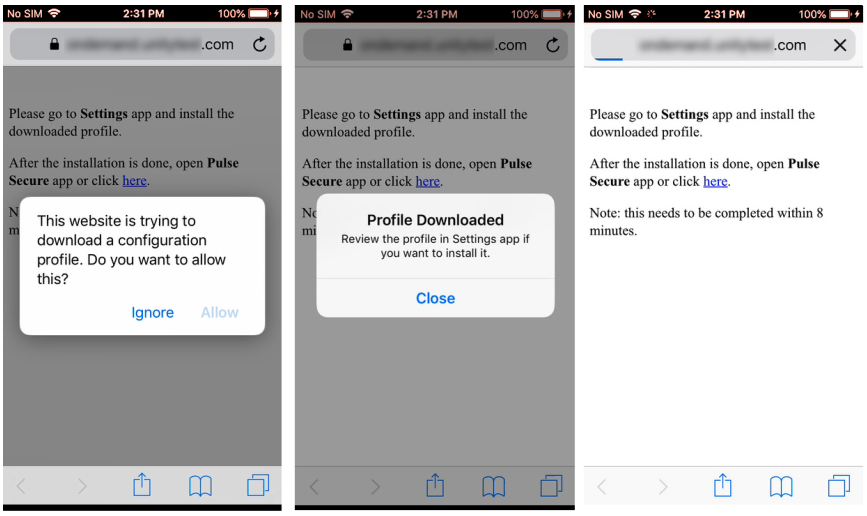
     FIGURE 45 Installing the Pulse Secure Profile Workspace Server Certificate

   - 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 46 Downloading a Profile

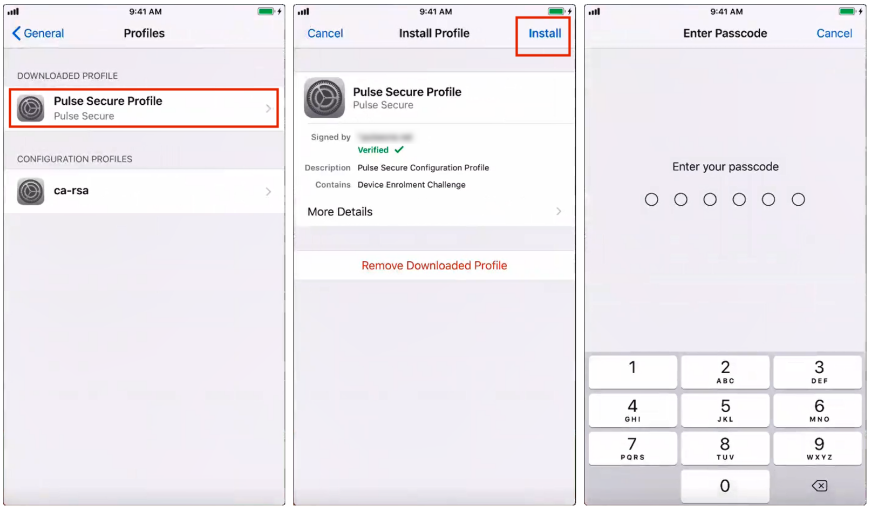
     On the **iOS Device Registration** page, press **Allow**, and then **Close**.

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

© 2019 Pulse Secure, LLC.

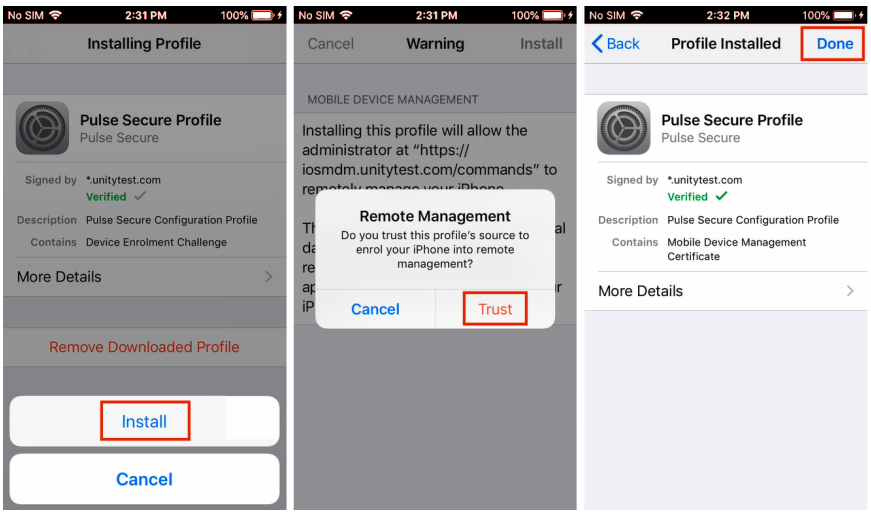
You must then manually access **Settings > General > Profiles**. Press the **Pulse Secure Profile**, then **Install**, and then enter your passcode.

FIGURE 47 Installing a Profile



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

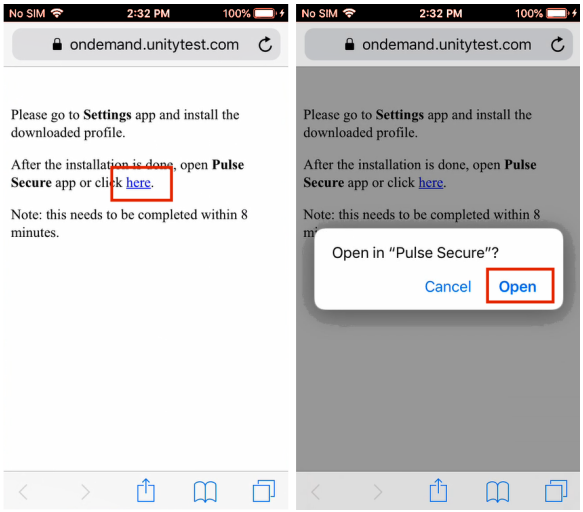
FIGURE 48 Installing a Profile: Complete



© 2019 Pulse Secure, LLC.

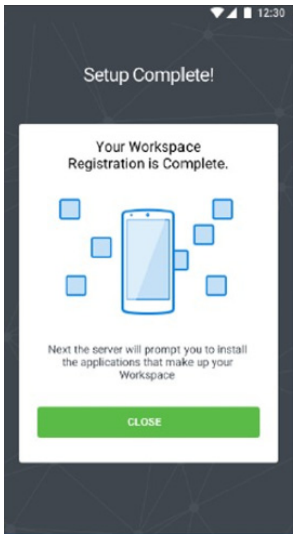
You can then return to the **iOS Device Registration** page and click the hyperlink to complete and then press **Open** to complete this manual process.

FIGURE 49 Opening a Profile



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

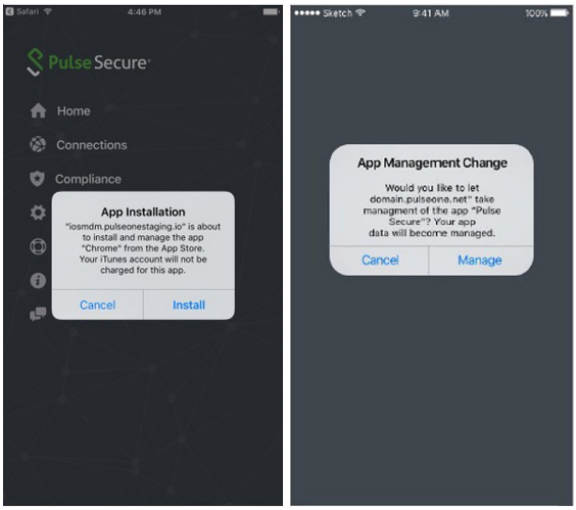
FIGURE 50 Setup Complete



© 2019 Pulse Secure, LLC.

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 51 Post Enrollment Configuration



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 41**. For example, managed clients will not install any applications after enrollment.

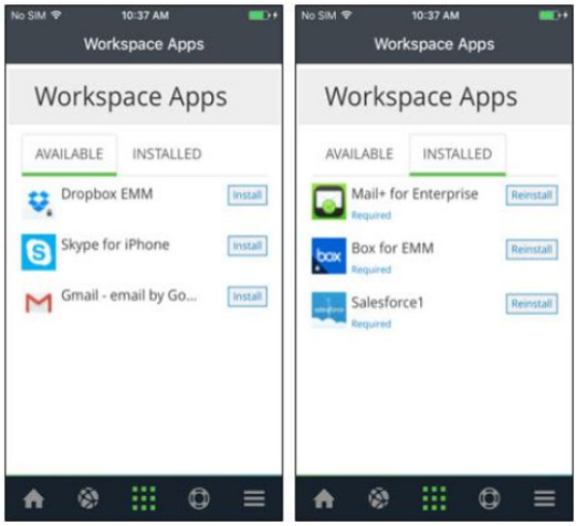
To install apps manually on a managed device:

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

© 2019 Pulse Secure, LLC.

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

FIGURE 52 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:

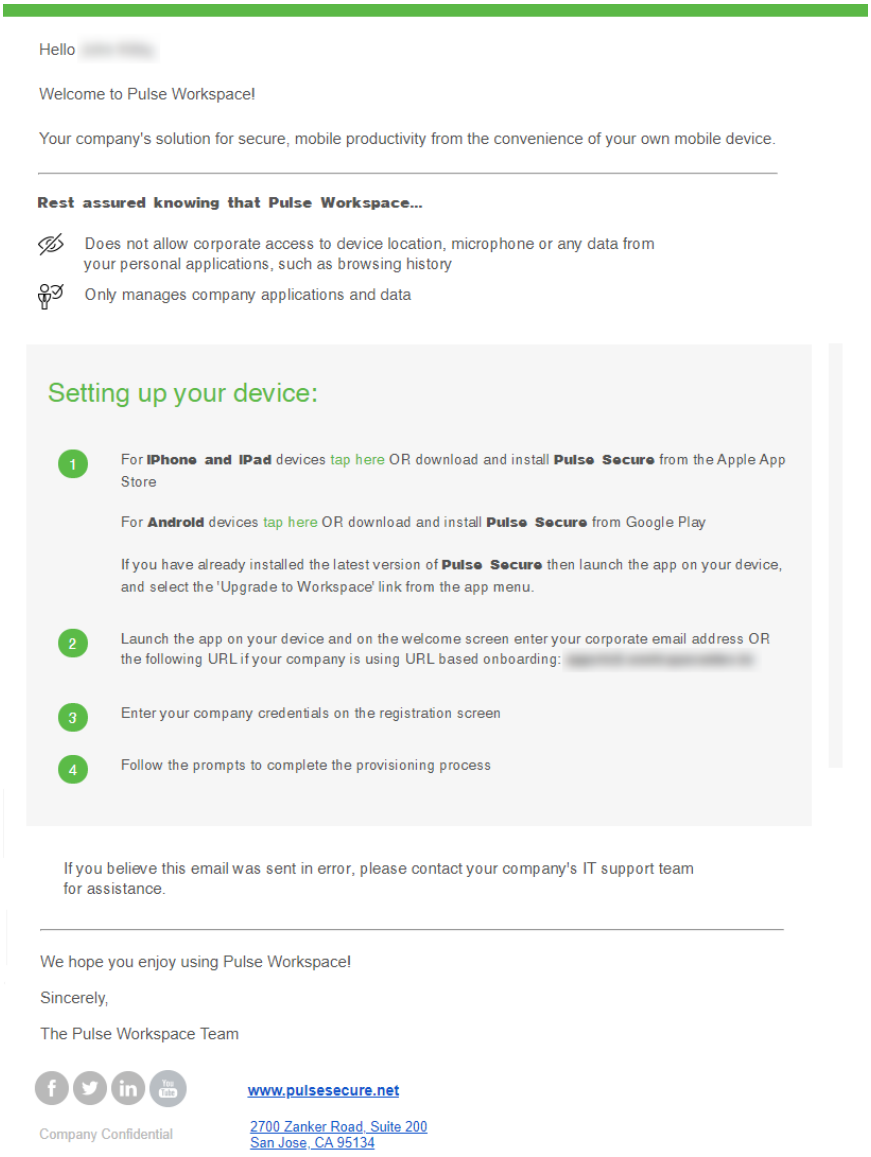
- **"Understanding Your SAML-Based Authentication Email" on page 52**.
- **"Understanding Your PIN-Based Authentication Email" on page 53**.
- **"Registering Your Android BYOD Device" on page 54**.

© 2019 Pulse Secure, LLC.

Understanding Your SAML-Based Authentication Email

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

FIGURE 53 Welcome Email: SAML Authentication



This email contains:

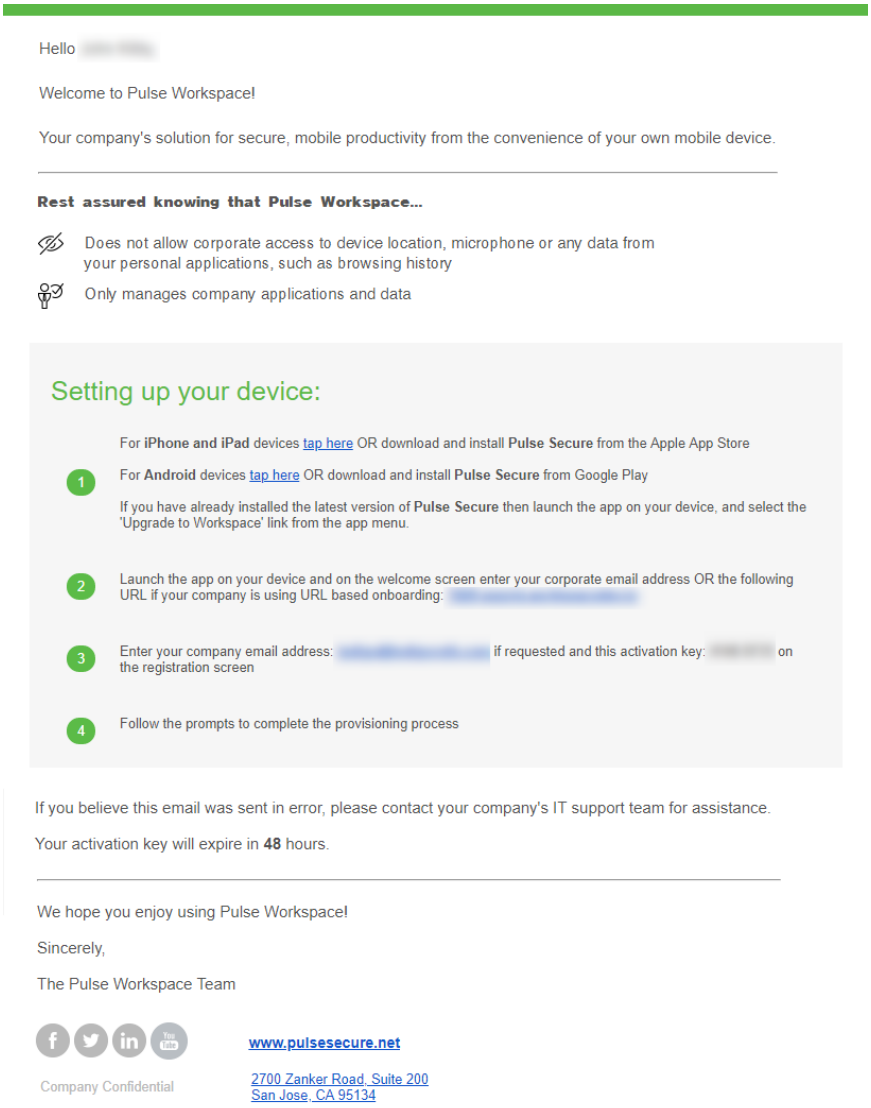
- A registration link to download and install Pulse Secure from the Google Play store.
- An Enterprise URL.
- Instructions for completing the device registration.

© 2019 Pulse Secure, LLC.

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 54 Welcome Email: PIN Authentication



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.

© 2019 Pulse Secure, LLC.

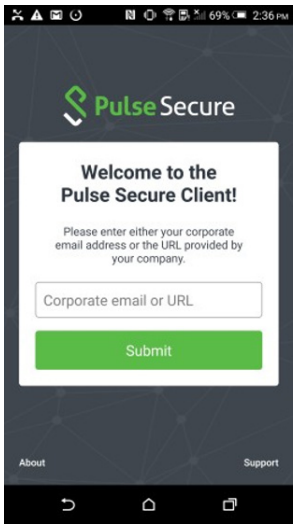
Registering Your Android BYOD Device

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 55 Welcome

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.

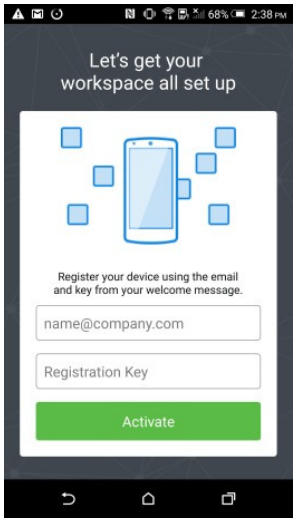
   On this screen, enter your corporate user name and password and click **Sign In**.

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

© 2019 Pulse Secure, LLC.

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

FIGURE 56 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.

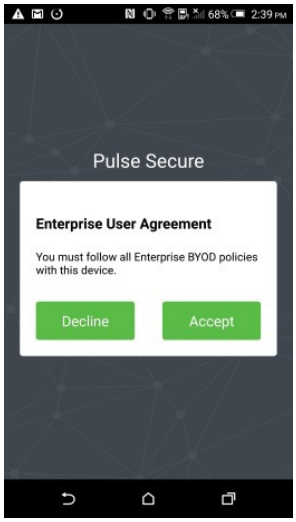
Note: To set up the Auto-Discovery experience, you will need to contact Pulse Secure Technical Support using a DevOps ticket. After the needed information is provided (and validated), Technical Support will enable the Auto-Discovery experience for your Email Domain.

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

© 2019 Pulse Secure, LLC.

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

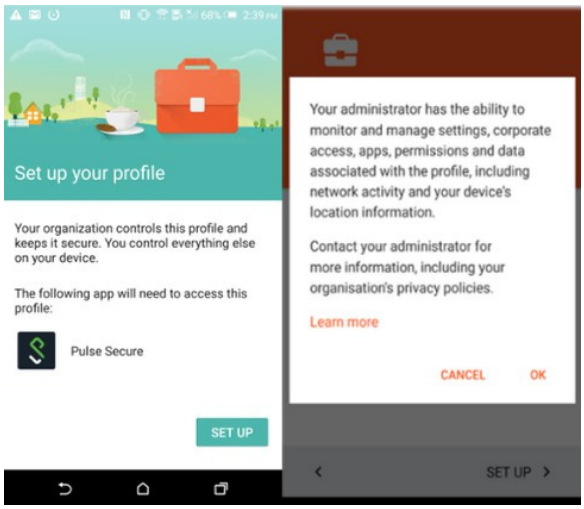
FIGURE 57 Enterprise User Agreement



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

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

FIGURE 58 Set Up Your Profile



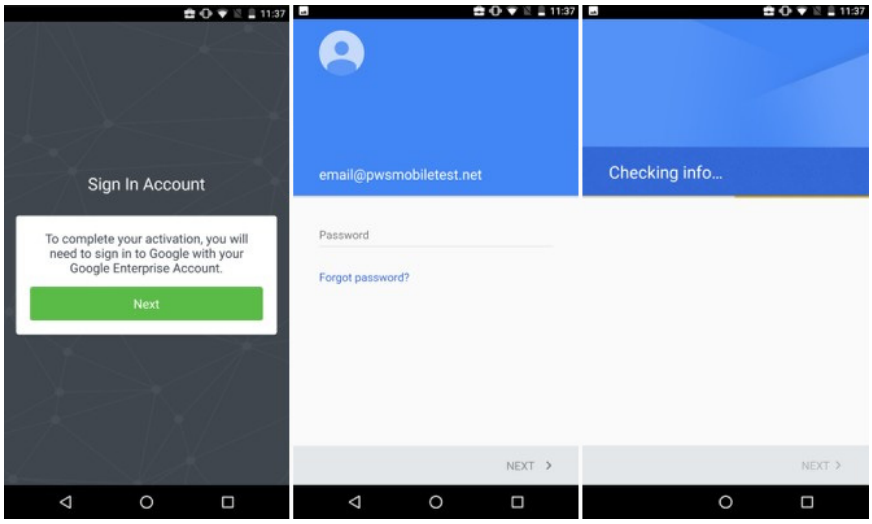
Note: If the device is not encrypted, Google will prompt to encrypt the device with encrypt option and then will reboot the device.

© 2019 Pulse Secure, LLC.

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

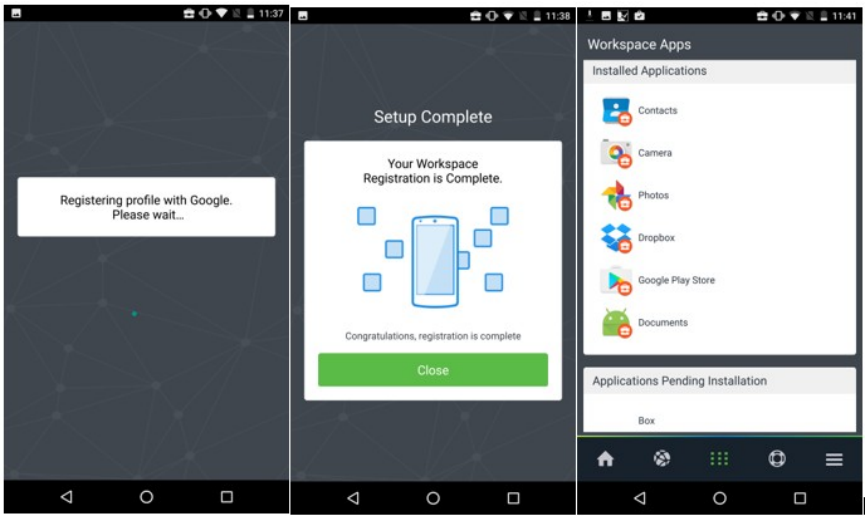
    - If the user's Google account does not exist, then user is prompted with the **Create Account** page.
    - If the Google account exists, the user is taken to the **Signing in Account** page. Press **NEXT** to sign into Google with your Google Enterprise Account.

FIGURE 59 Google Account



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

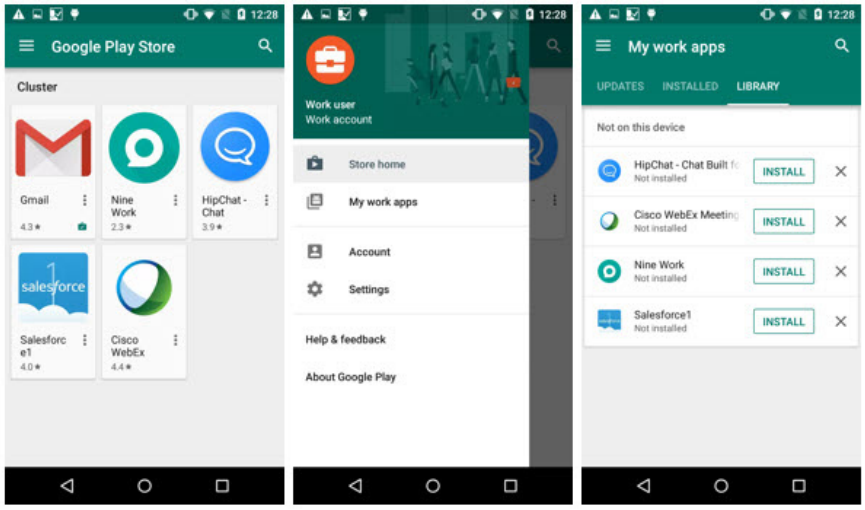
FIGURE 60 Workspace Apps



© 2019 Pulse Secure, LLC.

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

FIGURE 61 Workspace Apps Library



Configuring Corporate-Owned iOS Devices

Apple's Device Enrollment Program (DEP) provides a fast, streamlined way to deploy iOS and macOS 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 prep the devices before users get them. And with MDM, you can further simplify the setup process for users by removing specific steps in the Setup Assistant, so users are up and running quickly.

For full configuration details, refer to Apple Device Enrollment Program (DEP) section in the *Pulse Workspace Configuration Guide* in the Pulse One Cloud documentation.

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.

© 2019 Pulse Secure, LLC.

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:

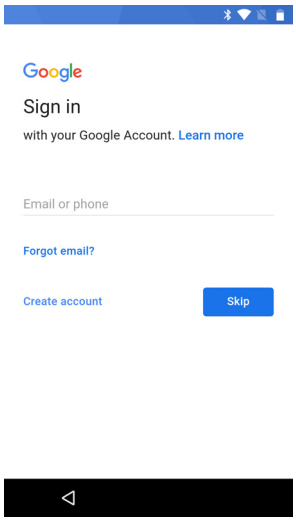
1. Log into the Pulse One appliance.
2. In the **Workspaces** menu, create (or edit) the required user. The user details should include:
    - The user's corporate email as the **Workspace Email**.
    - Your own email as the **Provisioning Email**, so that you receive the required registration information.
    - 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 62 Google Email

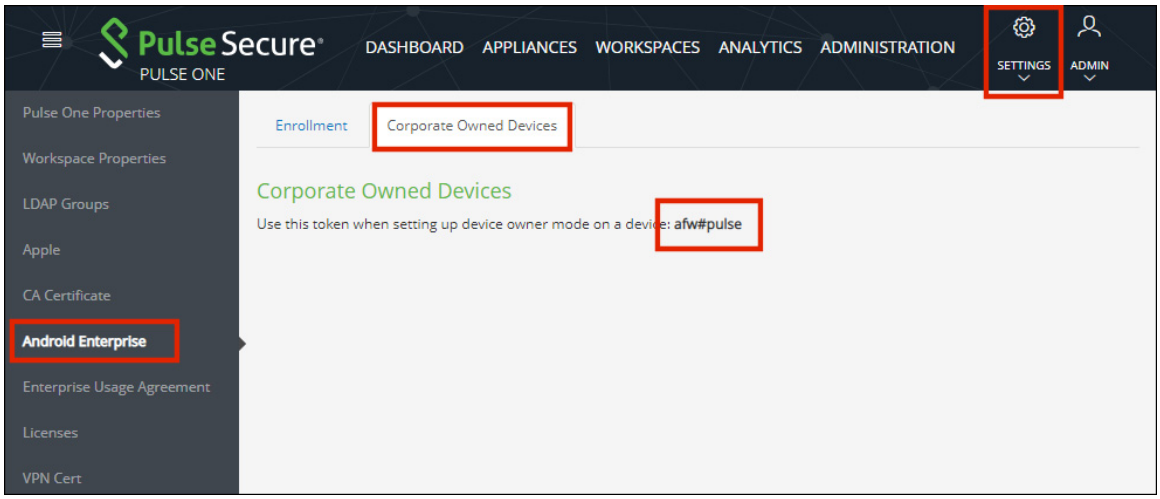


© 2019 Pulse Secure, LLC.

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

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

   FIGURE 63 Android Enterprise Settings



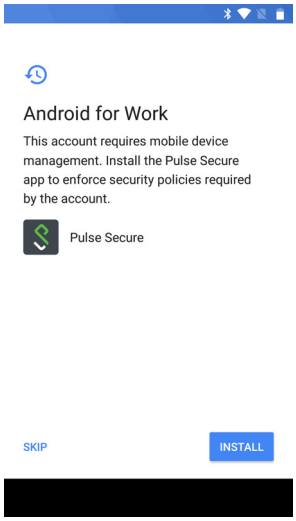
7. On the **Sign In** screen, press **Next**.

   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 64 Google Email



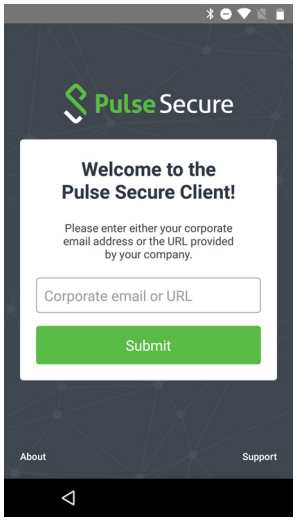
9. Click **Install**.

   Pulse Secure downloads and installs.

© 2019 Pulse Secure, LLC.

The Pulse Secure **Welcome** screen appears.

FIGURE 65 Welcome



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.

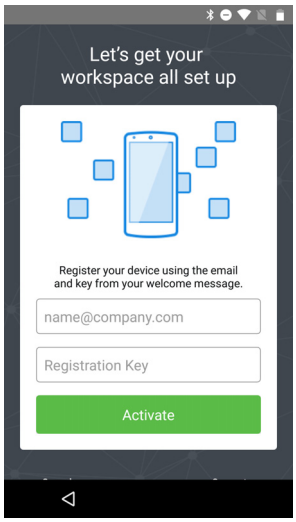
11. (Optional) If you are using a SAML-based registration, the SAML **Login** screen appears.

    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 66 Registration Key



© 2019 Pulse Secure, LLC.

On this screen:

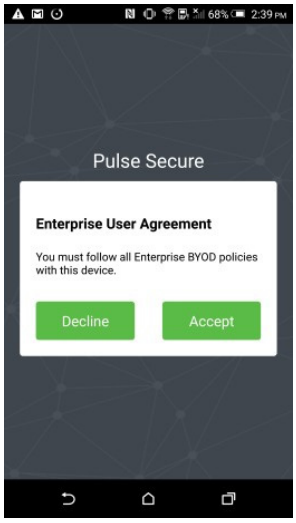
- Enter your corporate email address.
- Enter your registration key from your welcome email.
- Click **Activate**.

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.

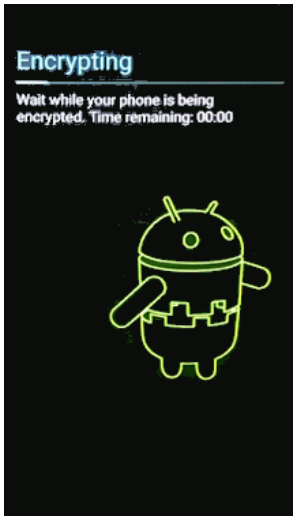
FIGURE 67 Enterprise User Agreement



© 2019 Pulse Secure, LLC.

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:

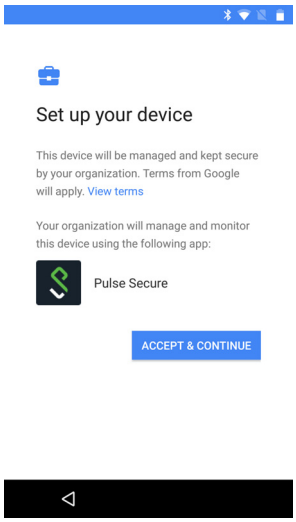
FIGURE 68 Encrypting



When encryption completes, the device reboots.

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

FIGURE 69 Set Up Work Device

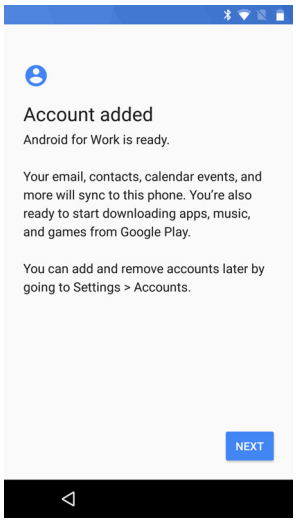


© 2019 Pulse Secure, LLC.

15. Click **Accept and Continue**.

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

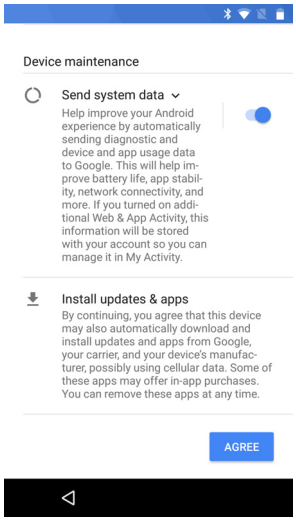
    FIGURE 70 Account Added



16. Click **Next**.

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

    FIGURE 71 Device Maintenance

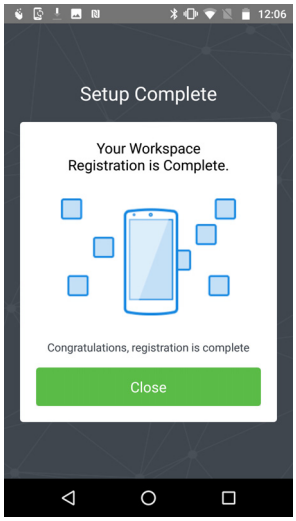


    Work through these screens without making changes.

© 2019 Pulse Secure, LLC.

The **Setup Complete** page then appears.

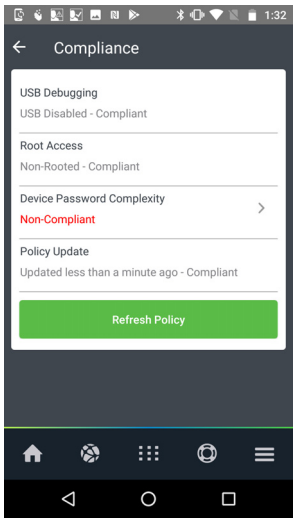
FIGURE 72 Setup Complete



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 73 Compliance



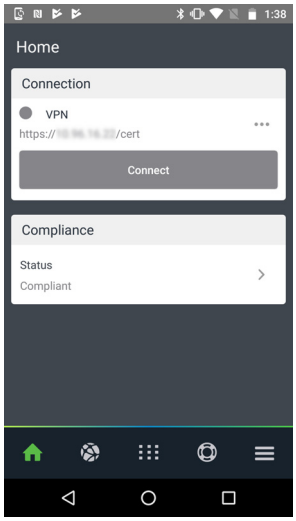
18. Make any required changes to bring your device into compliance.

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.

© 2019 Pulse Secure, LLC.

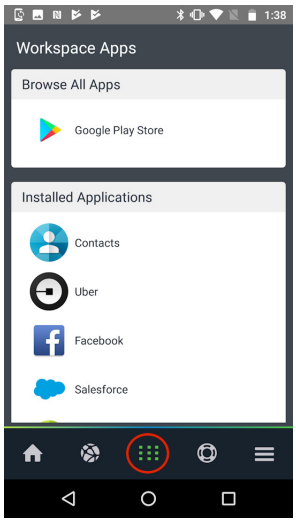
After this is complete, the Pulse Secure **Home** page then appears. For example:

FIGURE 74 Home



19. Press to see installed apps. For example:

FIGURE 75 Workspace Apps



The registration process is complete.

© 2019 Pulse Secure, LLC.

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 41**.

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 67**.
- **"Configuring VPN on Demand for Managed Clients" on page 67**.
- **"Enrolling Personal Devices as Managed Clients" on page 78**.

Enabling Managed Client Mode

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

Note: If the **Enable enrollment of managed clients?** workspace property is *False*, Pulse Workspace will enroll devices as *managed devices*. Pulse Secure recommends that the **Enable enrollment of managed 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 67**.

Configuring VPN on Demand for Managed Clients

After you have enabled managed client mode (see **"Enabling Managed Client Mode" on page 67**) you can enable VPN on Demand for *managed client* mobile devices, and configure it for use:

- **"Understanding VPN on Demand" on page 68**.
- **"Understanding VPN on Demand Rules Criteria" on page 69**.
- **"Understanding VPN on Demand Action Parameters" on page 70**.
- **"Enabling and Configuring VPN on Demand" on page 71**.

© 2019 Pulse Secure, LLC.

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 69**.

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 70**. 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**

© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

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.

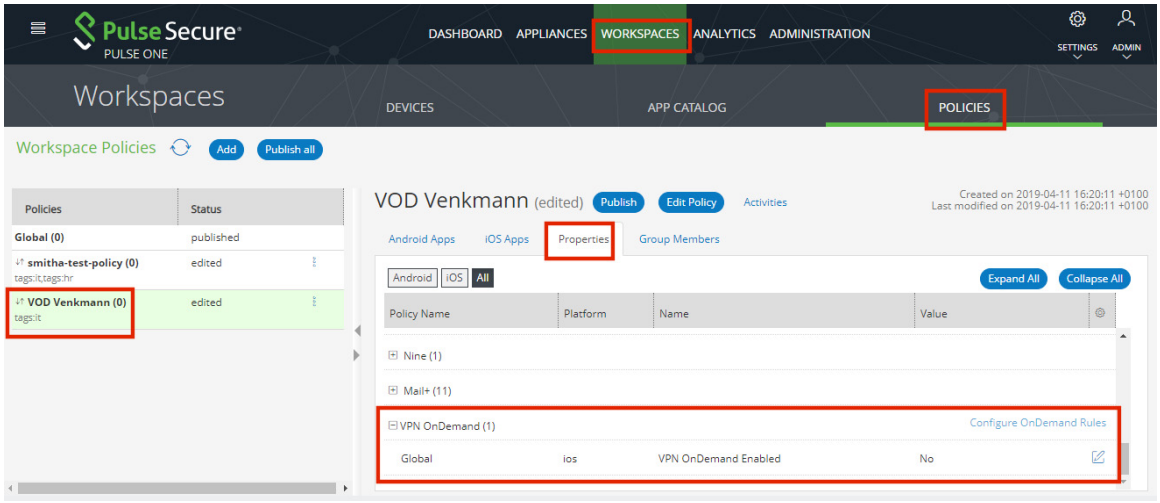
© 2019 Pulse Secure, LLC.

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 76 VPN on Demand: Policy Properties

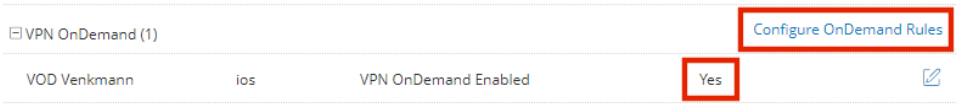


5. Set the **VPN OnDemand Enabled** property to *True*.

   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 77 VPN on Demand Enabled

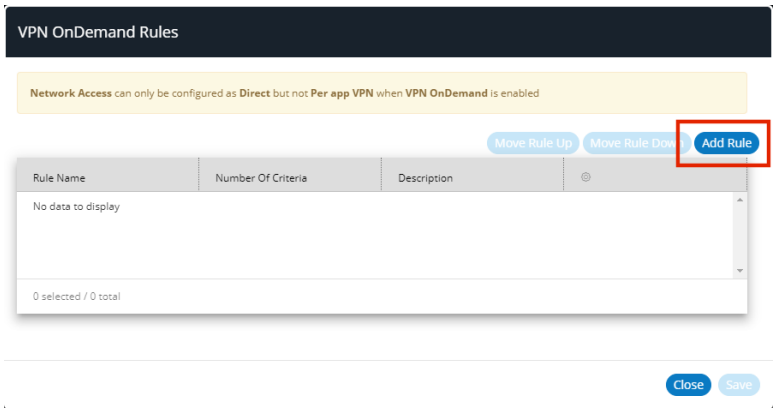


© 2019 Pulse Secure, LLC.

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:

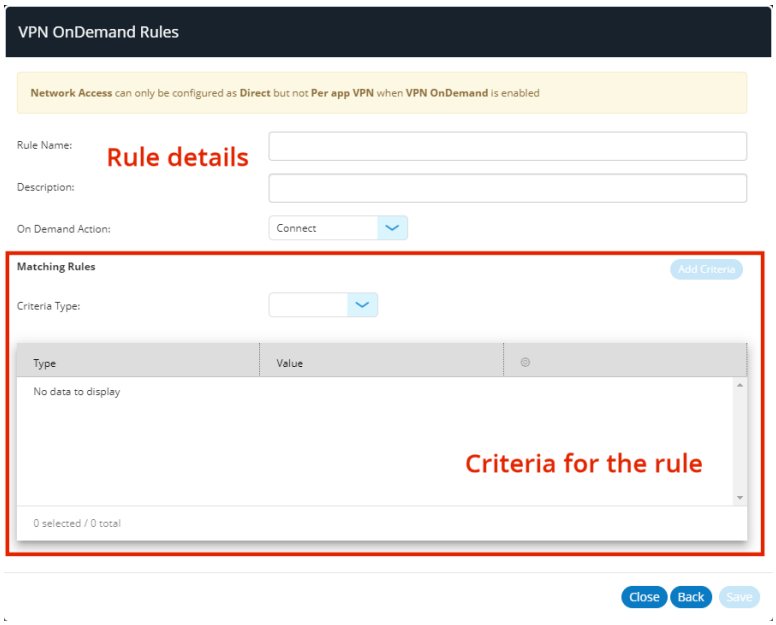
   FIGURE 78 VPN On Demand: List of Rules



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 79 VPN on Demand: Rule Definition



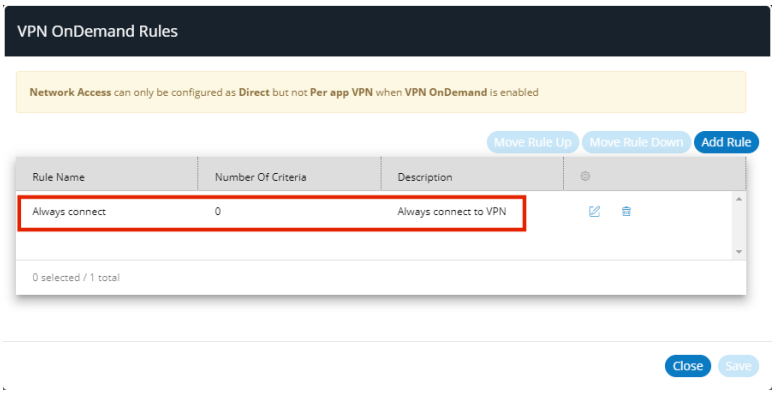
© 2019 Pulse Secure, LLC.

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 80 VPN on Demand: General Open Rule

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 68**.

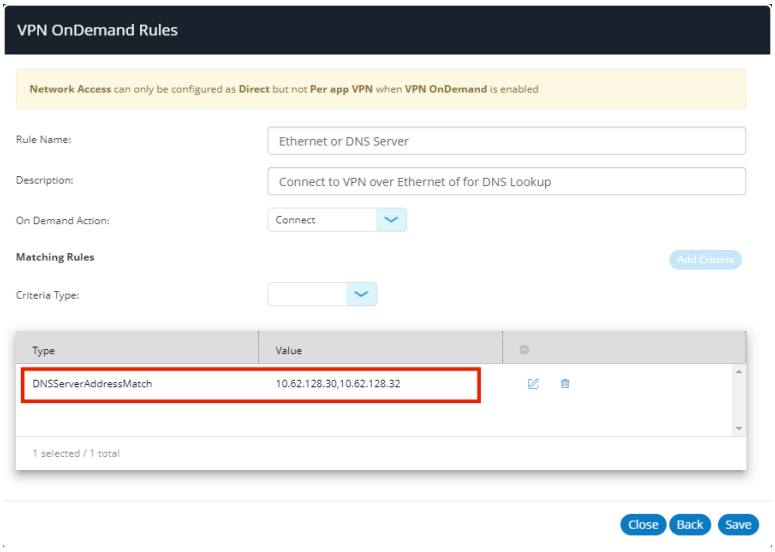
      Note: If you require an **On Demand Action** of *Evaluate Connection*, see the example later in this procedure.

    - Set the required **Criteria Type**, see **"Understanding VPN on Demand Rules Criteria" on page 69**.
    - Click **Add Criteria**.

© 2019 Pulse Secure, LLC.

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

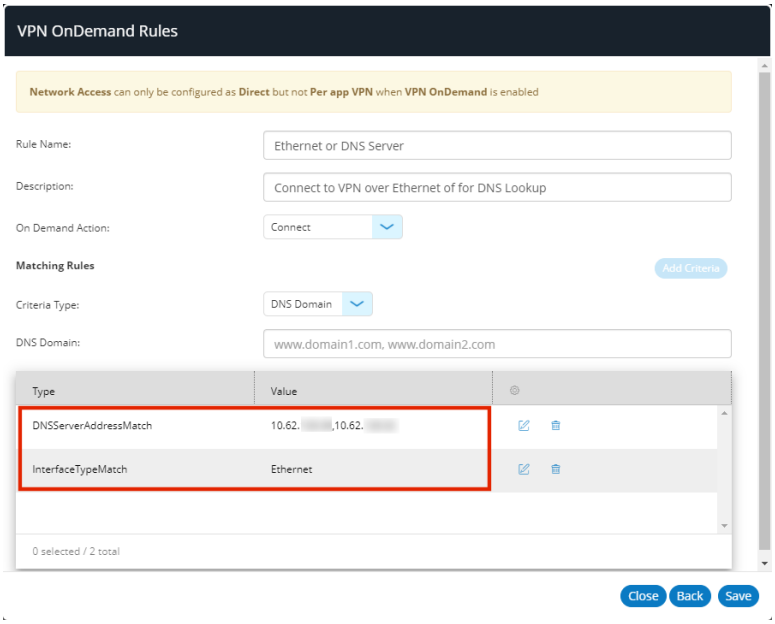
FIGURE 81 VPN on Demand: Rule with One Condition



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 82 VPN on Demand: Rule with Two Conditions



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

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

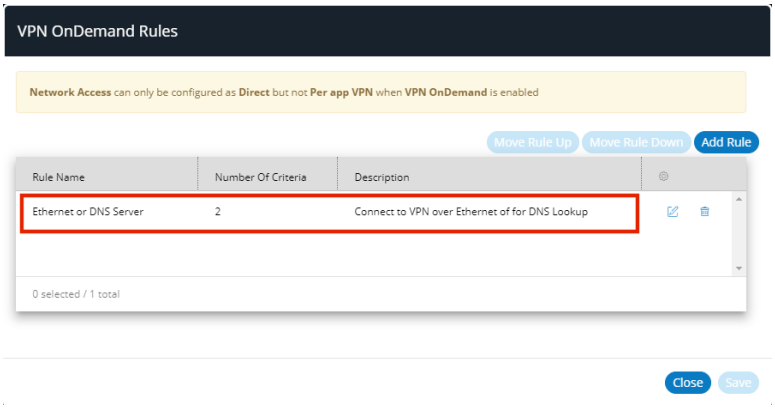
If at least one of the specified criteria matches, the rule is a match.

© 2019 Pulse Secure, LLC.

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

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

  FIGURE 83 VPN on Demand: Rule with Criteria



  In this example, there are two criteria.

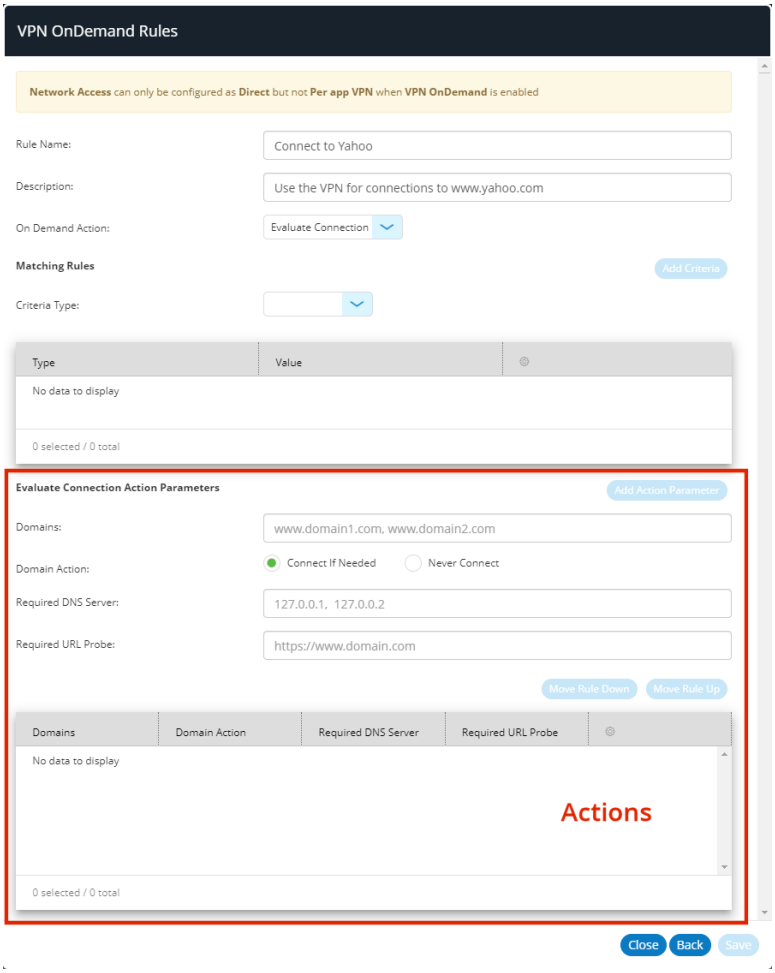
© 2019 Pulse Secure, LLC.

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 84 VPN on Demand: Rule with Action Parameters

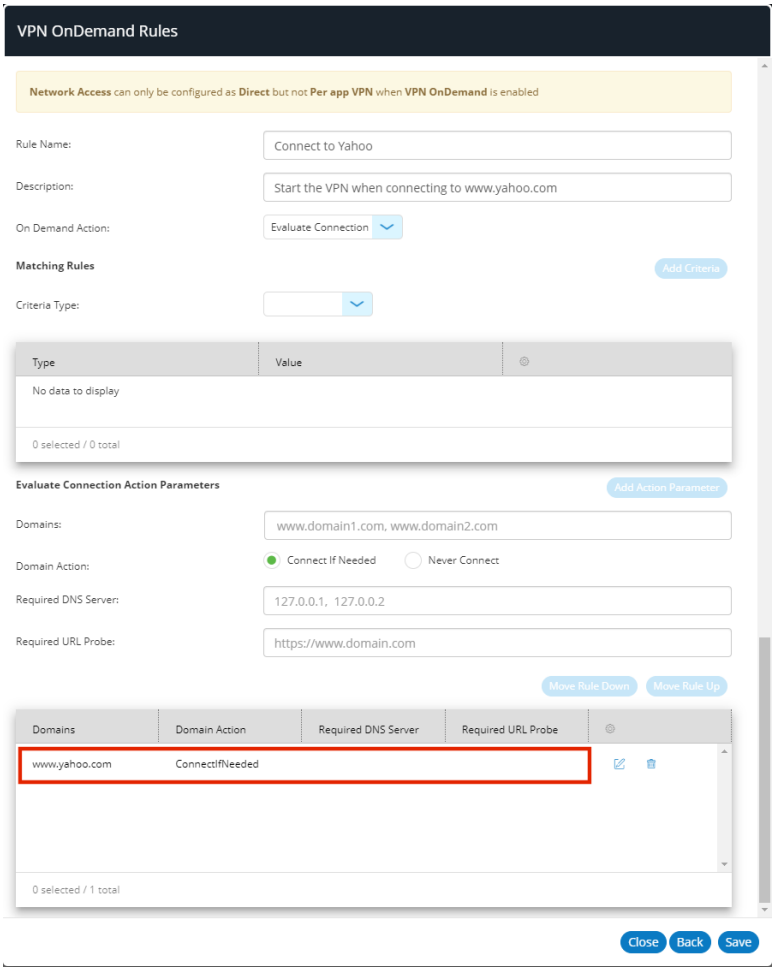


    - (Optional) Add one (or more) rules criteria, and add each to the list of criteria with **Add Criteria**. For details of criteria, see **"Understanding VPN on Demand Rules Criteria" on page 69**.

© 2019 Pulse Secure, LLC.

- 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 70**. For example:

FIGURE 85 VPN on Demand: Rule with Action Parameter



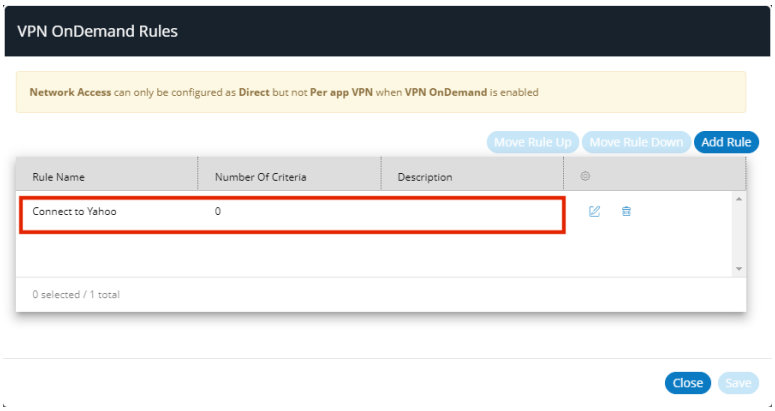
In this example, no rules criteria are specified, but a single action parameter activates the VPN when a connection to *www.yahoo.com* is requested.

© 2019 Pulse Secure, LLC.

- Click **Save**.

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

  FIGURE 86 VPN on Demand: Rule with Criteria



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 78**.

Enrolling Personal Devices as Managed Clients

After you have configured VPN on Demand (see **"Configuring VPN on Demand for Managed Clients" on page 67**) you can enroll devices using *managed client* mode.

- **"Adding a Personal Device to Pulse Workspace as a Managed Client" on page 78**.
- **"Enrolling a Personal Mobile Device as a Managed Client" on page 79**.

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 67**.
- Configure VPN on Demand, see **"Configuring VPN on Demand for Managed Clients" on page 67**.

© 2019 Pulse Secure, LLC.

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 79**.

Enrolling a Personal Mobile Device as a Managed Client

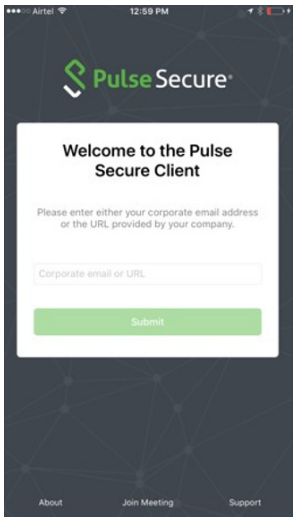
After a user's personal mobile device is added to Pulse Workspace with the intention of it being used as a managed client, the user receives a registration email at their declared personal email address.

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.

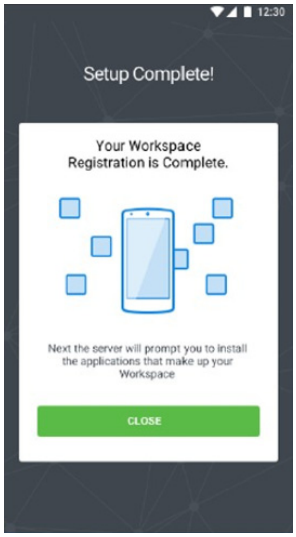
    FIGURE 87 Welcome



© 2019 Pulse Secure, LLC.

3. Perform the standard iOS BYOD enrollment procedure (see **"Registering an iOS BYOD Device" on page 44**) until the following screen appears:

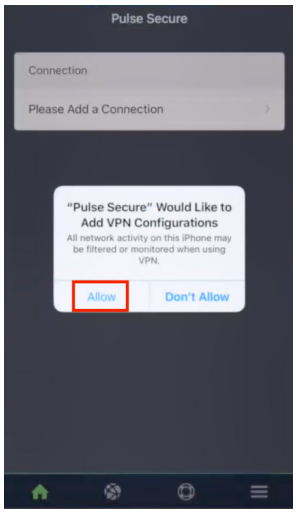
FIGURE 88 Setup Complete



4. Click **Close**.

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

FIGURE 89 Confirm VPN Config Policy



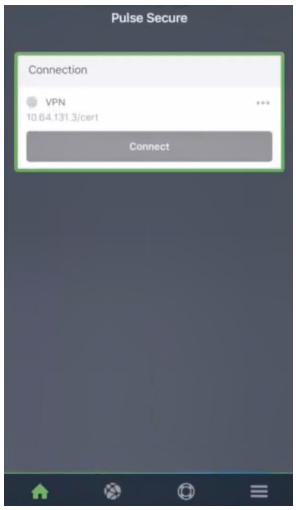
© 2019 Pulse Secure, LLC.

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.

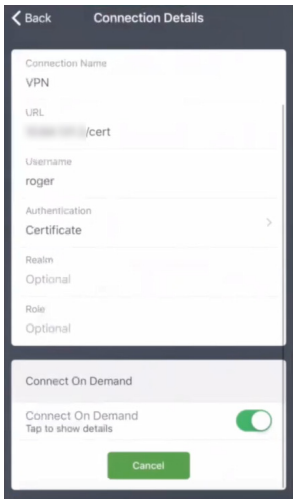
   FIGURE 90 VPN Connection



6. Press the VPN to view its details.

   Note: This configuration cannot be updated on your device.

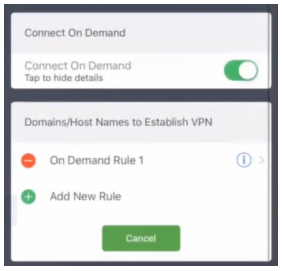
   FIGURE 91 VPN Configuration



© 2019 Pulse Secure, LLC.

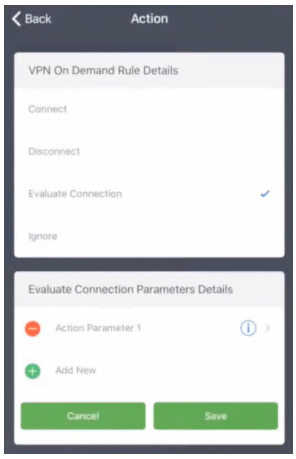
7. Press **Connect on Demand** to view configured VPN rules.

FIGURE 92 VPN Rules



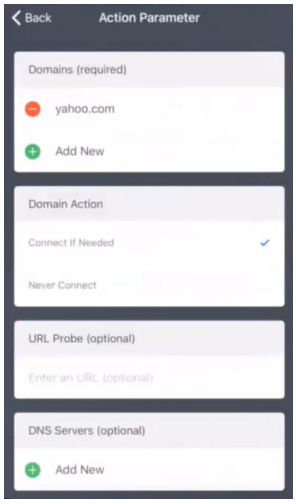
8. Press the configured rule (in this example, *On Demand Rule 1*) to view its details and actions.

FIGURE 93 VPN On Demand Rule Details



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

FIGURE 94 VPN On Demand Action Details

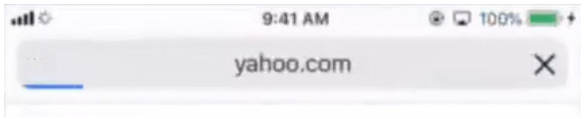


In this example, the *yahoo.com* domain will connect to the VPN when it is started.

© 2019 Pulse Secure, LLC.

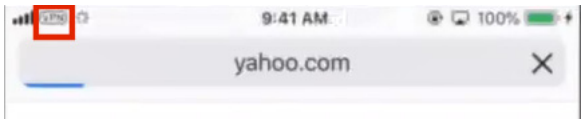
10. To test the VPN, start a browser and access the listed domain. (In this example, *yahoo.com*).

FIGURE 95 Browser Accessing Domain



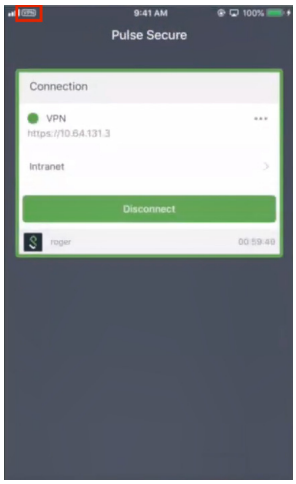
The VPN will active and display the VPN icon at the top of the screen. For example:

FIGURE 96 Browser Uses VPN



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

FIGURE 97 VPN Connection in Use



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

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Configuring Android Enterprise

- Overview 85
- Adding an Android App to the App Catalog 85
- Uploading Your In-House or Enterprise Apps using Google Play Console. 98
- Configuring Policy Settings 102

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 86**.
- **"Adding an Android App to the App Catalog from Google Play" on page 87**.
- **"Adding an Android App to the App Catalog Manually" on page 92**.
- **"Uploading an Android App to the App Catalog from Pulse One" on page 94**.

© 2019 Pulse Secure, LLC.

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

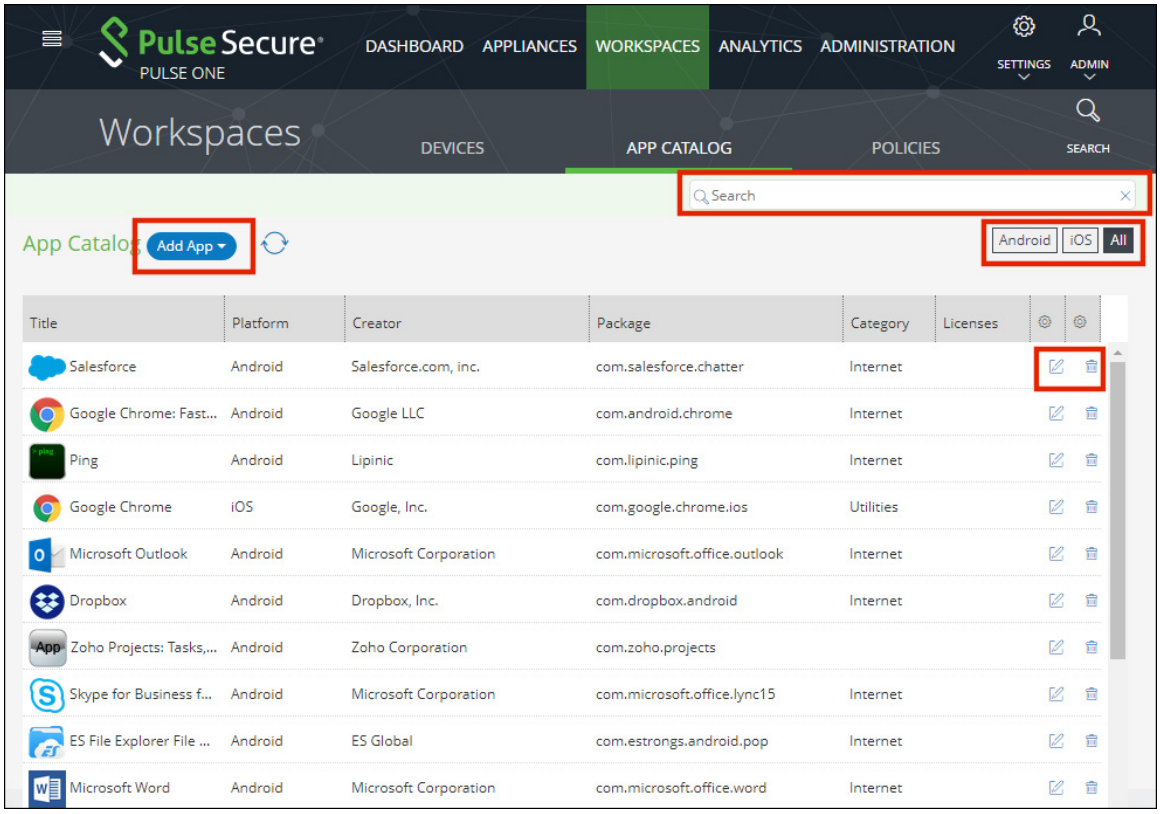
The **App Catalog** page lists the apps that have been added to the management console. On this page, you can see the app details or add a new app.

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 98 App Catalog



© 2019 Pulse Secure, LLC.

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.

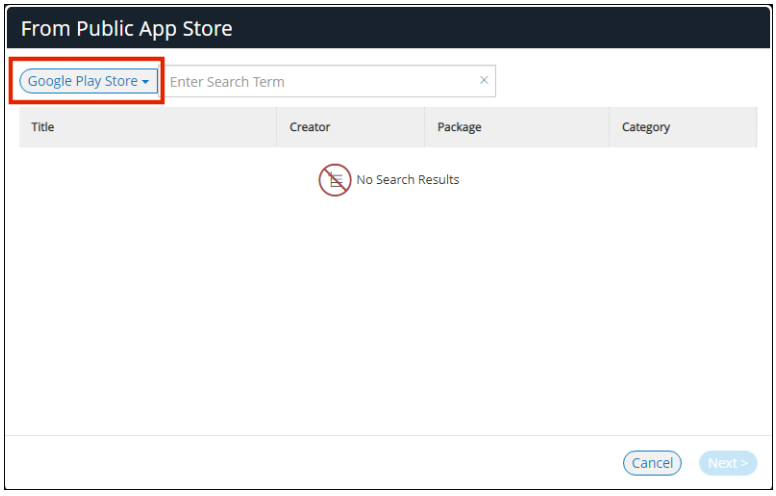
   The **App Catalog** page appears.

   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 149**.

FIGURE 99 Add App From Google Play Store



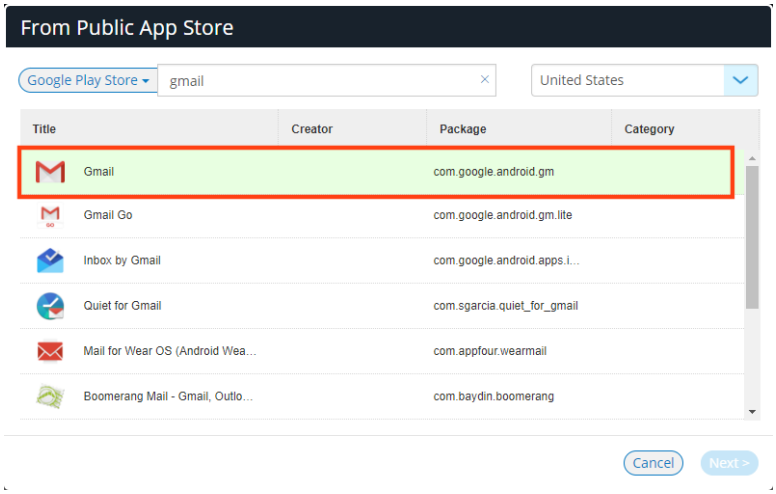
© 2019 Pulse Secure, LLC.

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 100 Select App from Search Result

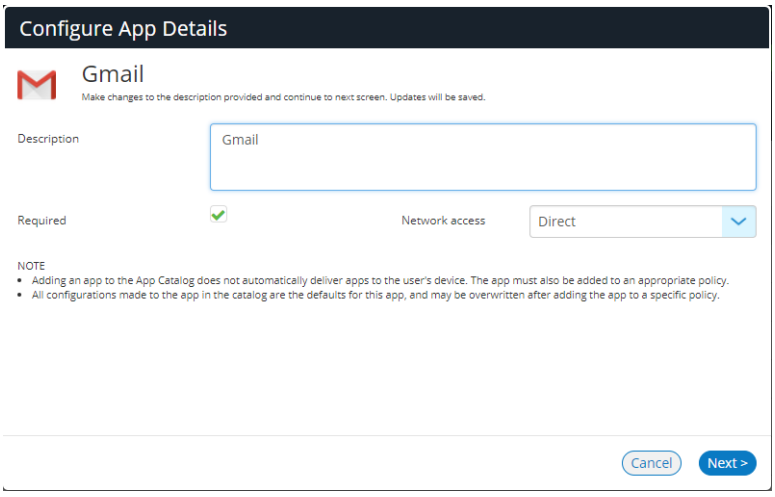


   The **Configure App Details** dialog appears.

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 101 Configure App Details

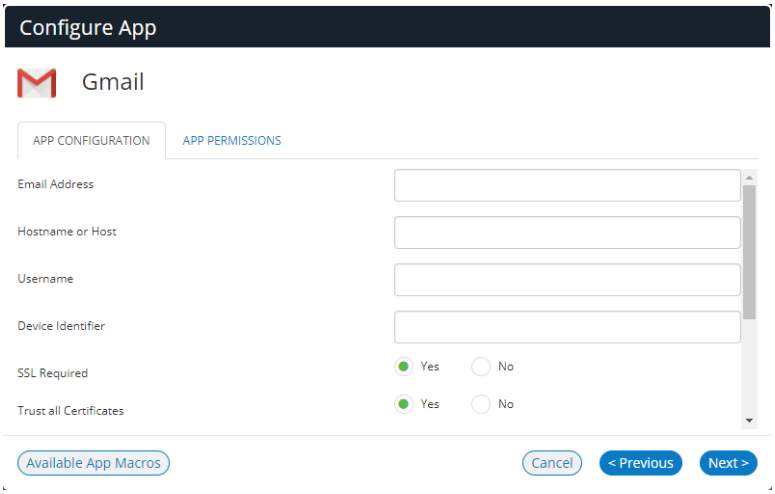


© 2019 Pulse Secure, LLC.

- Click **Next**.

  The **Configure App** dialog appears:

  FIGURE 102 Configure App



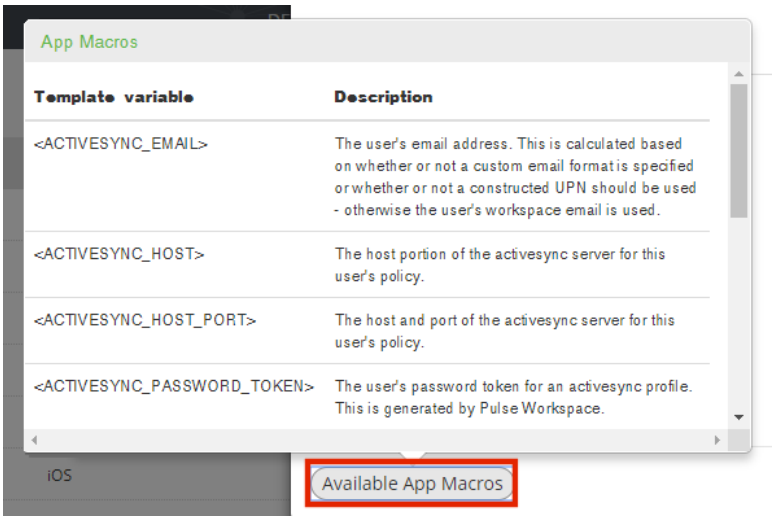
8. In the **Configure App** dialog:

   - 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 103 Available App Macros



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

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

© 2019 Pulse Secure, LLC.

- 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.

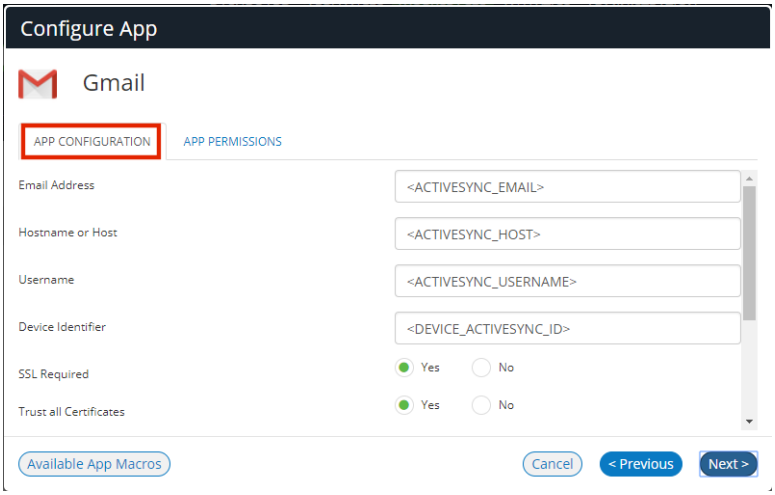
- Select whether to **Allow Unmanaged Accounts** to access the app.

- (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 104 App Configuration Complete

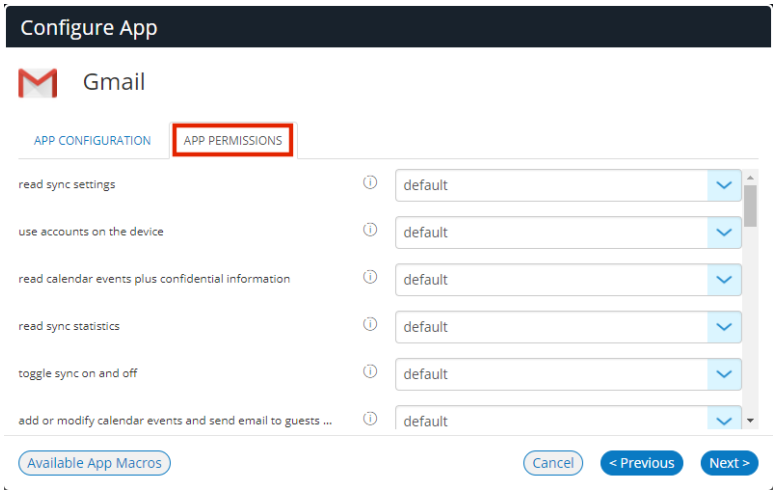


- Click **Next**.

© 2019 Pulse Secure, LLC.

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:

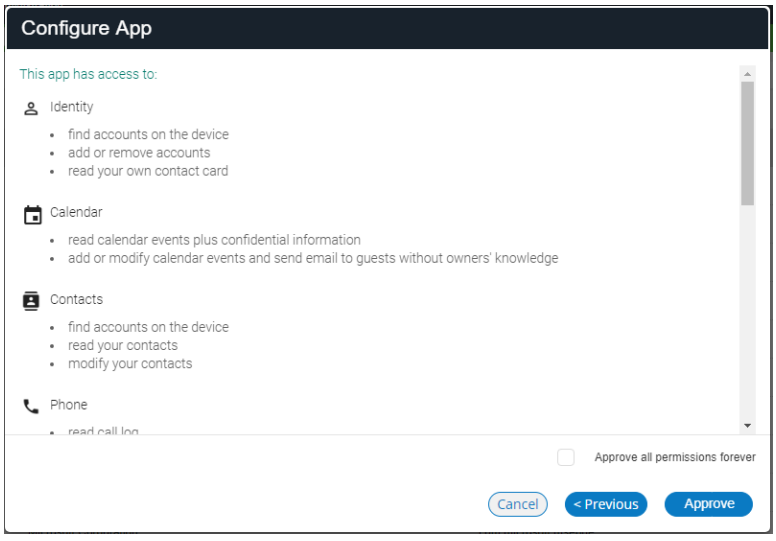
FIGURE 105 Configure App Permissions



Note: For information about app permission properties, see **"Workspaces" on page 149**.

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

FIGURE 106 Approve App Permissions



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

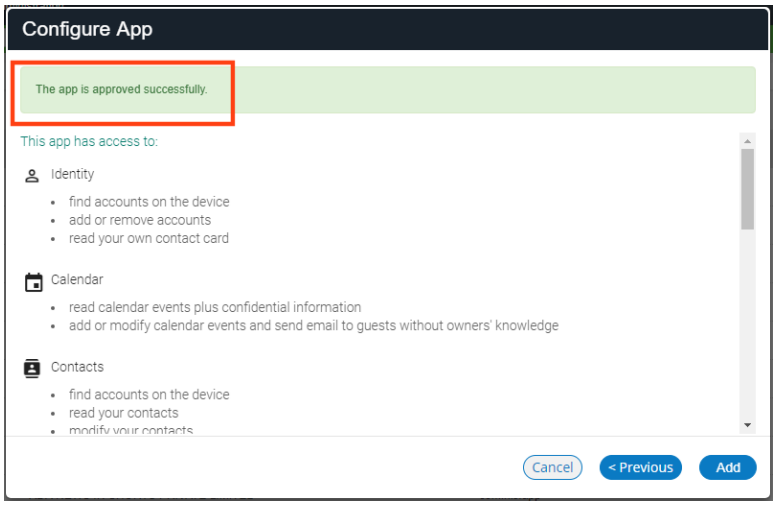
   Note: All revoked (or newly-added) permissions will be granted by default if this check box is selected.

© 2019 Pulse Secure, LLC.

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

    A confirmation message appears.

    FIGURE 107 App Added



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 102**.

Adding an Android App to the App Catalog Manually

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

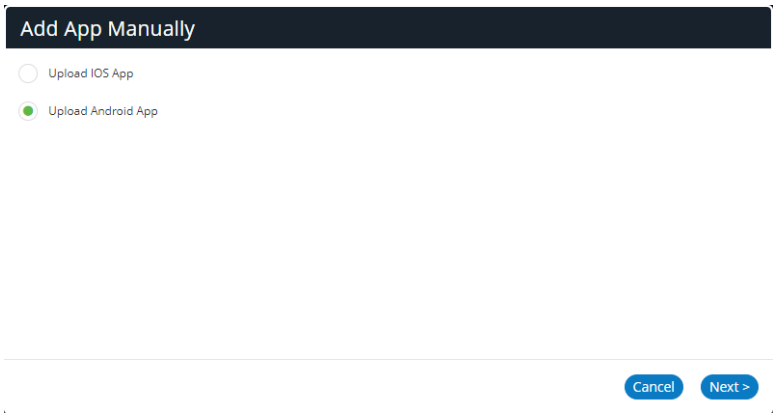
1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab. The **App Catalog** page appears.

© 2019 Pulse Secure, LLC.

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

   The **Add App Manually** dialog appears.

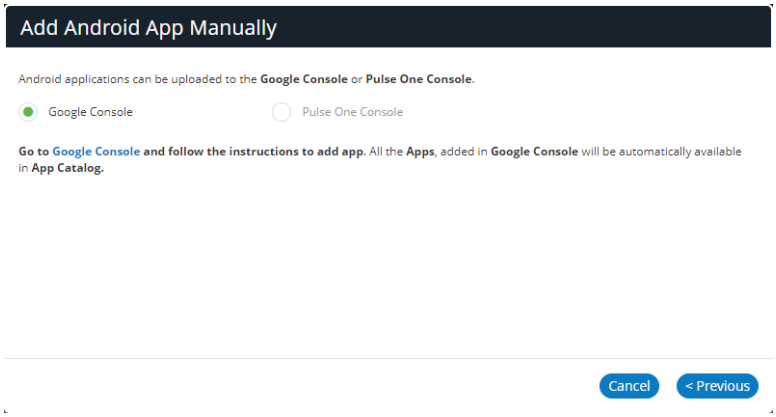
   FIGURE 108 Add Android App Manually



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

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

   FIGURE 109 Add Android App Manually

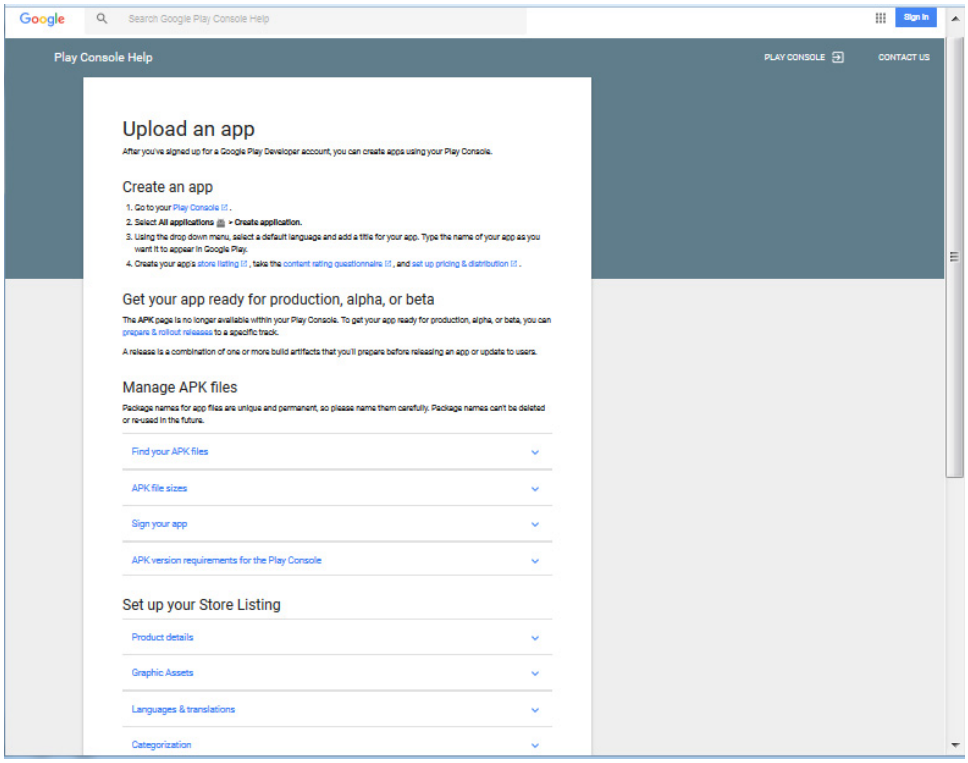


5. In the **Add Android App Manually** window, select **Google Console**.
6. Select the **Google Console** hyperlink.
7. Log in with Google enterprise credentials.

© 2019 Pulse Secure, LLC.

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

   FIGURE 110 Upload an Android App



   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 87**.

The next step is to add the app to a specific policy. For details, see **"Adding an Android App to a Policy" on page 102**.

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.

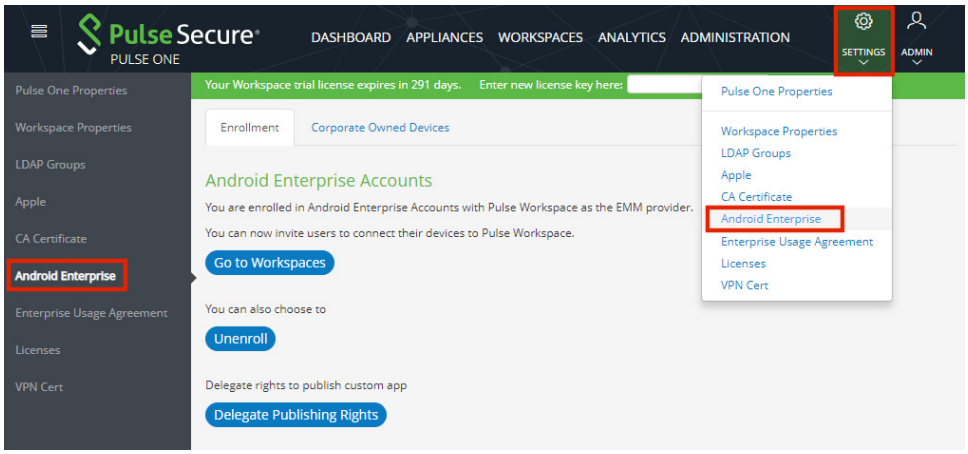
Note: You cannot delegate publishing rights for Android app upload when your Android Enterprise is enrolled using the Google Apps setup method.

© 2019 Pulse Secure, LLC.

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 111 Android Enterprise Properties



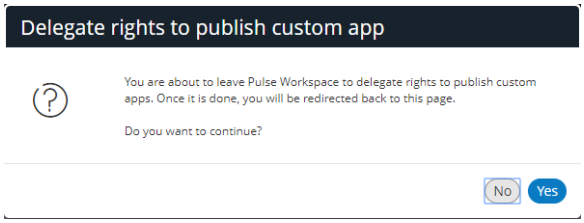
   The **Android Enterprise Accounts** page appears.

   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 112 Delegate Publishing Rights



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.

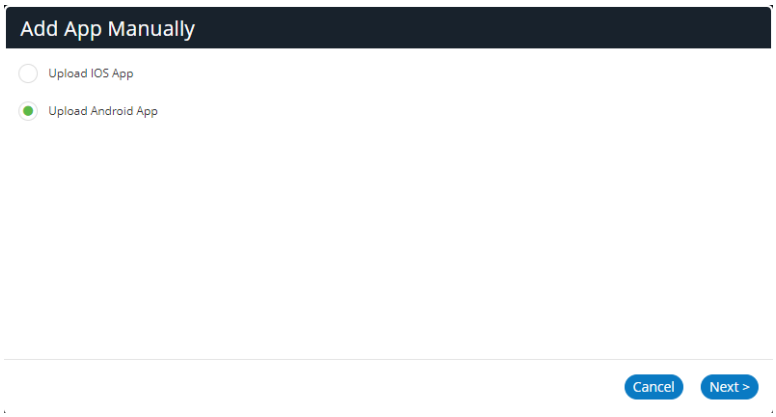
© 2019 Pulse Secure, LLC.

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.

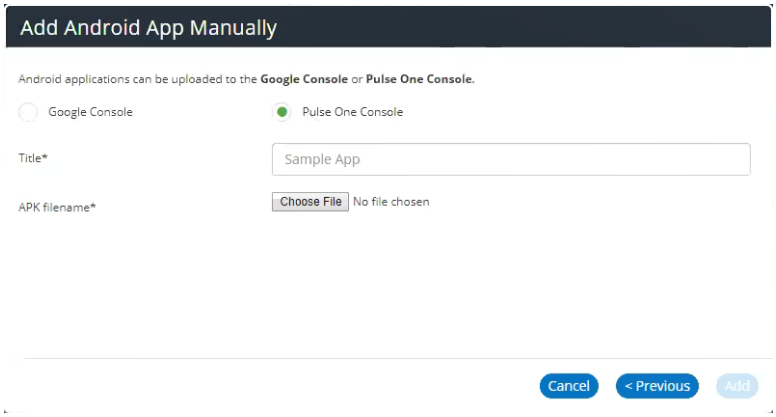
   FIGURE 113 Add Android App Manually



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

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

   FIGURE 114 Add Android App Manually



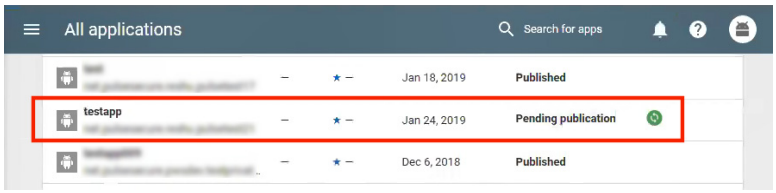
5. In the **Add Android App Manually** window, select **Pulse One Console**.
6. Enter a **Title** for the app.
7. Click **Choose File** and locate the required Android APK filename.

© 2019 Pulse Secure, LLC.

8. Click **Add**.

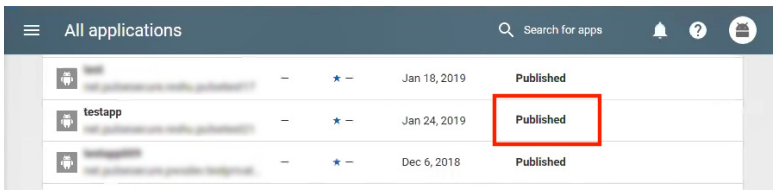
   The APK is uploaded automatically to the Google Play console in an Pending publication state. For example:

   FIGURE 115 Uploaded Android App Unpublished



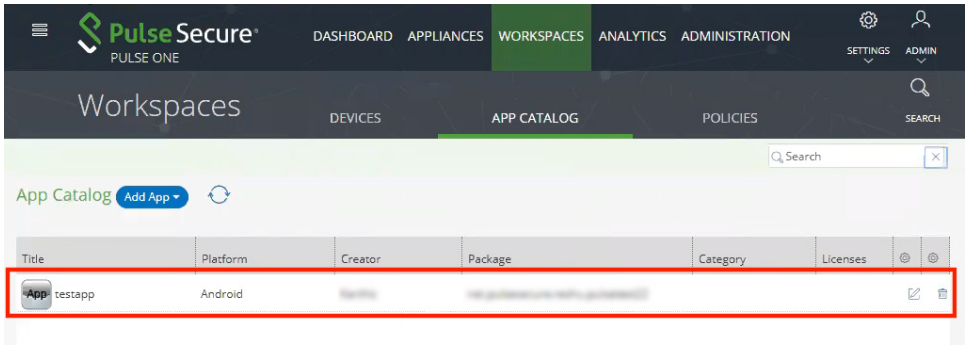
   The approval and publication can takes up to ten minutes. After publication, the state updates:

   FIGURE 116 Uploaded Android App 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 117 Uploaded Android App Added to App Catalog



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 102**.

© 2019 Pulse Secure, LLC.

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:

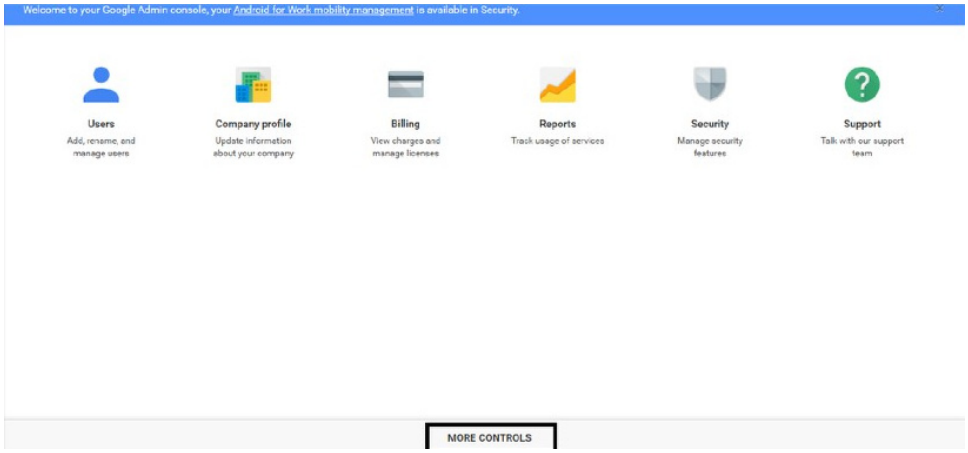
- "Logging into the Google Play Admin Console" on page 98.
- "Publishing a Private App on the Google Play Store" on page 99.
- "Approving a Private App for AFW Provisioning" on page 101.

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 118 Google Play Admin Console

3. Click the **Wifi** Icon to open the filter panel.

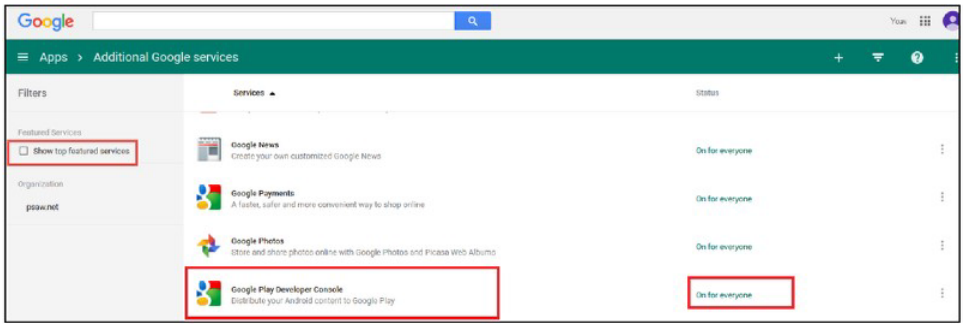
   FIGURE 119 Wifi Icon

4. Under **Featured Services** filter, clear the **Show top featured services** check box.

© 2019 Pulse Secure, LLC.

5. Enable the **Google Play Developer Console service** by clicking the **On for everyone** status.

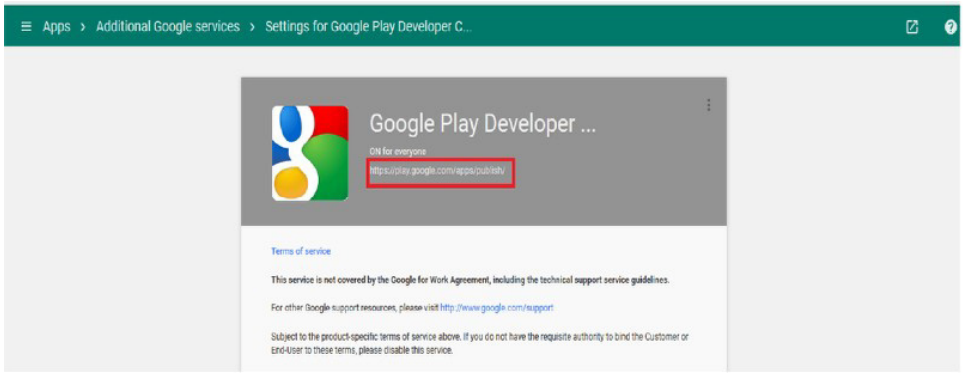
FIGURE 120 Additional Google Services



Publishing a Private App on the Google Play Store

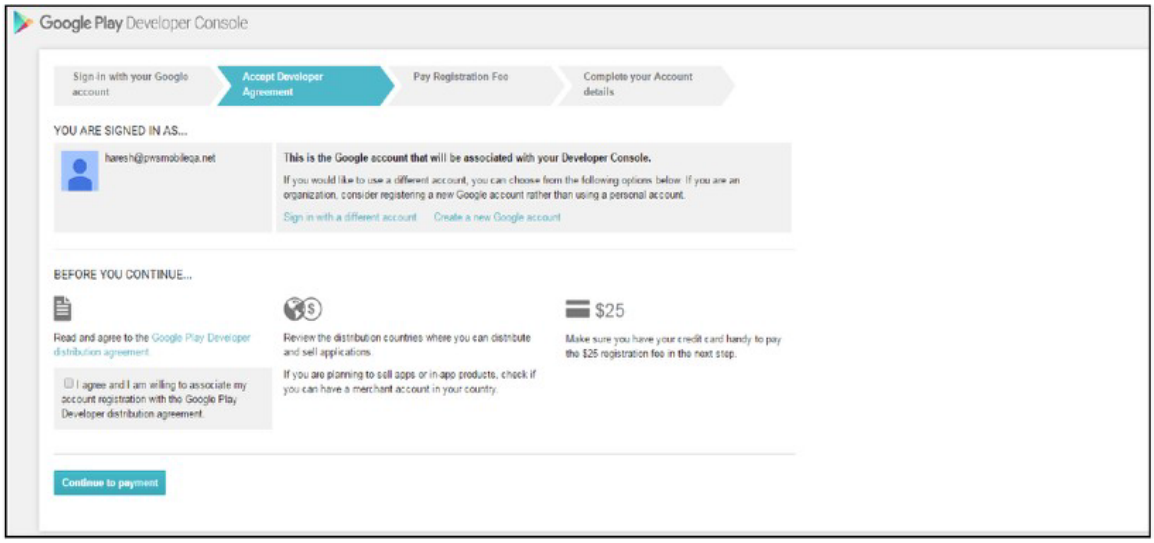
1. Launch the link **https://play.google.com/apps/publish/** to upload the private app.

FIGURE 121 Publish the Private App on Google Play Store



2. If required, pay the registration fee. The registration may take up to 48 hours to complete.

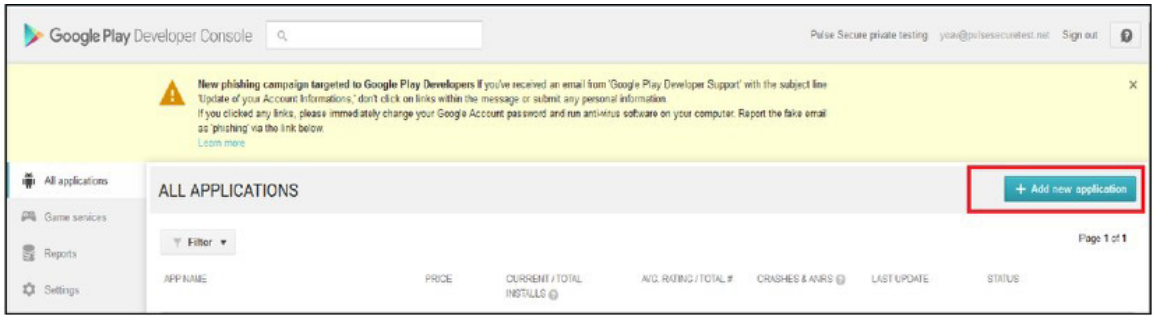
FIGURE 122 Accept Developer Agreement



© 2019 Pulse Secure, LLC.

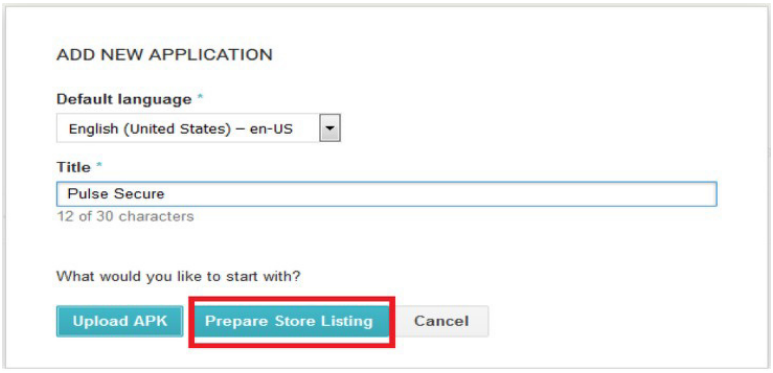
3. Click the **Add new application** button and upload the APK. Add the required graphics and other mandatory information.

FIGURE 123 Add New Application



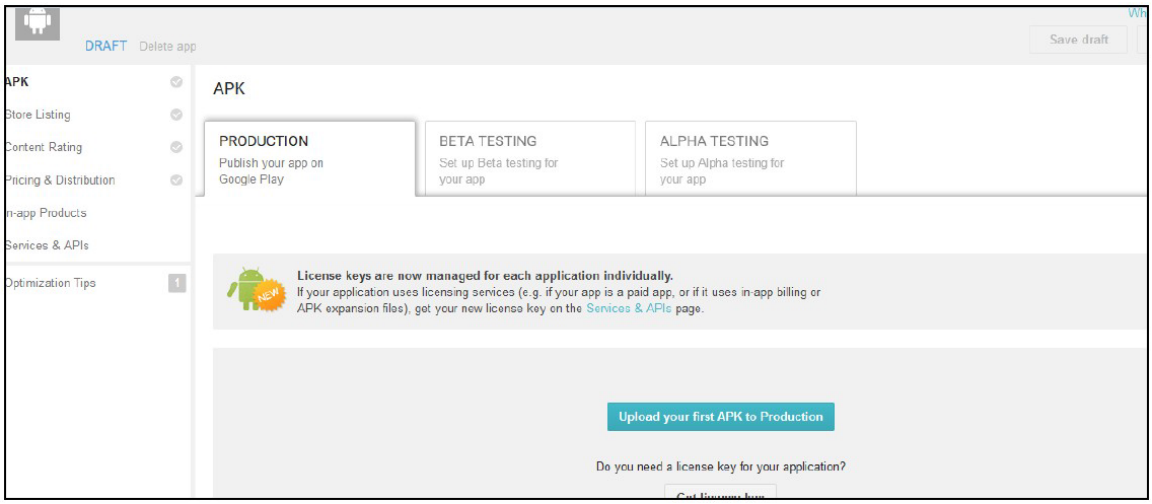
4. In the **Add New Application** page, select the language and enter a title for the application.
5. Click the **Prepare Store Listing** button.

FIGURE 124 Prepare Store Listing



6. Upload the new APK by clicking on the **Upload your first APK to Production** button.

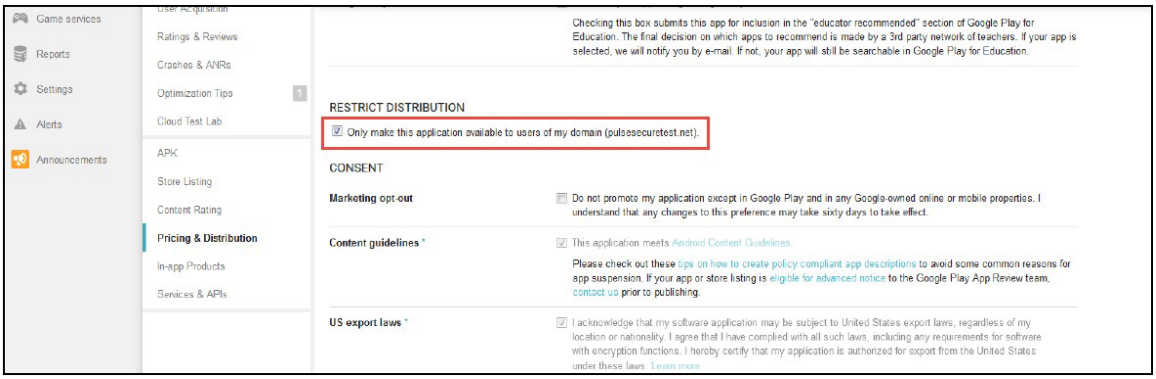
FIGURE 125 Upload APK to Production



© 2019 Pulse Secure, LLC.

7. Under **Pricing & Distribution**, select the **Only make this app available to users of my Google apps domain name** check box.

FIGURE 126 Restrict Distribution



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 pages for the procedure to distribute apps in your organization:

   - https://support.google.com/a/answer/2494992?hl=en
   - https://support.google.com/googleplay/work/answer/6145139?hl=en

© 2019 Pulse Secure, LLC.

Configuring Policy Settings

This section describes the following procedures:

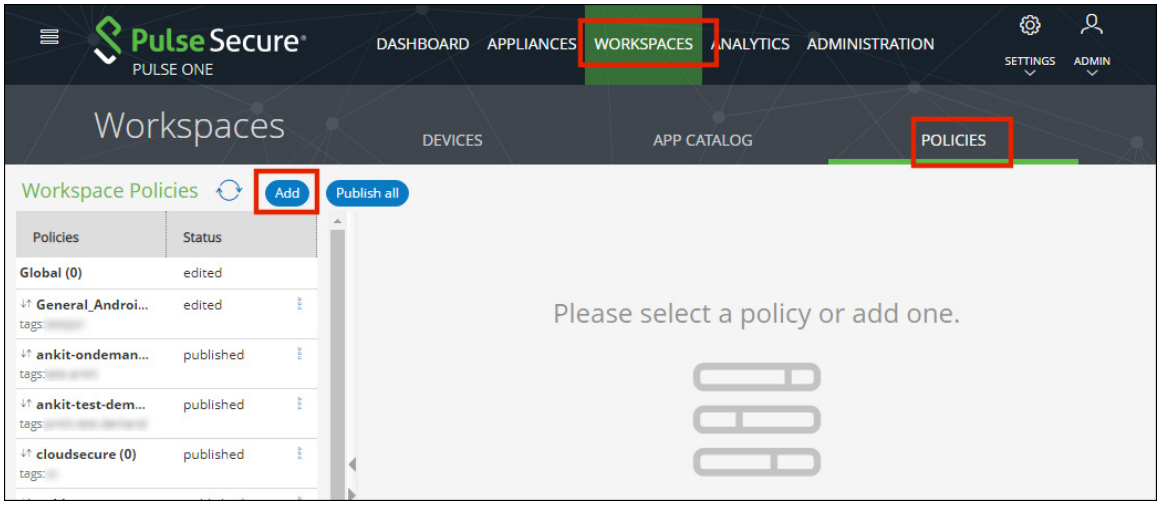
- "Adding an Android App to a Policy" on page 102.
- "Configuring Policy Properties" on page 106.
- "Setting a Password Policy" on page 108.
- "Locking a Work Profile" on page 109.

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.

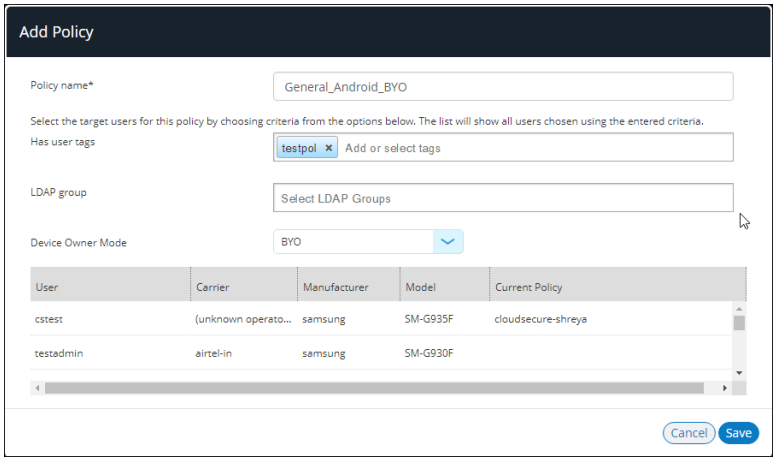
FIGURE 127 Add Policy



© 2019 Pulse Secure, LLC.

5. Enter a **Policy Name**, complete the **Has user tags** property, and click **Save**. For example:

FIGURE 128 Add Policy Details



The policy is added to the **Policies** list in the **Workspace Properties** page.

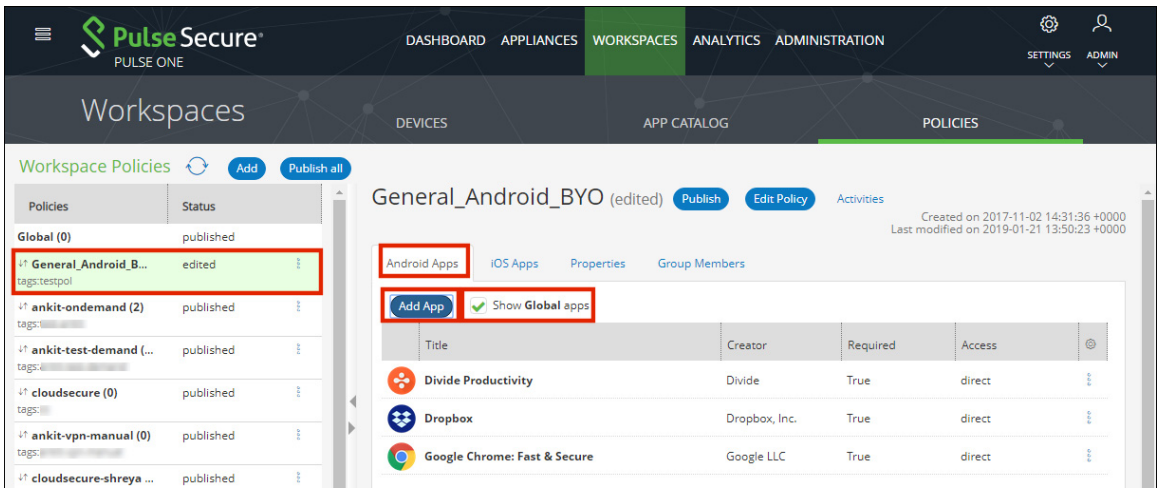
You must now add apps from the Google Play Store to this policy.

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 129 Add App to Policy

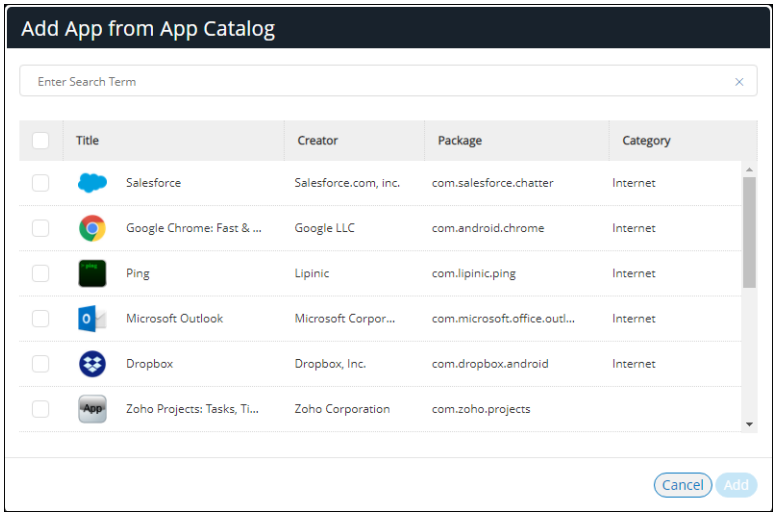


9. In the **Add App from App Catalog** dialog, enter the app name in the **Search** box and press **Enter**.

© 2019 Pulse Secure, LLC.

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

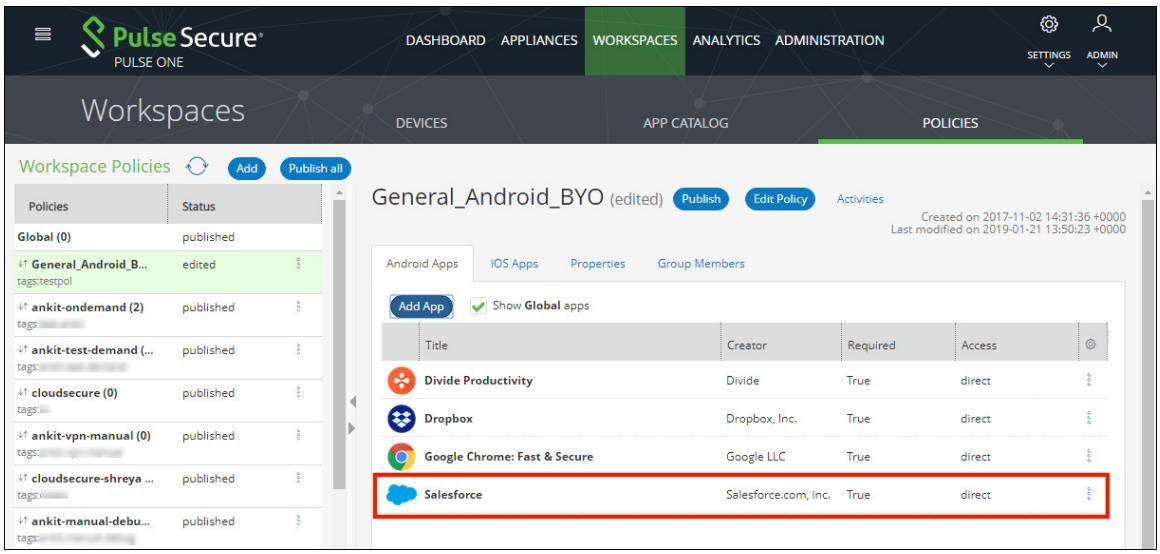
FIGURE 130 Add App from App Catalog



10. From the apps list, select the required app and click **Add**.

    The app is added to the policy. For example:

FIGURE 131 Updated App List for Policy



11. In the **Android Apps** list, select the **Actions** icon (⋮) for the app and click **Edit app rule**.

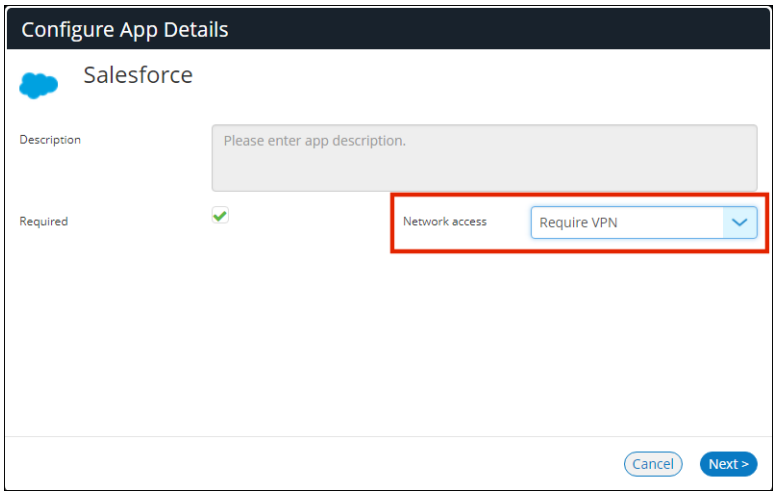
    The **Configure App Details** dialog appears.

© 2019 Pulse Secure, LLC.

12. Make the required configuration changes.

    For example, if you access the app through VPN only, then set **Network access** to *Require VPN*.

    FIGURE 132 Configure App Details



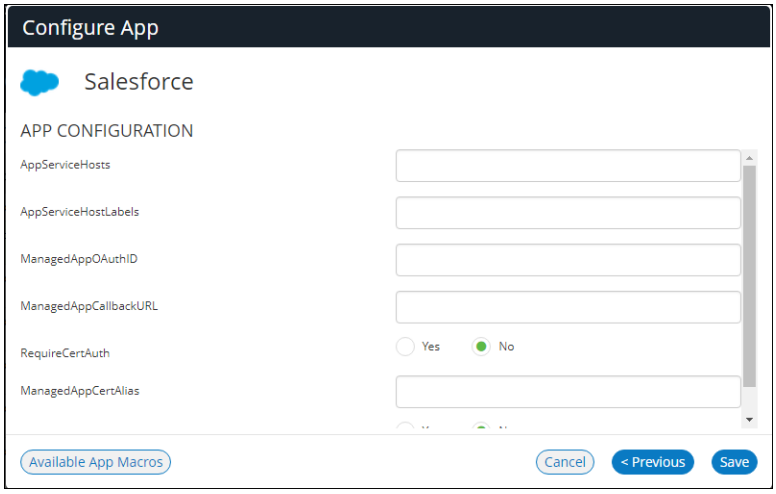
    Note: You cannot change the **Description**.

13. Click **Next**.

    The **Configure App** dialog appears.

14. Supply the required configuration and click **Save**. For example:

    FIGURE 133 Configure App



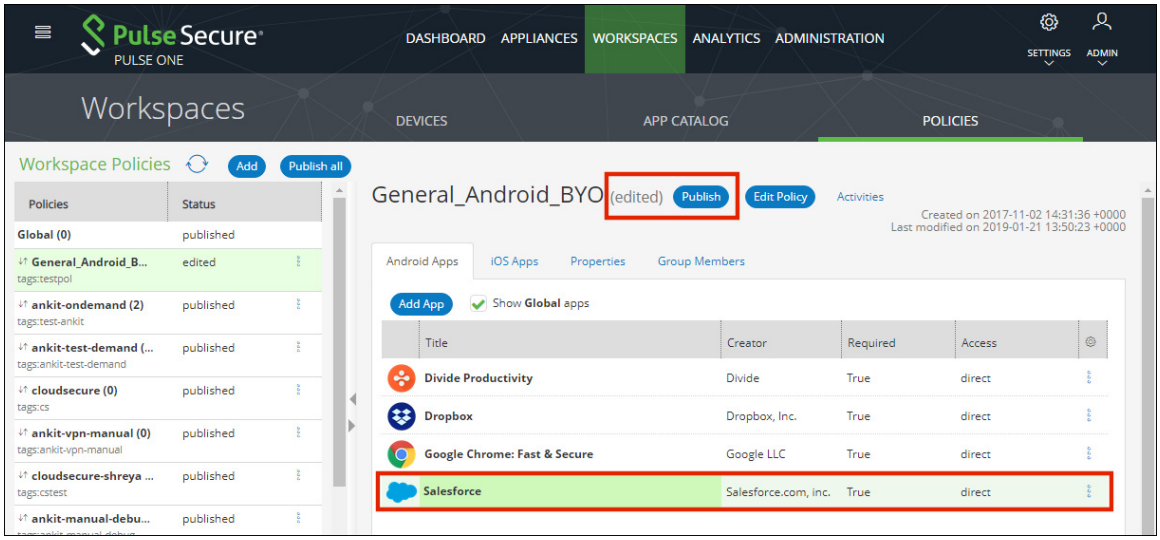
15. Some apps need permissions to access. For these apps, the **App Permissions** dialog appears. Select the required permissions for the app and click **Save**.

    For information about enabling app permission property and configuring default runtime permission, see **"Managing Pulse One Properties" on page 197**.

© 2019 Pulse Secure, LLC.

16. Select the app from the app list and click **Publish**.

    FIGURE 134 Publish App



    The **Publish** confirmation dialog appears.

17. Click **Yes**. The app is published.

This completes adding an Android app to a policy.

Configuring Policy Properties

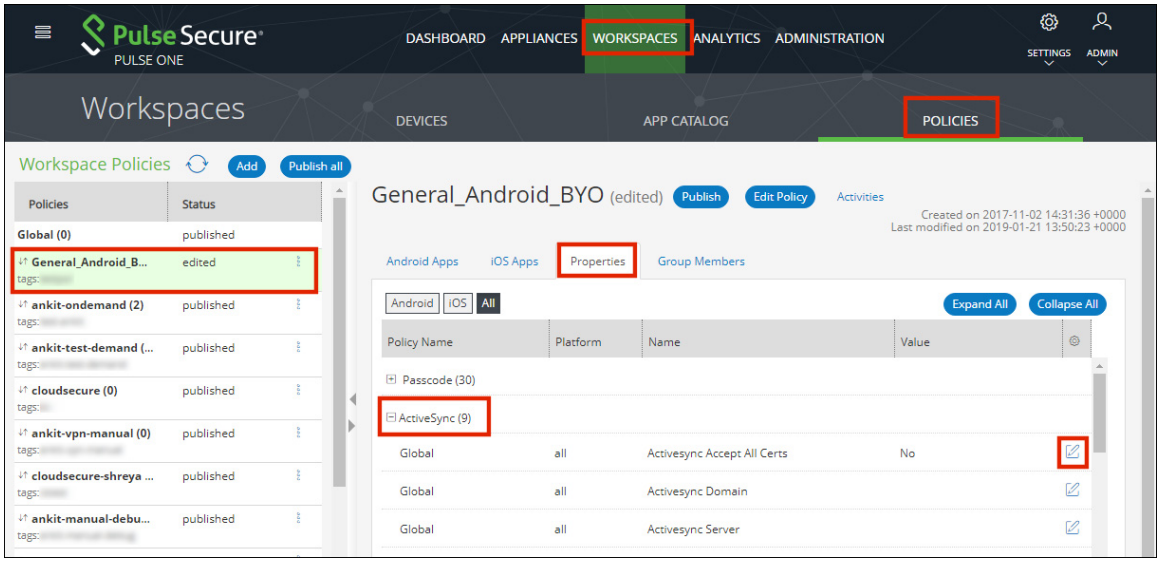
To set the properties for a policy:

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*.

© 2019 Pulse Secure, LLC.

6. Locate the required policy in the expanded list and click its **Edit** icon.

FIGURE 135 Edit Policy



7. Make the required changes and **Save** each. For example:

FIGURE 136 Edit Property

© 2019 Pulse Secure, LLC.

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 135**.

Password policies are configured in the admin console and deployed on Android devices.

To set a password:

1. Select the **Workspace** tab.
2. Select the **Properties** tab.
3. Select the required policy.
4. Click the **Properties** tab.
5. Click the **Edit** icon corresponding to *Screenlock Password Quality*.
6. In the **Edit Property** window, select one of the following screen unlocking mechanisms and click **Save**.
    - *none*
    - *biometric*
    - *password*
    - *pattern*
    - *pin*
    - *pin_complex*
    - *alpha*
    - *alphanumeric*
    - *complex*

If a user has not defined screen lock in his device, then the password policy defined by the admin will be forced to the user's device.

© 2019 Pulse Secure, LLC.

Locking a Work Profile

Android 7.0 (Nougat) or later supports lock work profile on devices. To open a work app, device prompts for the passcode. Administrator can define the length of the passcode, number of invalid passcode attempts.

To set up or change the work profile lock:

1. On your device, go to **Settings > Security > Work profile security**.
2. Tap the lock type you'd like to use and follow the instructions.
3. (Optional) If you're changing your work profile lock, enter the pattern, PIN, or password when prompted.
4. If necessary, choose how you want your work notifications to show on your device when it's locked.

   Note: You can change your work notification settings at any time.
5. Tap **Done**.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Workspace Management

- Managing Users 111
- Working with the App Catalog 122
- Managing Policies 132
- Configuring Workspace Properties 148
- Configuring Auto-Config of a VPN Provider on Mobile Devices. 153
- Configuring Appliance ActiveSync 160
- Configuring Certificate-Based ActiveSync 161
- Working with Device Location. 165

Managing Users

Pulse One users with a Workspace license entitlement can manage Workspaces from the **Workspaces** menu.

- "Adding a User" on page 111.
- "Deleting a User" on page 114.
- "Verifying an LDAP Group" on page 115.
- "Adding a Policy Tag to a Workspace User Account" on page 116.
- "Performing Workspace Actions" on page 116.
- "Understanding the Workspace Details Window" on page 119.

Adding a User

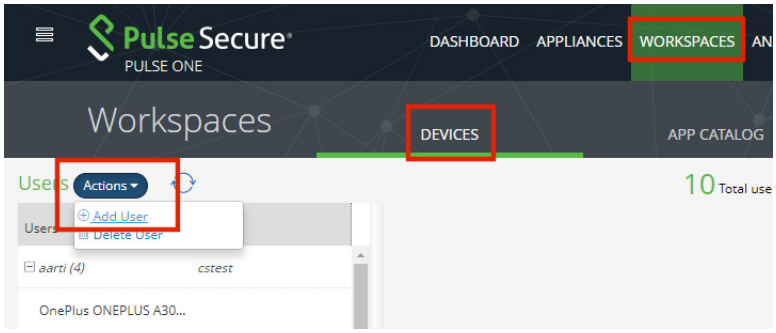
This section details the steps to add a new user to your domain.

1. Select the **Workspaces** menu.
2. Select the **Devices** tab. A list of **Users** appears.

© 2019 Pulse Secure, LLC.

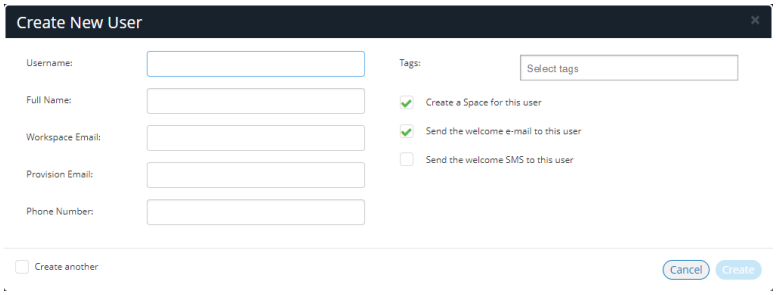
3. Click the **Actions** drop-down menu, and click **Add User**.

FIGURE 137 Add User



The **Create New User** dialog appears.

FIGURE 138 Create New User



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**

© 2019 Pulse Secure, LLC.

7. Click **Create** to complete the process.

   The new user is added to the **Users** list.

© 2019 Pulse Secure, LLC.

Deleting a User

This section details the steps to delete a user from your domain.

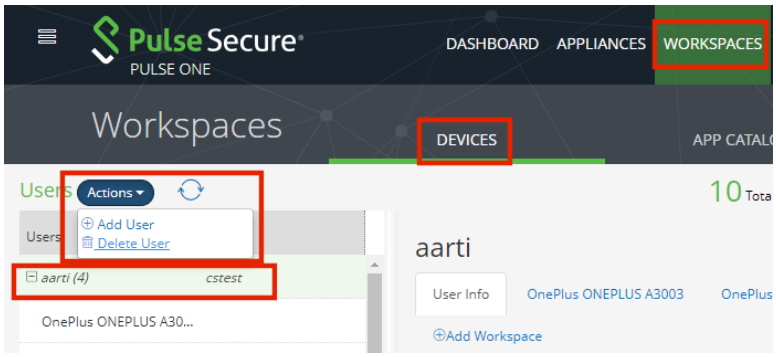
Note: You must delete all workspaces/devices from a user before you can delete the user.

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 139 Delete User

   A confirmation dialog appears.
8. Click **Yes** to confirm the user deletion.

   The selected user is removed from the **Users** list.

© 2019 Pulse Secure, LLC.

Verifying an LDAP Group

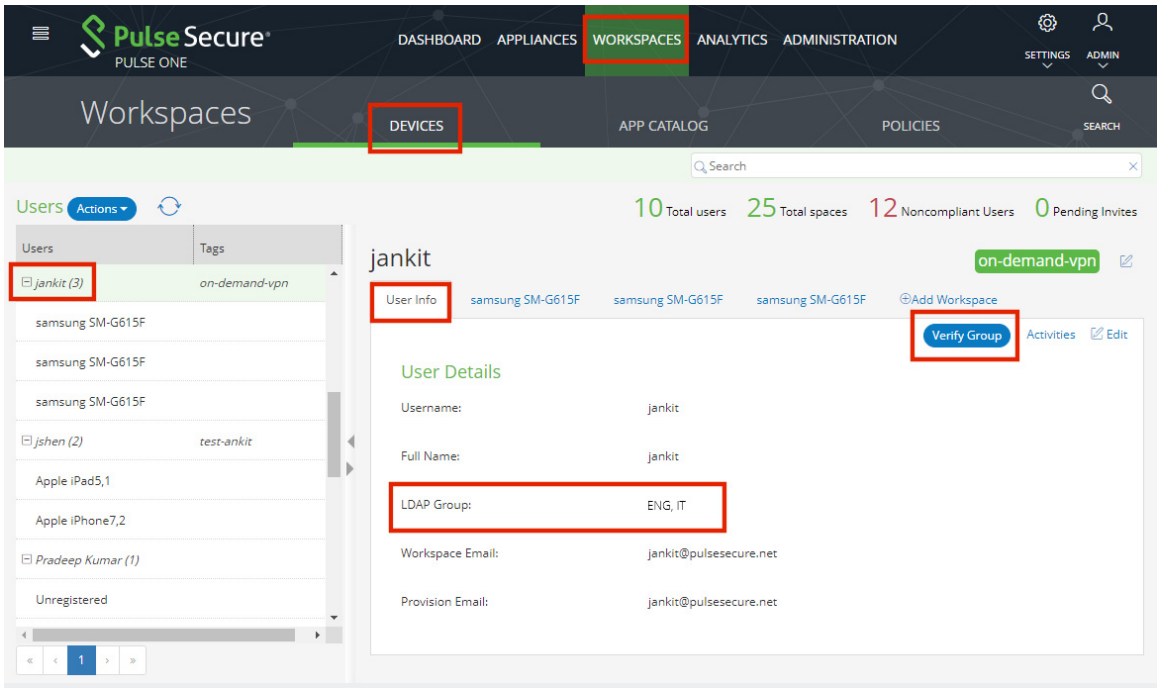
When a user group is changed in the back-end Active Directory server, the change is not immediately reflected in the User Info page. The **Verify Group** button is provided to re-verify the user's LDAP group and recalculate the policy for the user.

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 140 Verify Group



© 2019 Pulse Secure, LLC.

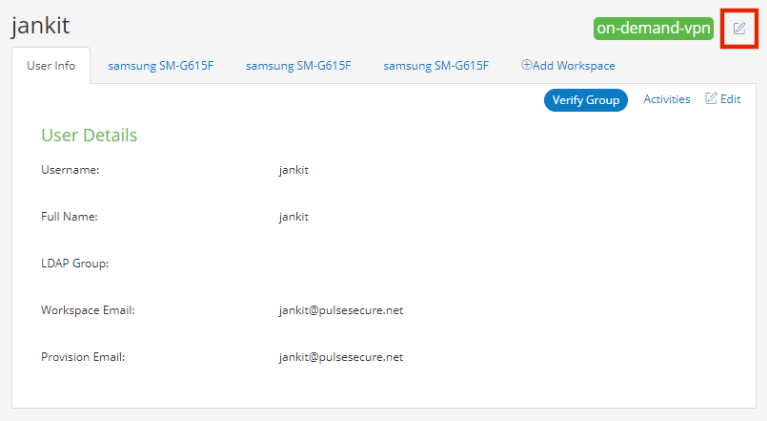
Adding a Policy Tag to a Workspace User Account

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.

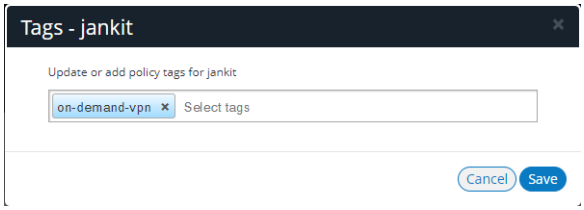
1. Select the **Workspaces** menu.
2. Select the **Devices** tab. A list of **Users** appears.
3. Locate the required user in the list, or (optionally) click the **Search** button and use the search box.
4. Click the **Tags** icon located at the corner of the user details panel. For example:

   FIGURE 141 Tags Icon

   The **Tags** dialog appears. For example:

   FIGURE 142 Add 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.

© 2019 Pulse Secure, LLC.

4. Expand the required user, and select the required workspace.
5. Select **Actions** from the Workspace panel. For example:

FIGURE 143 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 150**.
- **Show Wifi Certificate Info** – shows if the WiFi certificate is valid. This action is not active when **Force Update Wifi Cert** is present.

© 2019 Pulse Secure, LLC.

- **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 150**.
- **Update Location** – updates the location of the device (iOS only), see **"Locating a Device" on page 179**.
- **Lost Mode** – indicates that the device is lost, see **"Working with Lost Mode for a Device" on page 180**.
- **Request Lost Mode Location** – requests a location update for a lost device (iOS only), see **"Working with Lost Mode for a Device" on page 180**. 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 180**. 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 180**. 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 149**

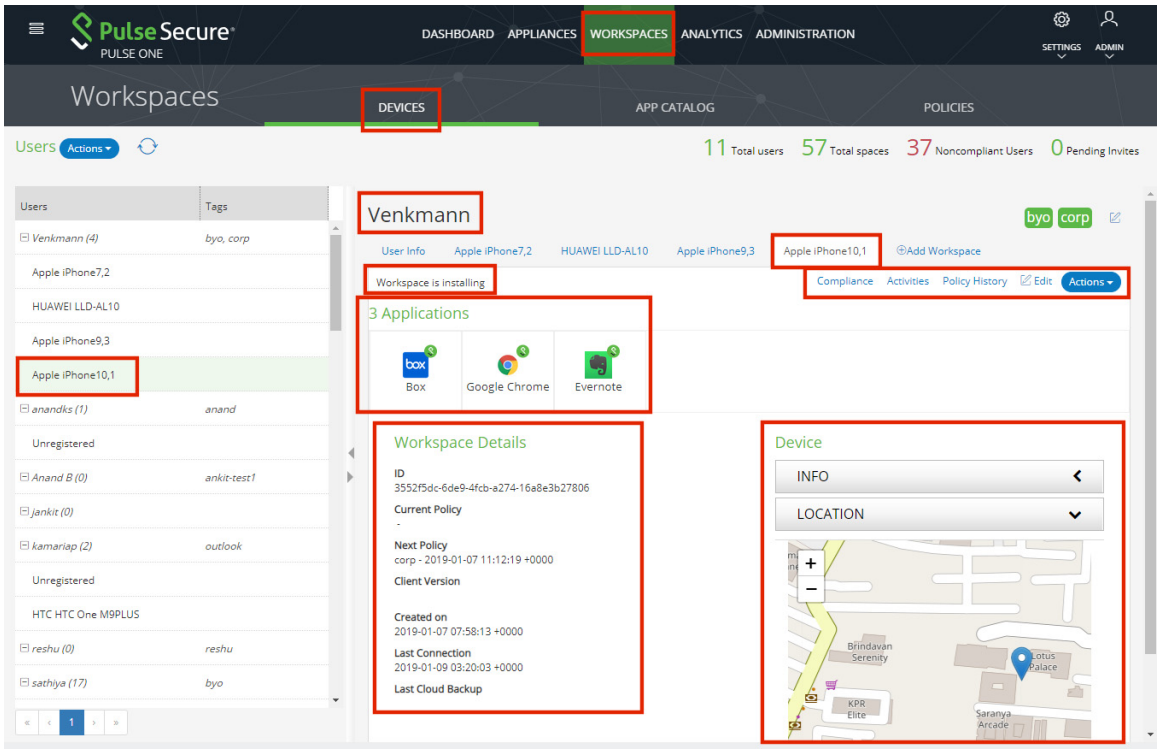
© 2019 Pulse Secure, LLC.

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.
- **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 165**.

FIGURE 144 Workspace panel



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.

© 2019 Pulse Secure, LLC.

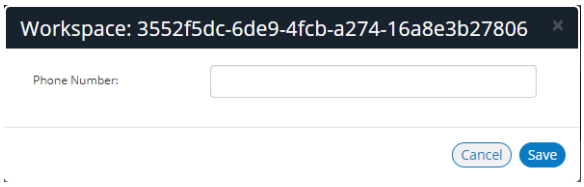
- **Profile password complexity** – Indicates the profile password type. That is: none, biometric, password, pattern, pin, pin_complex, alpha, alphanumeric or complex.
- **Device password complexity** – Indicates the device password type. That is: none, biometric, password, pattern, pin, pin_complex, 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 165**.
- **iOS Minimum Pulse Client version** – Indicates the policy's minimum Pulse Client version.

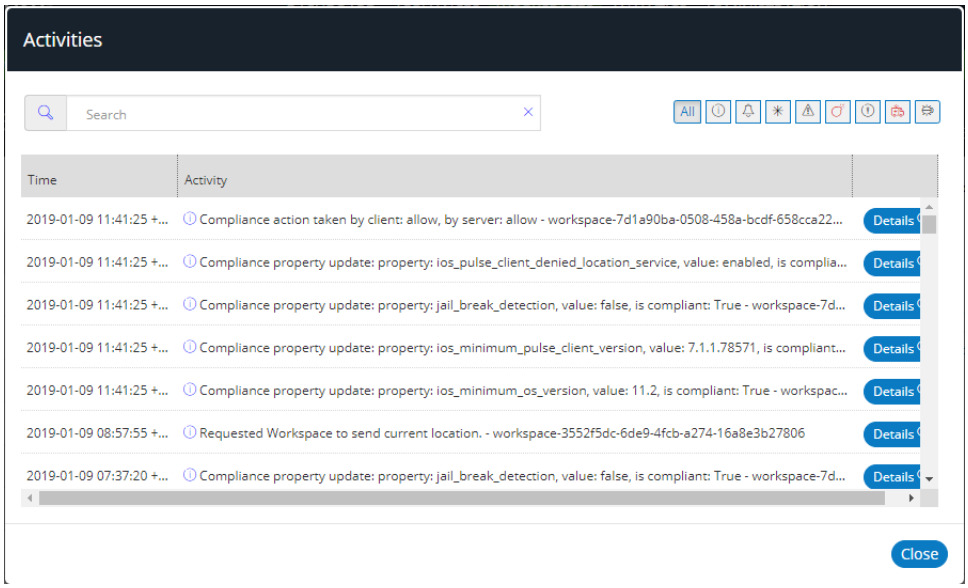
The **Edit** window allows you to view and edit the phone number to which the welcome SMS is sent. For example:

FIGURE 145 Workspace Details



The **Activities** window displays the log of Workspace activity. Double click an activity to see the detailed view.

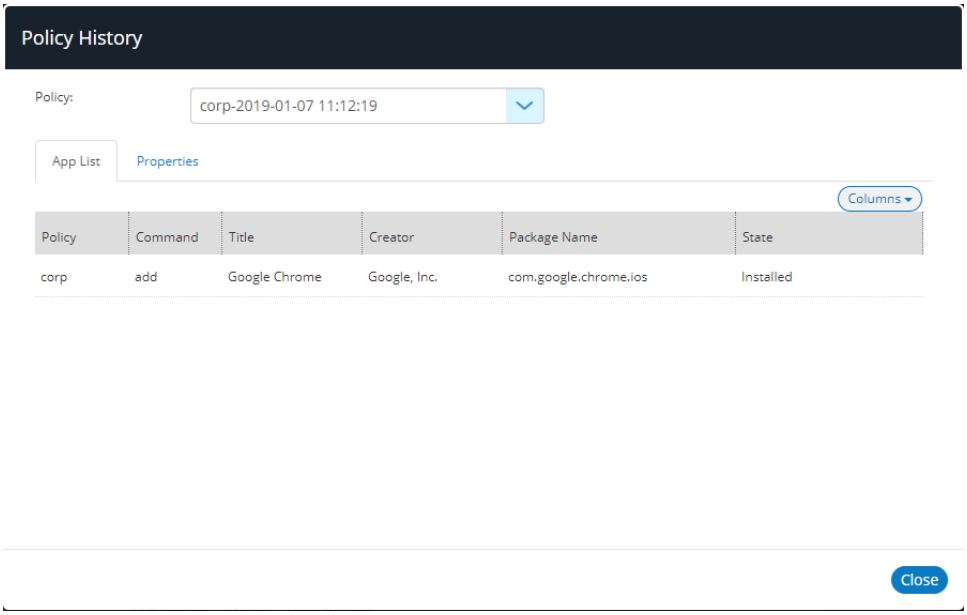
FIGURE 146 Activities



© 2019 Pulse Secure, LLC.

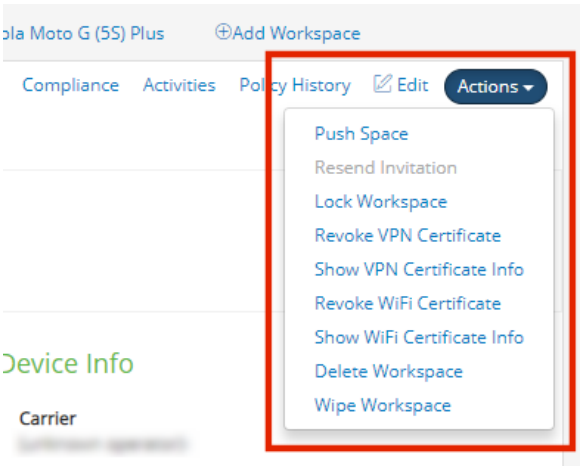
The **Policy History** window displays the current and previous policies applied to a Workspace.

FIGURE 147 Policy History



The **Actions** menu displays the list of actions available for the Workspace.

FIGURE 148 Workspace Actions



© 2019 Pulse Secure, LLC.

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 122.
- "Adding iOS Apps to the App Catalog" on page 125.

  Note: The addition of Android apps to the App Catalog is described in "Adding an Android App to the App Catalog" on page 85.

- "Adding iOS Apps to a Policy from the App Catalog" on page 130.

  Note: The addition of Android apps to a Policy from the App Catalog is described in "Configuring Policy Settings" on page 102.

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.

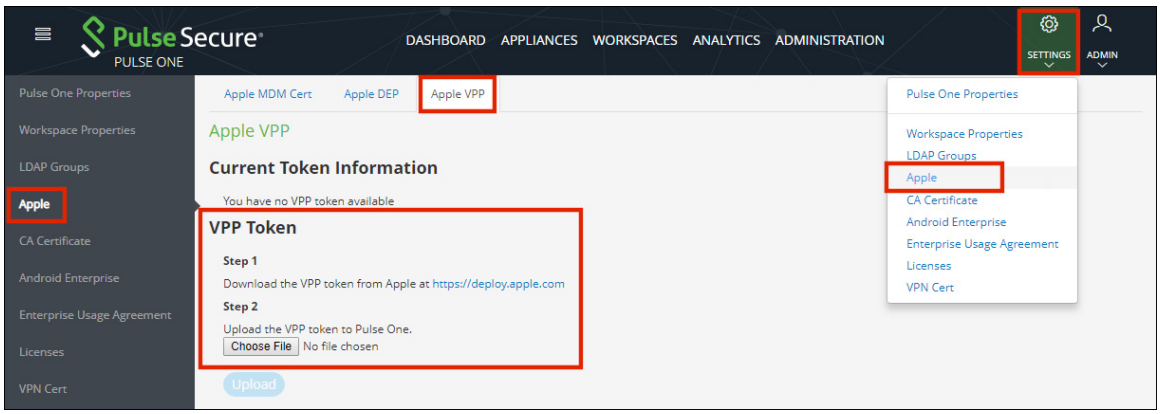
You can assign VPP-licensed apps to policies, and then apply those policies to iOS devices.

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 149 Apple VPP page



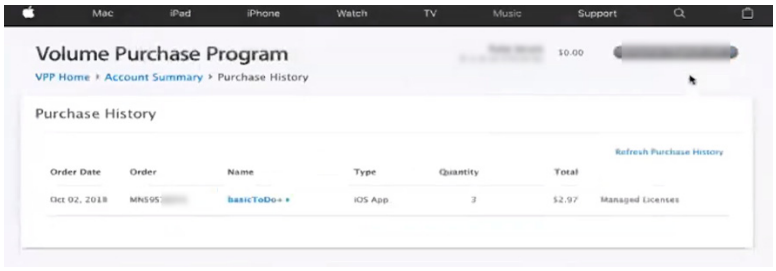
© 2019 Pulse Secure, LLC.

3. Under **VPP Token**, click the link to access the Apple Deployment Program (ADP) website.
4. On the ADP website, enroll your business.

   Note: You require the Data Universal Numbering System (D-U-N-S) number for your business.

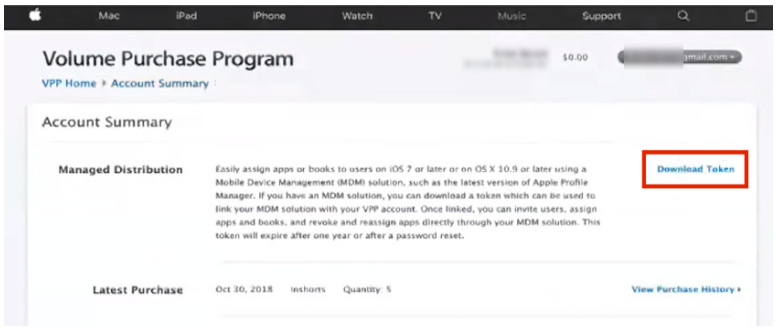
   Note: If you have previously registered your business on ADP to use Apple DEP, the same ADP account can be used for Apple VPP.
5. Verify your account using the two-step email verification process.
6. On the Apple VPP website, purchase iOS apps in the required quantities. For example:

   FIGURE 150 VPP purchases



7. On the Apple VPP **Account Summary** page, click **Download Token** and save the file locally.

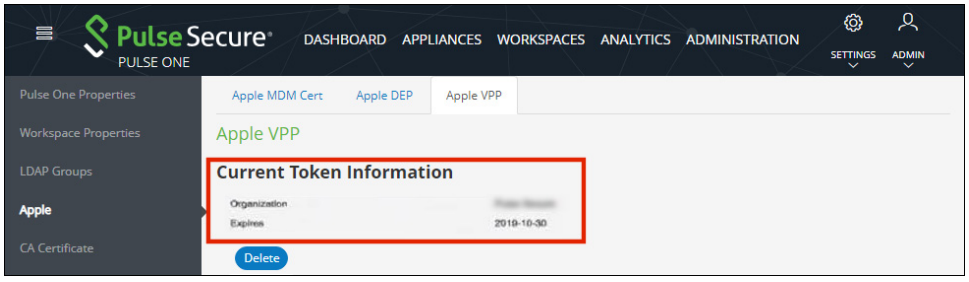
   FIGURE 151 Download VPP Token



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 152 Current Token Information

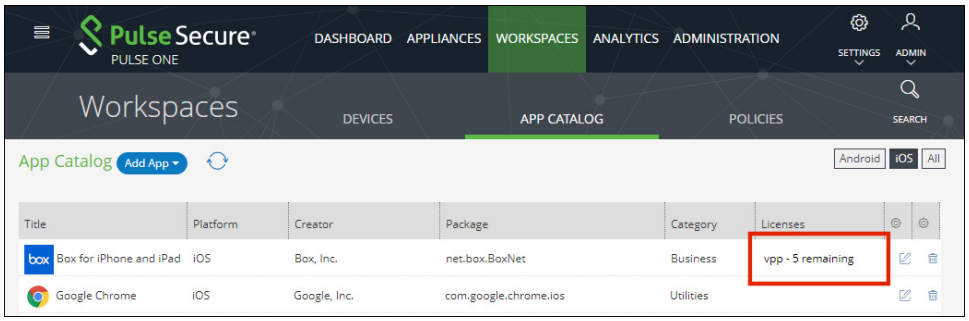


© 2019 Pulse Secure, LLC.

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 153 App Catalog With VPP Licenses



11. Add VPP-licensed apps to new or existing policies.

12. (Optional) If the policies are in use, publish the policies.

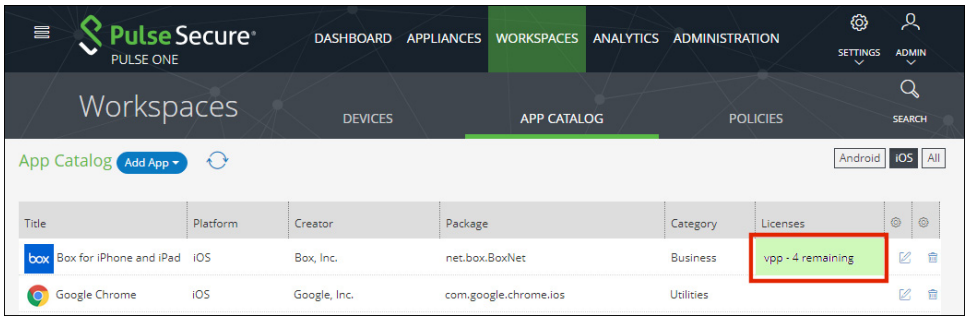
    The VPP-licensed apps are installed on all devices that use the policy, subject to license availability.

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 154 Updated License Counts



© 2019 Pulse Secure, LLC.

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 125**.
- Manually, from a third-party source, see **"Adding an iOS App to the App Catalog Manually" on page 127**.

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.

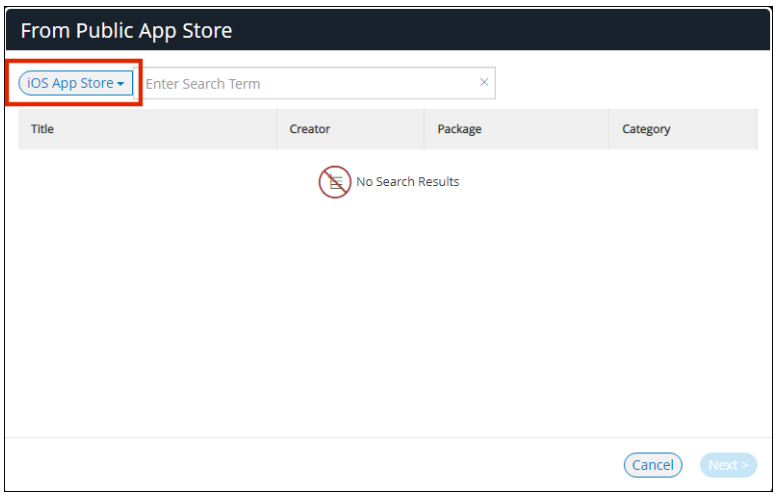
1. Select the **Workspaces** menu.
2. Select the **App Catalog** tab.

   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 155 Add iOS App From Store



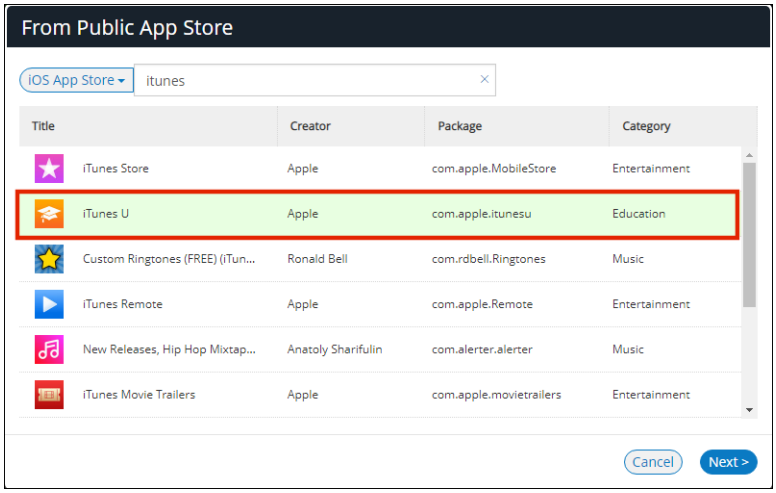
5. Type the name of the app in the **Search** box and press Enter.

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

© 2019 Pulse Secure, LLC.

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

FIGURE 156 Select iOS App from Search Result

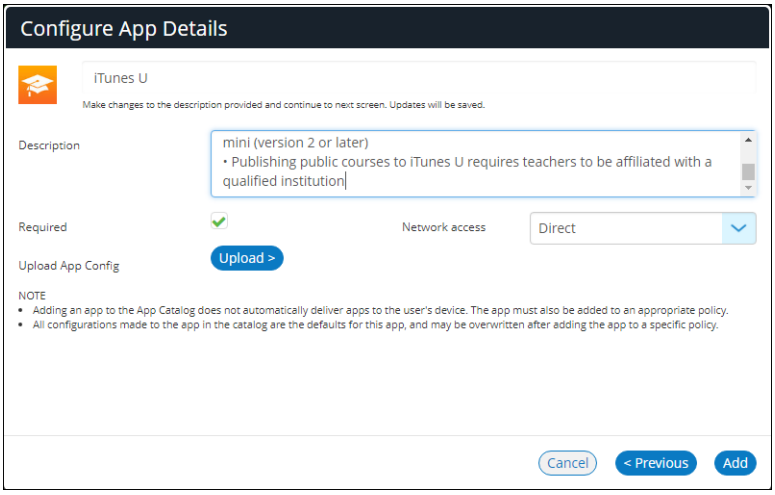


The **Configure App Details** dialog appears.

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 157 Configure iOS App Details



© 2019 Pulse Secure, LLC.

- 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 130**.

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.

© 2019 Pulse Secure, LLC.

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

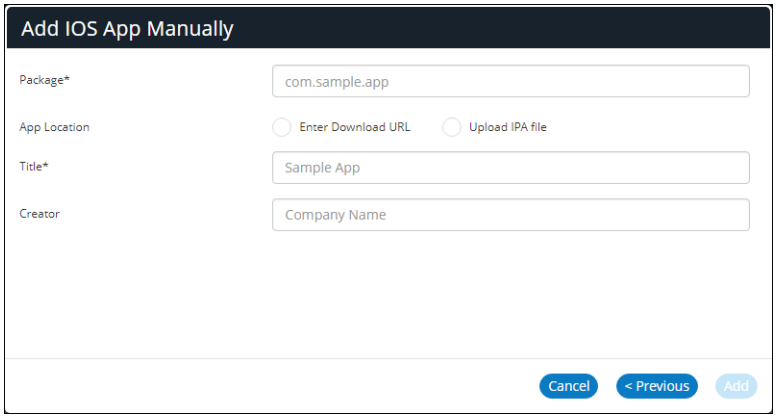
   The **Add App Manually** dialog appears.

   FIGURE 158 Add App Manually

4. In the **Add App Manually** window, select **Upload iOS App** and click **Next**.

   The **Add iOS App Manually** dialog appears:

   FIGURE 159 Add iOS App Manually



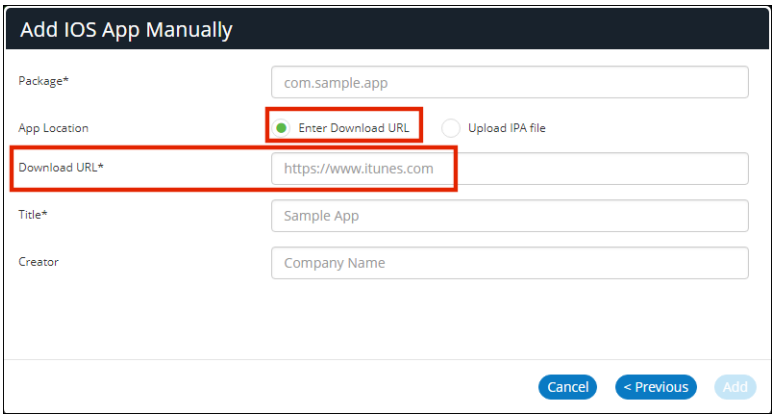
5. Specify the app **Package**. For example: com.demo.word.
6. Specify the app **Title**. This will be the name of the app in the **App Catalog**.
7. Specify the app **Creator**. That is, the provider of the app.

© 2019 Pulse Secure, LLC.

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 160 Source an iOS App from a URL

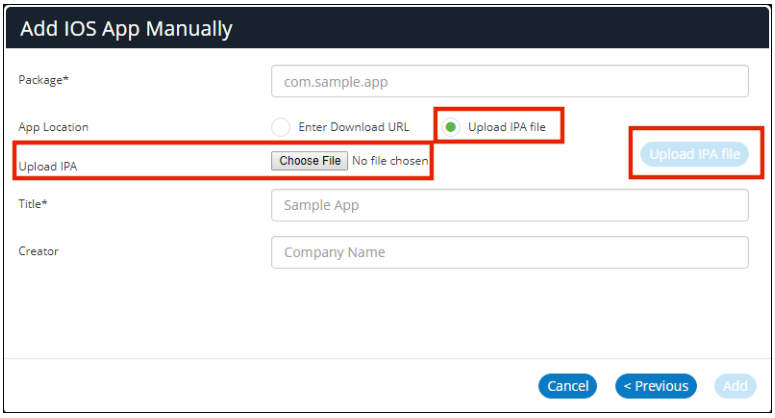
    - Specify the **Download URL**.

    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 161 Source an iOS App from a Local Copy

    - 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 130**.

© 2019 Pulse Secure, LLC.

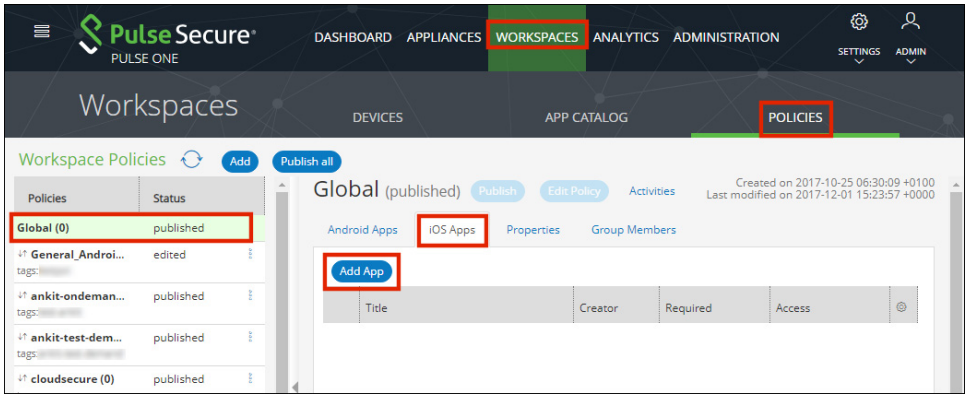
Adding iOS Apps to a Policy from the App Catalog

To add the app to a policy:

1. Select the **Workspaces** menu.
2. Select the **Policies** tab.

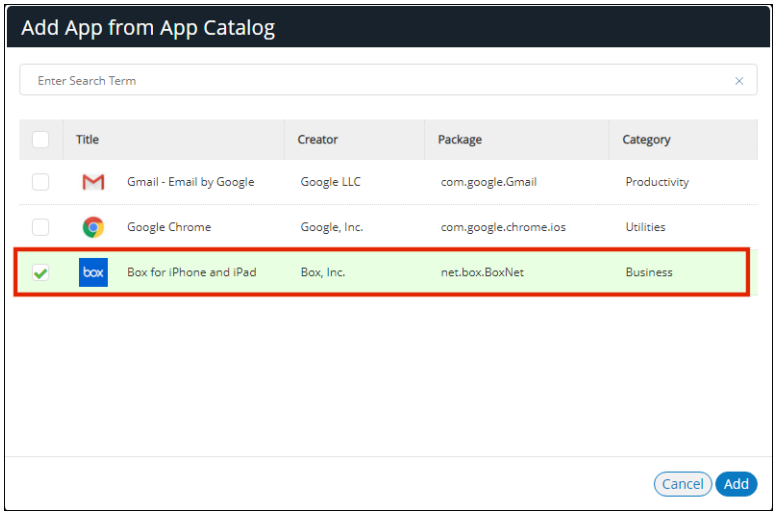
   A list of policies is displayed.
3. Select a policy from the list, select the **iOS Apps** tab, and click **Add App**.

   FIGURE 162 Add iOS App



   The **Add App from App Catalog** dialog appears.
4. Select the app from the app catalog list and click **Add**.

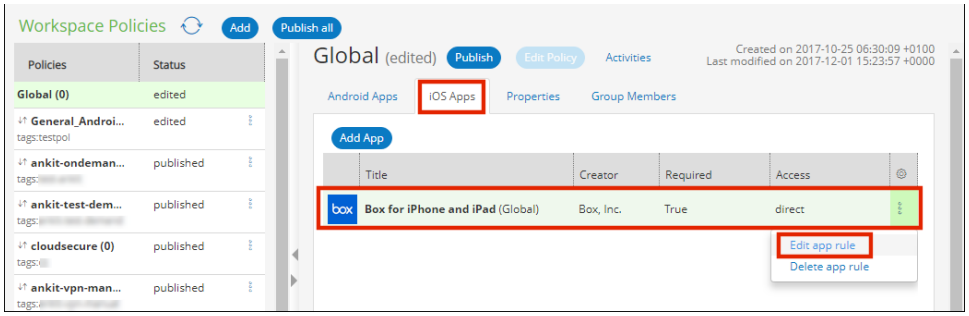
   FIGURE 163 Add App from App Catalog



© 2019 Pulse Secure, LLC.

5. In the **iOS Apps** tab, select the app and click **Edit app rule**.

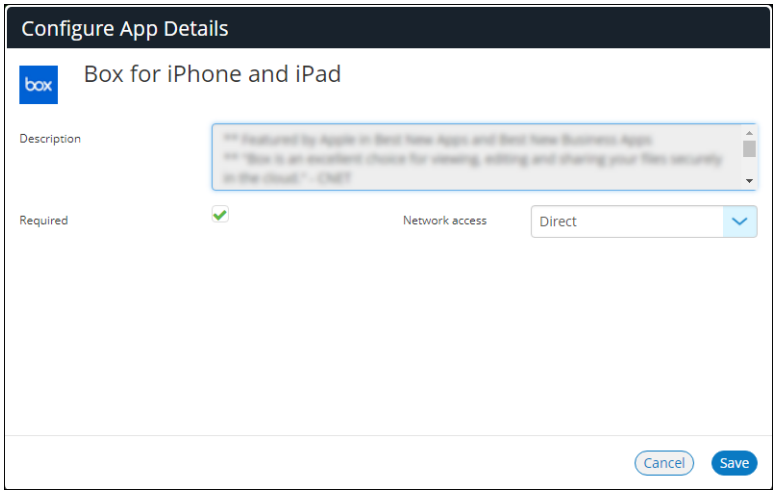
FIGURE 164 Edit App Rule



The **Configure App Details** dialog appears.

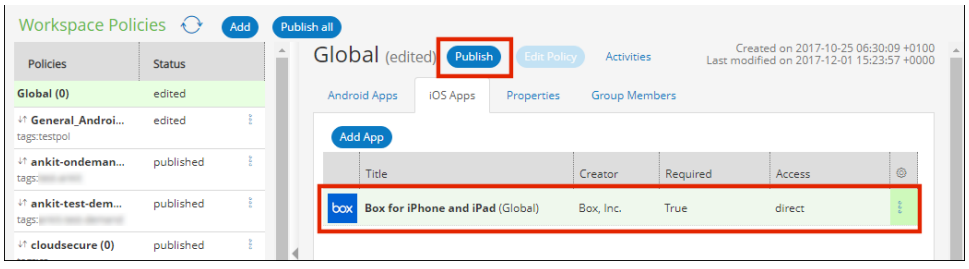
6. In the **Configure App Details** dialog, make appropriate changes and click **Save**.

FIGURE 165 Configure App Details



7. Select the app and click **Publish**.

FIGURE 166 Publish App



A confirmation prompt appears.

8. Click **Yes** to confirm the publication.

This completes the process.

© 2019 Pulse Secure, LLC.

Managing Policies

This section describes the following tasks:

- "Creating a Policy" on page 132.
- "Understanding Policy Properties" on page 135.

Creating a Policy

When you create a policy, you define specific users and device types to which the policy applies:

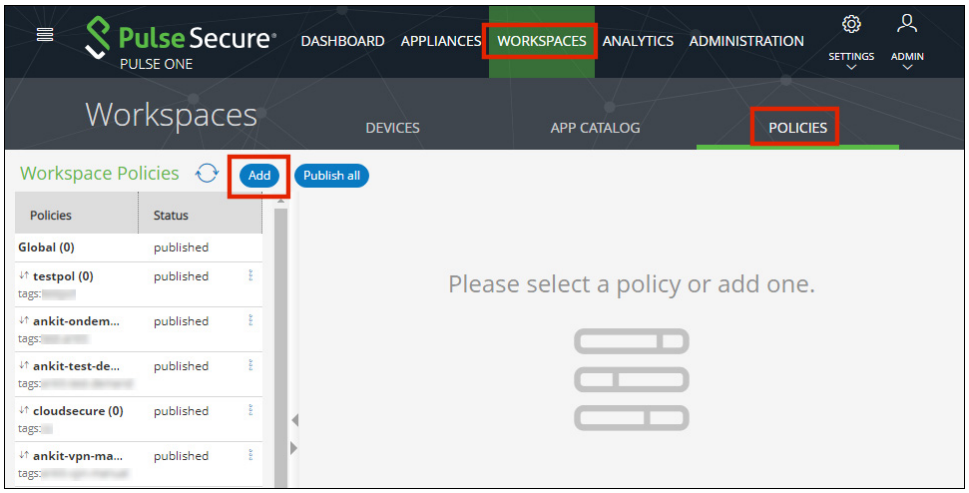
- Each policy applies to users listed as its **User tags**.
- Each policy can have one of three **Device User Mode** settings:
    - BYO: The policy is applied to a user's BYO devices only.
    - Corporate Owned: The policy is applied to a user's corporate owned devices only.
    - Both (BYO and Corporate 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 167 Workspace Policies



   The **Add Policy** dialog appears.

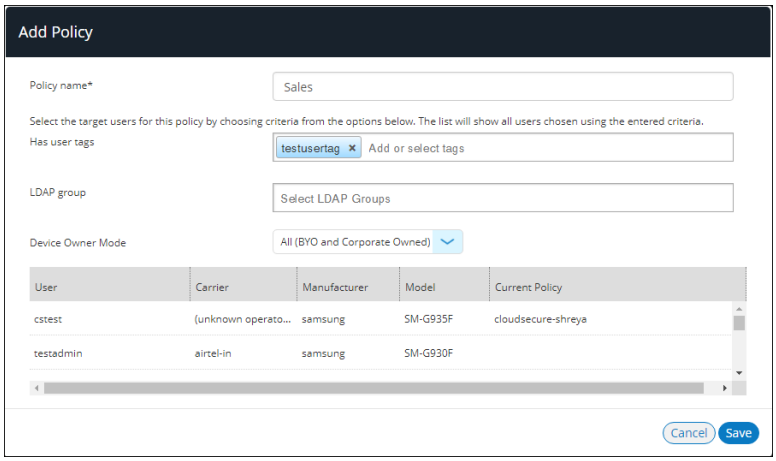
© 2019 Pulse Secure, LLC.

4. Specify the **Policy Name**.

   Note: Policy names are not unique. Policies are unique based on their search criteria.

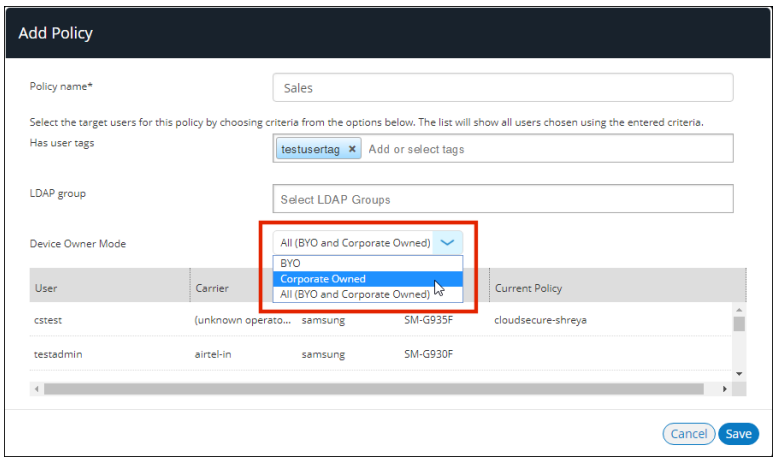
5. Specify the **User tags** and **LDAP Group** for the policy. For example:

   FIGURE 168 Add Policy



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 169 Add Device Owner Mode to Policy



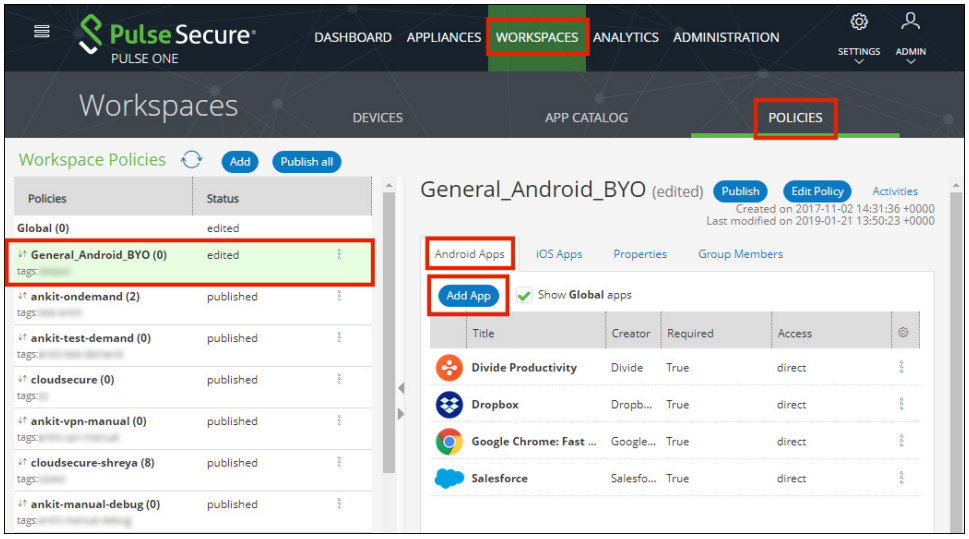
7. Click **Save**.

   The policy is created with an edited state.

© 2019 Pulse Secure, LLC.

8. You can now add applications and properties to the policy before applying the policy to mobile devices. For example:

FIGURE 170 Add Apps and Properties

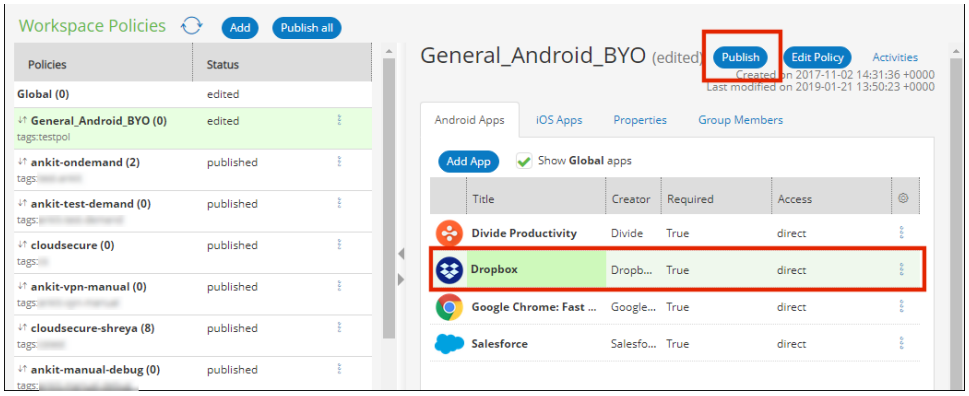


9. After you have completed editing the policy, click **Publish**.

   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 171 Publish the Policy

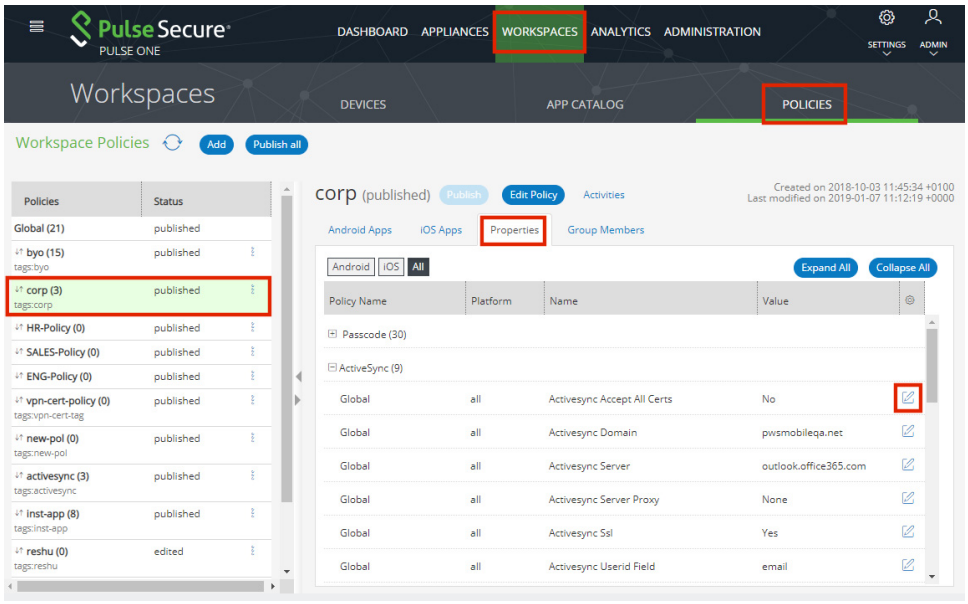


© 2019 Pulse Secure, LLC.

Understanding Policy Properties

This section describes all supported policy properties for a workspace.

FIGURE 172 Policy Properties



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.

© 2019 Pulse Secure, LLC.

- **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.

© 2019 Pulse Secure, LLC.

- **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.

© 2019 Pulse Secure, LLC.

ActiveSync

All **ActiveSync** properties are supported by both Android and iOS. See also **"iOS ActiveSync" on page 143**.

- **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 150** 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.

© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

- **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.

© 2019 Pulse Secure, LLC.

- **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.

© 2019 Pulse Secure, LLC.

- **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*.

© 2019 Pulse Secure, LLC.

- **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.

© 2019 Pulse Secure, LLC.

- **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 27**.

© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

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 41**.

- **VPN OnDemand Enabled** – Boolean. If *True*, VPN on Demand is enabled, see **"Configuring Managed Clients" on page 67**.

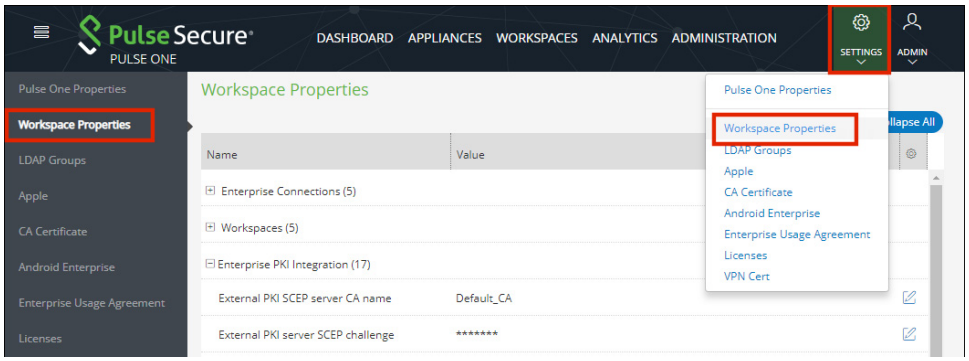
© 2019 Pulse Secure, LLC.

Configuring Workspace Properties

To configure Workspace properties:

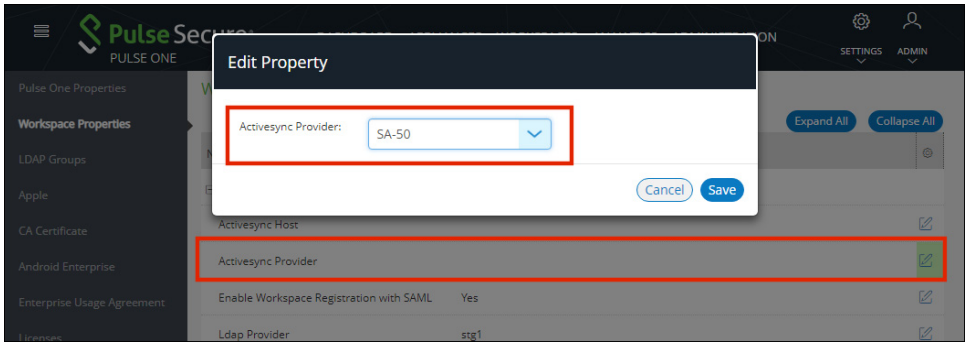
1. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties**.

   FIGURE 173 Workspace Properties



2. Click the **Edit** button corresponding to the field you want to edit.
3. Change the value and then click **Save**. For example:

   FIGURE 174 Edit Property



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.

© 2019 Pulse Secure, LLC.

- **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 153**.

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 116**.
- **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 172**.

  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 clients** – Boolean. This controls how mobile devices are enrolled by Pulse Workspace:
  - If *True*, mobile devices will be enrolled as *managed clients.*

    Note: Currently, the *managed client* method is only supported on iOS devices.
  - If *False* (default), mobile devices will be enrolled as *managed workspaces*.

  For full details, see **"Understanding Managed Devices and Managed Clients" on page 41**.
- **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 165**.
- **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 165**.

© 2019 Pulse Secure, LLC.

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 138**. 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 138**. 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.

© 2019 Pulse Secure, LLC.

- **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 138**.

  - 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.

© 2019 Pulse Secure, LLC.

- **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.

© 2019 Pulse Secure, LLC.

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 153.
- "Ensuring that PCS is Synchronized with Pulse One" on page 155.
- "Configuring a VPN Provider in the Workspace Properties" on page 156.
- "Updating and Publishing a Policy to Use a Specified VPN Provider" on page 158.

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

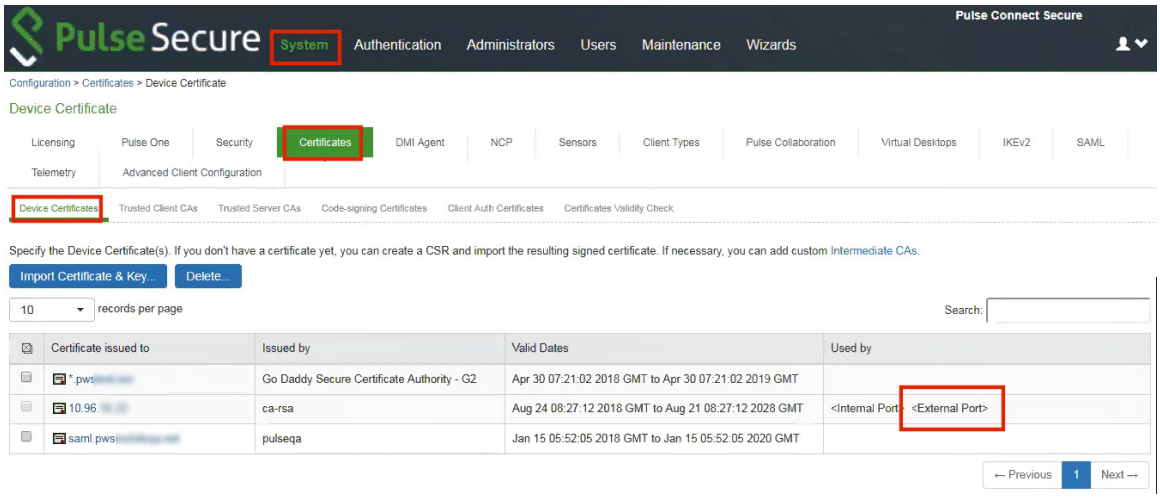
First, you must ensure that the PCS that will act as the VPN provider has a CA certificate assigned to its external port.

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 175 Device Certificates



© 2019 Pulse Secure, LLC.

In this example:

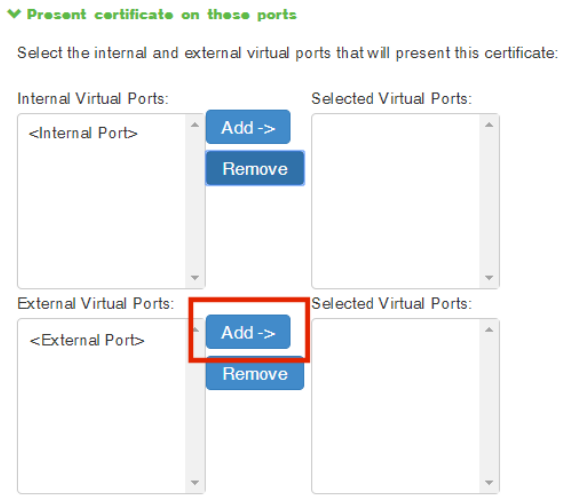
- The *10.96.xx.xx* CA certificate has a **Used by** property that includes <External Port>, which indicates that it is associated and in use on the external interface of the PCS appliance.
- The other certificates have no **Used by** values set. These certificate are not currently assigned to any interface 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:

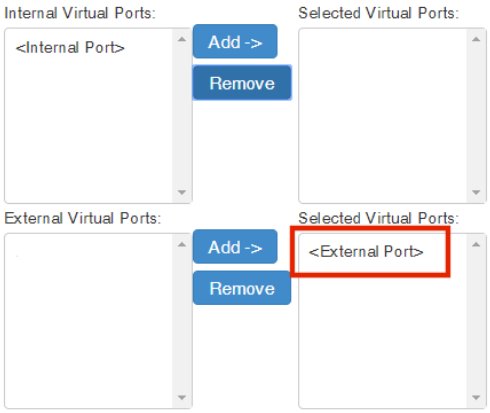
   FIGURE 176 CA Certificate Not Associated with PCS Interfaces



© 2019 Pulse Secure, LLC.

5. Under **External Virtual Ports**, click **Add** to move <External Port> into **Selected Virtual Ports**. For example:

   FIGURE 177 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 155**.

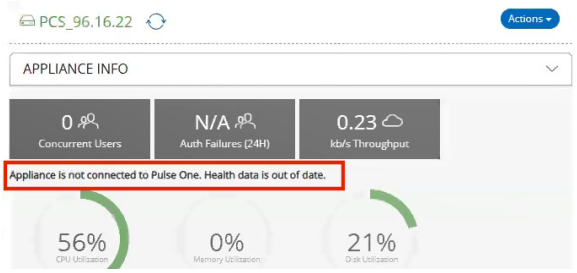
Ensuring that PCS is Synchronized with Pulse One

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 178 PCS Appliance Information



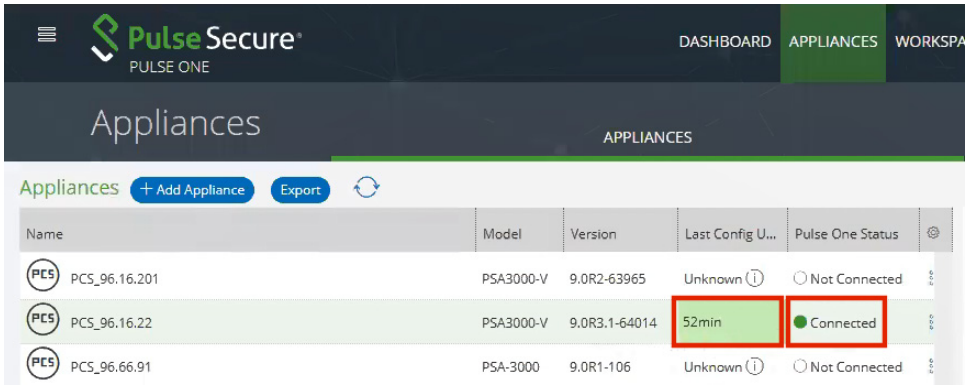
© 2019 Pulse Secure, LLC.

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:

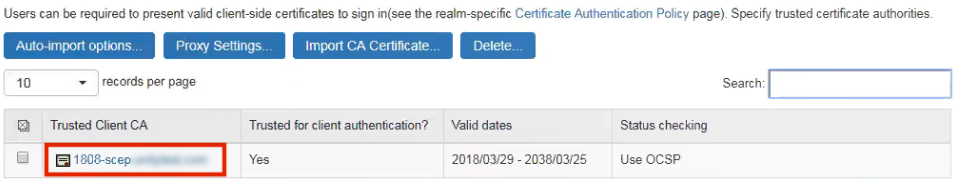
FIGURE 179 Synchronized PCS on Pulse One



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 180 Confirm Upload of the CA Certificate



You must now configure the VPN Provider workspace property, see **"Configuring a VPN Provider in the Workspace Properties" on page 156**.

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:

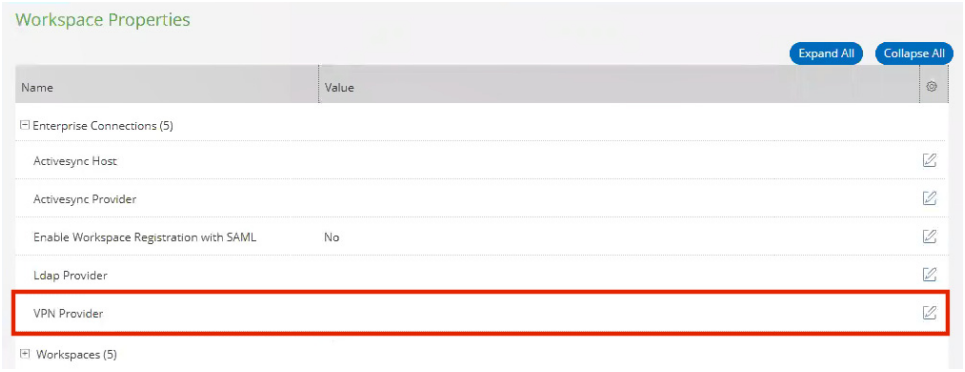
1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page and select **Workspace Properties**.

   The **Workspace Properties** page appears.

© 2019 Pulse Secure, LLC.

3. Expand the Enterprise Connections category. For example:

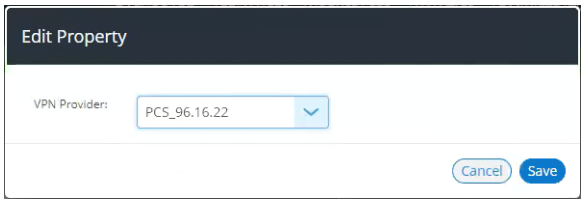
   FIGURE 181 Workspace Properties



4. Click the **Edit** ( ) icon for the **VPN Provider** entry.

   The **Edit Property** dialog appears. For example:

   FIGURE 182 Edit VPN Provider



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 183 Updated Workspace Properties

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 158**.

© 2019 Pulse Secure, LLC.

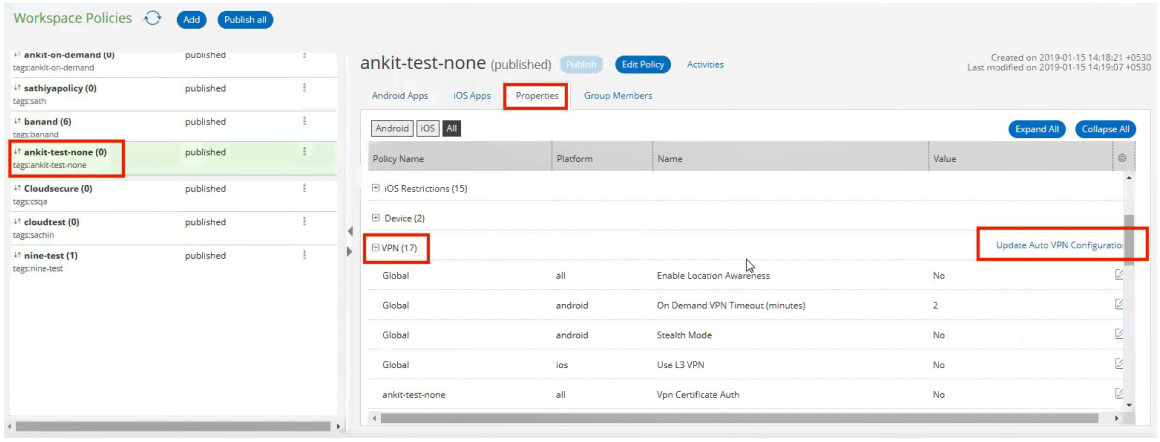
Updating and Publishing a Policy to Use a Specified VPN Provider

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 184 VPN Policy Properties: Auto Update VPN Configuration

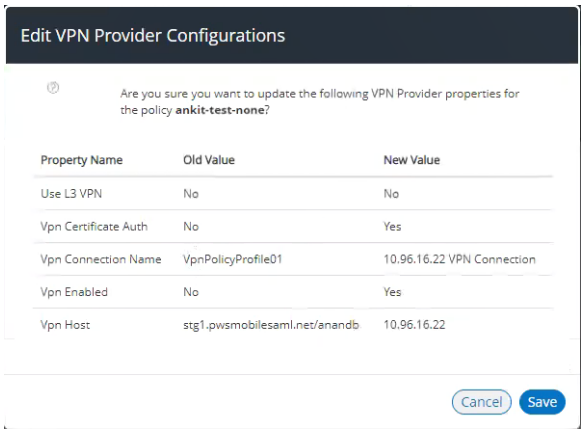


© 2019 Pulse Secure, LLC.

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:

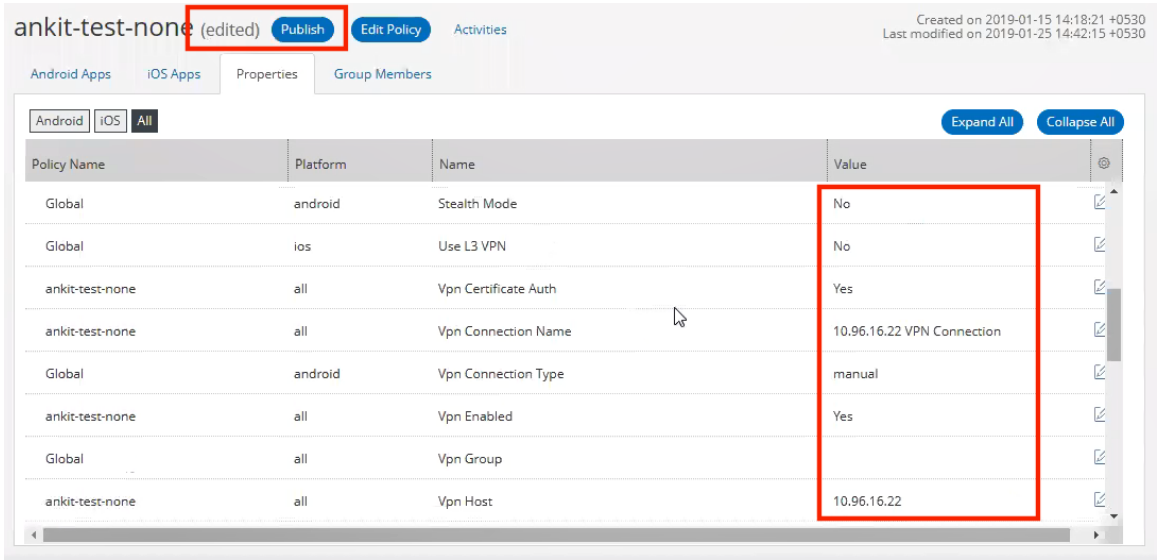
   FIGURE 185 Edit VPN Provider Configurations



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 186 Updated VPN Policy Properties



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.

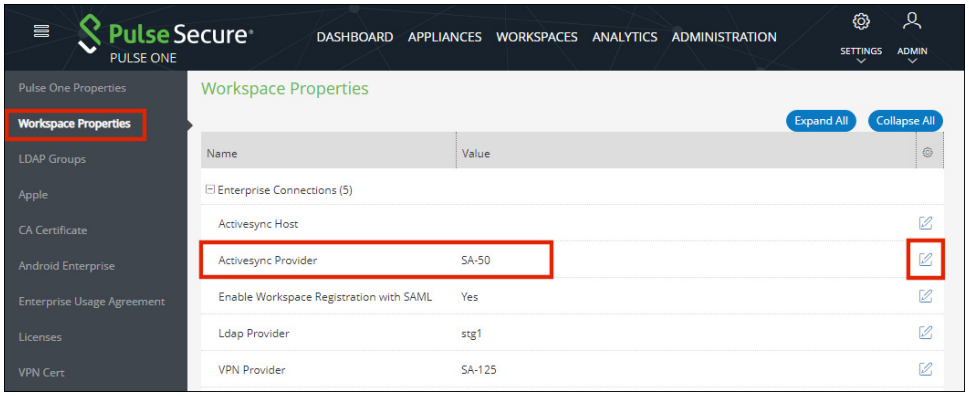
© 2019 Pulse Secure, LLC.

Configuring Appliance ActiveSync

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.

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

   FIGURE 187 Workspace Properties



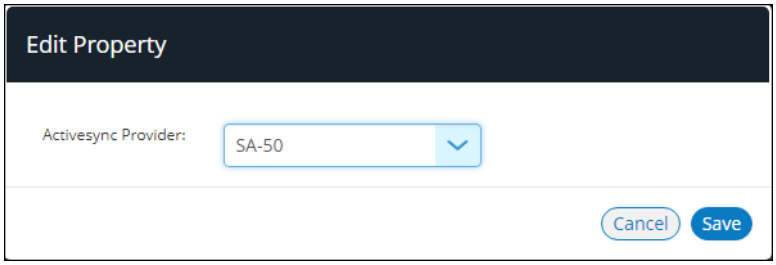
2. The **Activesync Provider** field must be set to the Connect Secure device. This requires ActiveSync configuration in the Pulse Connect Secure server, and for the details refer to the section "ActiveSync Configuration" in the *Pulse Workspace Configuration Guide*.

3. Click the **Edit** ( ) icon.

   The **Edit Property** dialog appears.

4. Modify the **ActiveSync** property of the policy. For example:

   FIGURE 188 ActiveSync property



5. Click **Save**.

© 2019 Pulse Secure, LLC.

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 161**.
- 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 162**.

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.

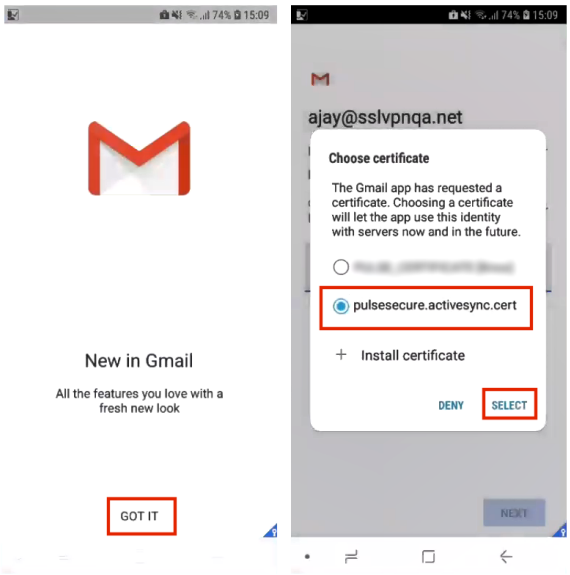
© 2019 Pulse Secure, LLC.

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 161**) 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 189 First Use of Gmail



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.

© 2019 Pulse Secure, LLC.

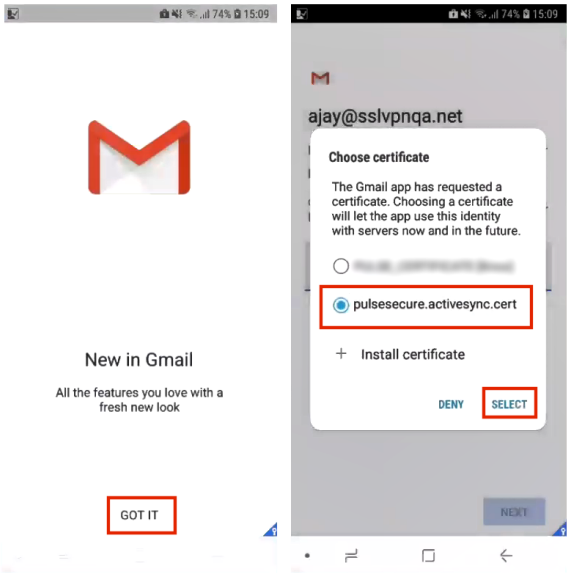
4. If you want Windows CAWE to deliver an ActiveSync certificate to Android devices:
    - Set the **Use Windows CA server CAWE to request ActiveSync certificates for both Android and iOS devices** to *True*.
    - Set the **Use SCEP to request certificate for Android ActiveSync from external PKI server** 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.

© 2019 Pulse Secure, LLC.

On each device, when a supported app (see **"Configuring Certificate-Based ActiveSync" on page 161**) 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 190 First Use of Gmail



© 2019 Pulse Secure, LLC.

Working with Device Location

This section describes the device location functionality in Pulse Workspace.

- "Overview of Device Location" on page 165.
- "Creating a Google API Key" on page 166.
- "Configuring Device Location" on page 172.
- "Locating a Device" on page 179.
- "Working with Lost Mode for a Device" on page 180.

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.

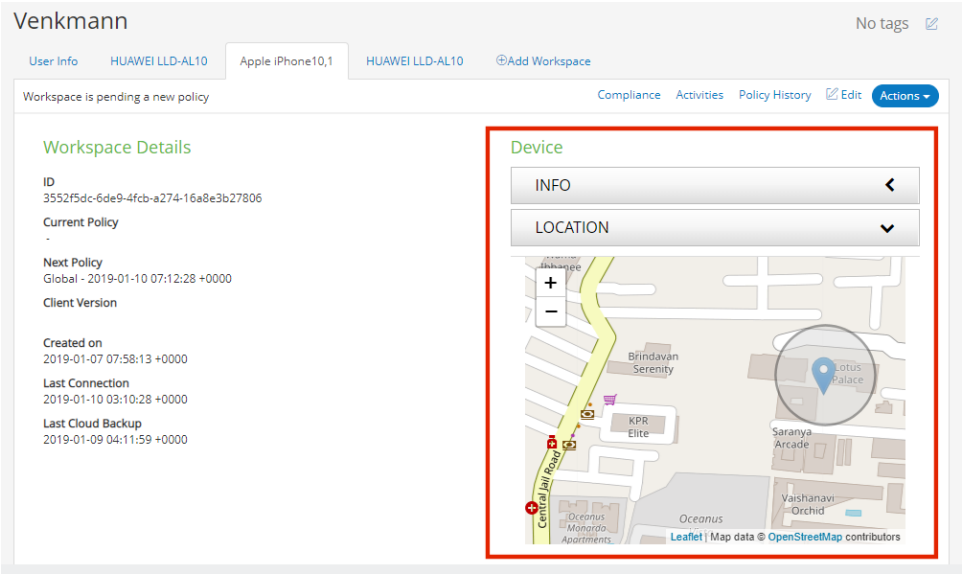
Device location can be enabled by admins and configured for use through policies applied to devices. Pulse Workspace uses an Apple/Google push service to send a notification to the Pulse Client App which is installed on a device. The Pulse Client then uses location services to locate the device and notify 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 191 Device Location Map



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 166**.

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 166**.
- **"Creating a Google Cloud Project" on page 168**.
- **"Generating a Google API Key for a Project" on page 170**.

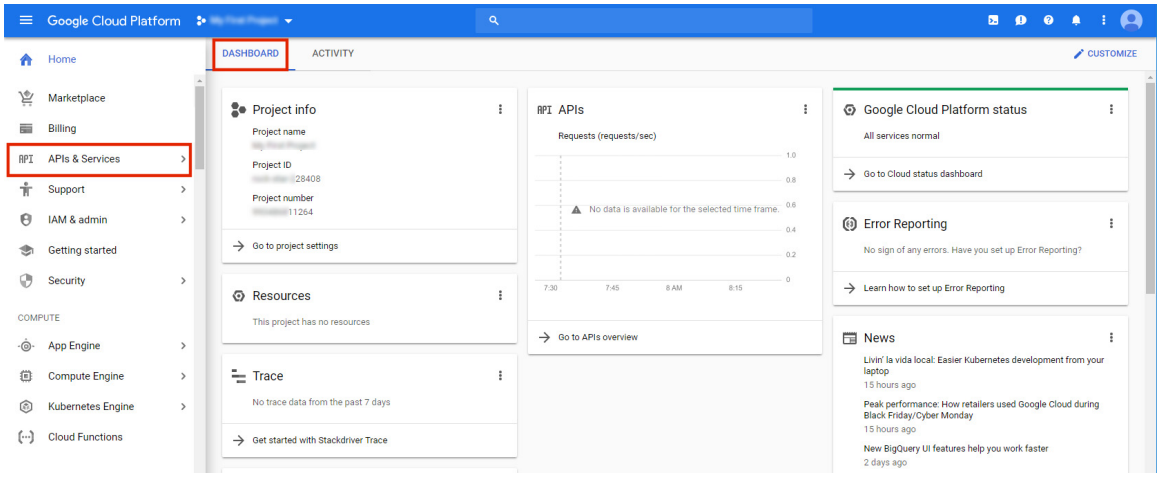
Enabling the Maps JavaScript API

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 192 Google Cloud Platform Dashboard

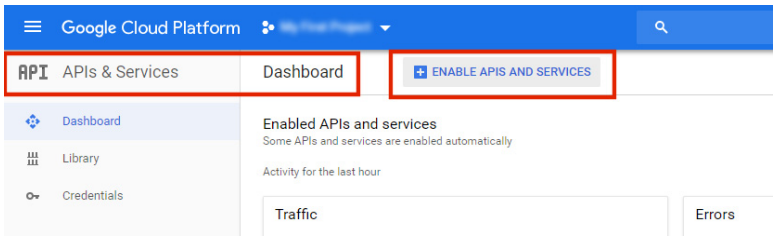


© 2019 Pulse Secure, LLC.

4. In the left menu, click **APIs & Services** and then click **Dashboard**.

   The **APIs & Services Dashboard** appears. For example:

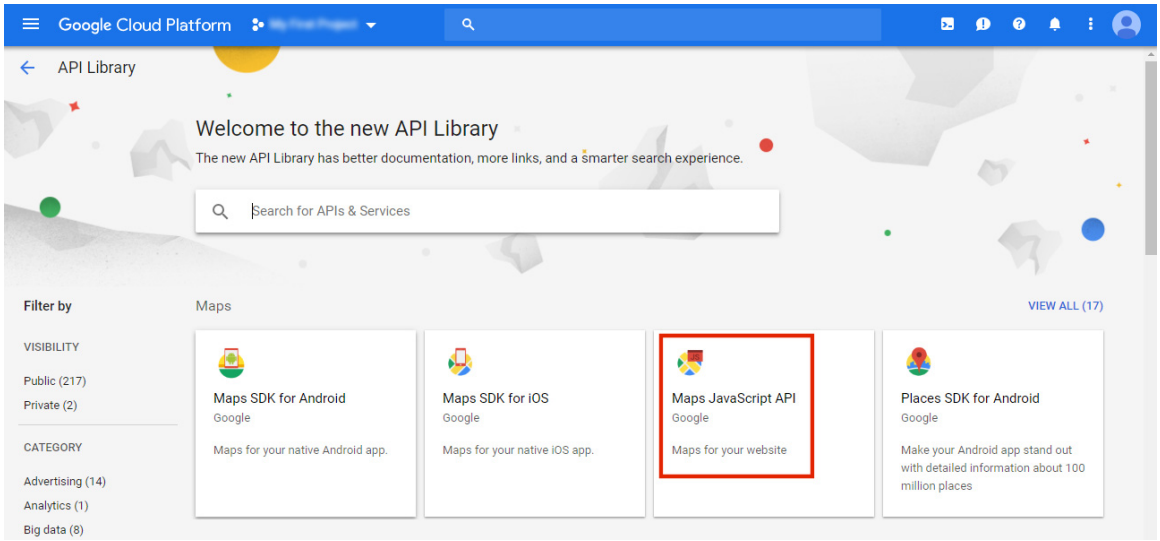
   FIGURE 193 Google Cloud APIs and Services Dashboard



5. Click **Enable APIs and Services**.

   The **API Library** page appears. For example:

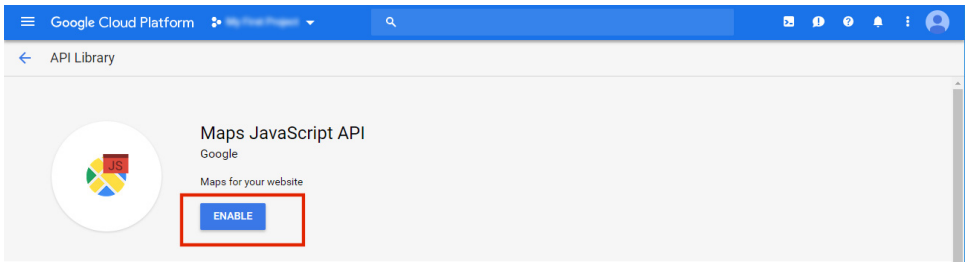
   FIGURE 194 Google Cloud API Library



6. Under **Maps**, click **Maps JavaScript API**.

   The **Maps JavaScript API** page appears.

   FIGURE 195 Google Cloud Maps JavaScript API

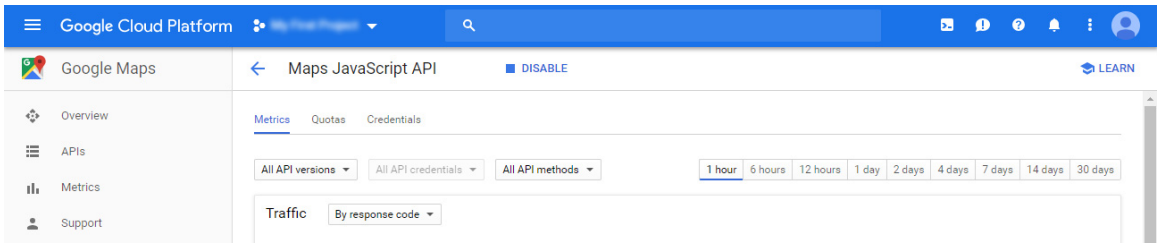


© 2019 Pulse Secure, LLC.

7. Click **Enable**.

   The **Maps JavaScript API** page updates.

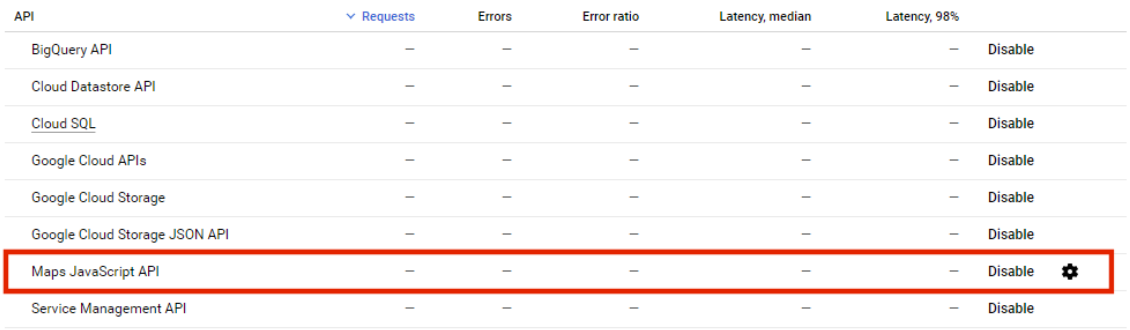
   FIGURE 196 Google Cloud Maps JavaScript API Updated



8. Return to the **APIs & Services Dashboard** and view the list of APIs.

   The list now includes Maps JavaScript API. For example:

   FIGURE 197 Google Cloud **APIs and Services Dashboard Updated**



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 168**.

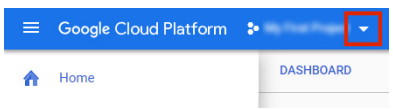
Creating a Google Cloud Project

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:

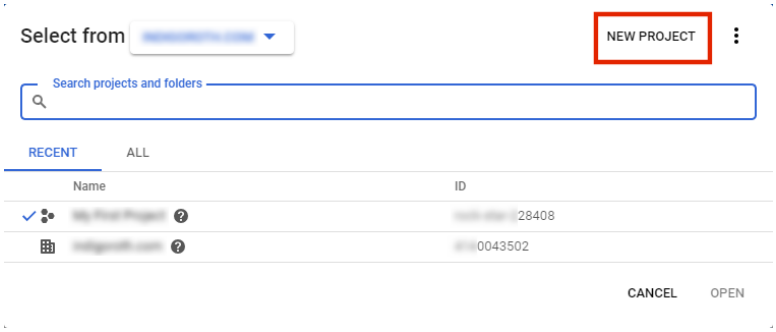
   FIGURE 198 Google Cloud Project Pull-Down



© 2019 Pulse Secure, LLC.

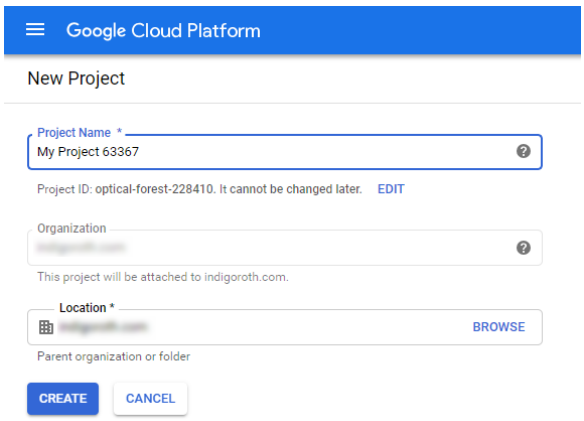
The **Select from** dialog appears. For example:

FIGURE 199 Google Cloud Select Project



5. (Optional) Click **New Project**, complete the **New Project** page for your required project and click **Create**. For example:

FIGURE 200 Google Cloud New Project



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 170**.

© 2019 Pulse Secure, LLC.

Generating a Google API Key for a Project

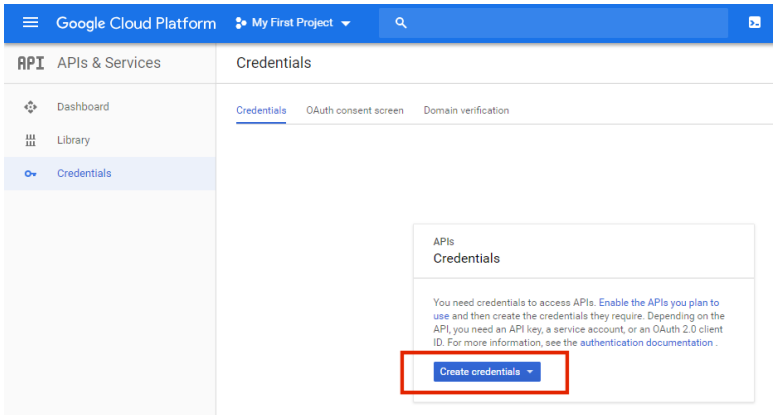
After you have enabled the Google Maps JavaScript API and opened the required Google Cloud Platform project, you can create the Google API key for the project.

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:

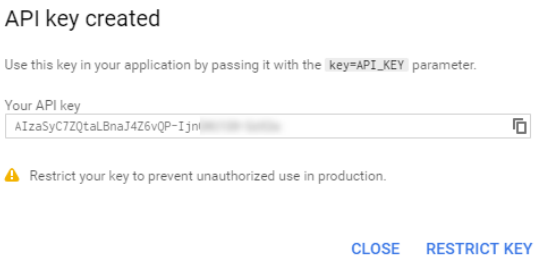
   FIGURE 201 Google Cloud Credentials

   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 202 Google Cloud API Key Created

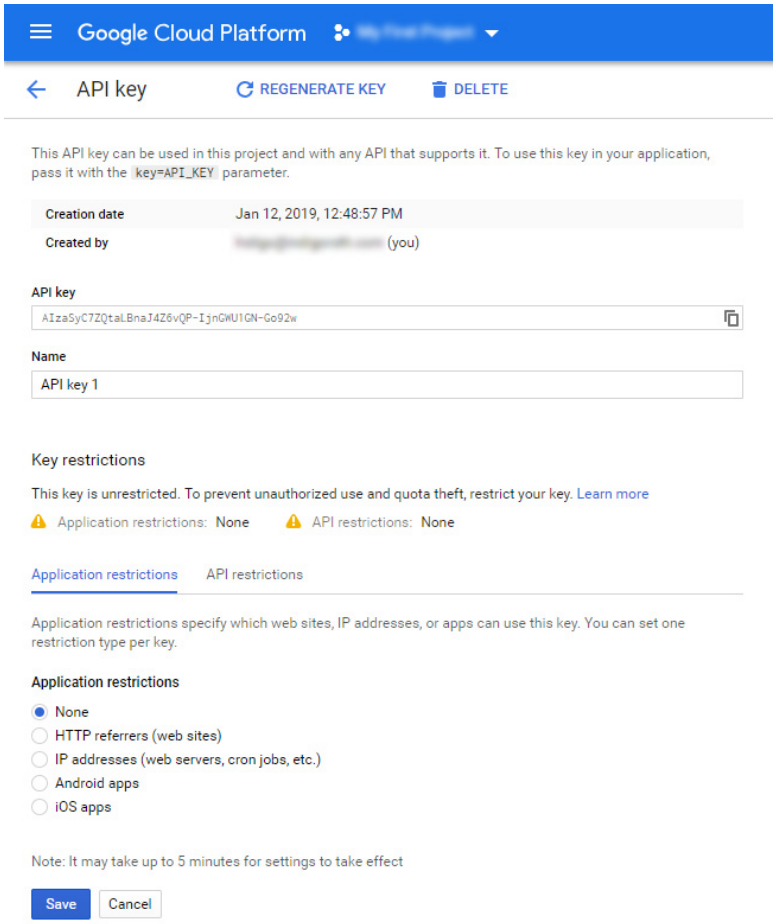
4. (Optional) Record **Your API key** and click **Close**.

   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**.

© 2019 Pulse Secure, LLC.

The **API key** page appears. For example:

FIGURE 203 Google Cloud API Key



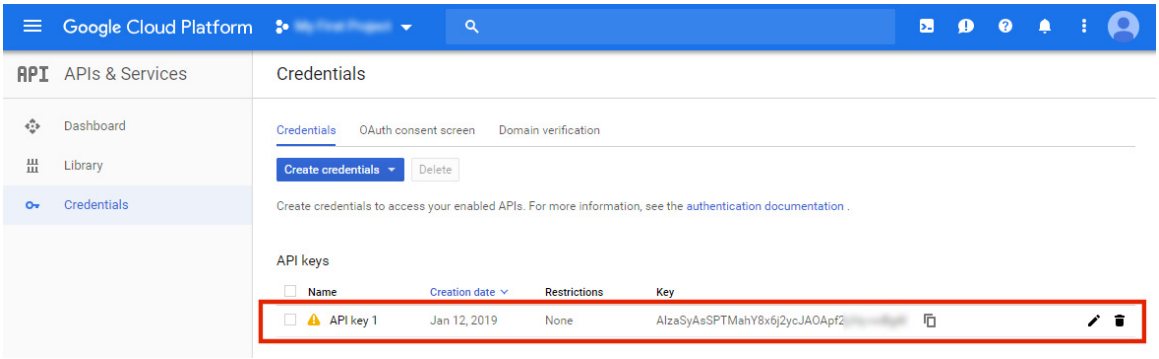
On this page, you can optionally perform any of the following:

- 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.

© 2019 Pulse Secure, LLC.

After you have created your API key, it is listed on the **Credentials** page. For example:

FIGURE 204 Google Cloud Credentials New API Key



You can then use the API key to enable Pulse Workspace to render device locations using Google Maps, see **"Configuring Device Location" on page 172**.

Configuring Device Location

Perform the following steps to configure device location:

- **"Configuring Workspace Properties to Enable Device Location" on page 172**.
- **"Configuring a Policy to Support Device Location" on page 174**.
- **"Configuring a Device After Device Location is Enabled" on page 176**.

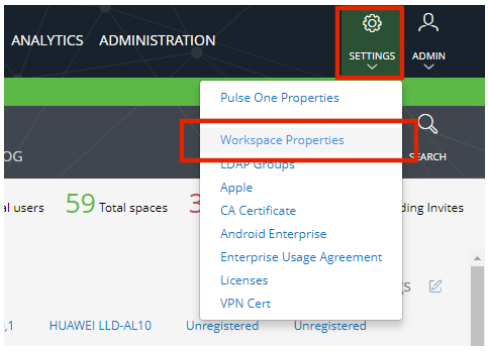
Note: Device location requires iOS v10 or later, or Android 8.0 or later.

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 205 Settings Menu

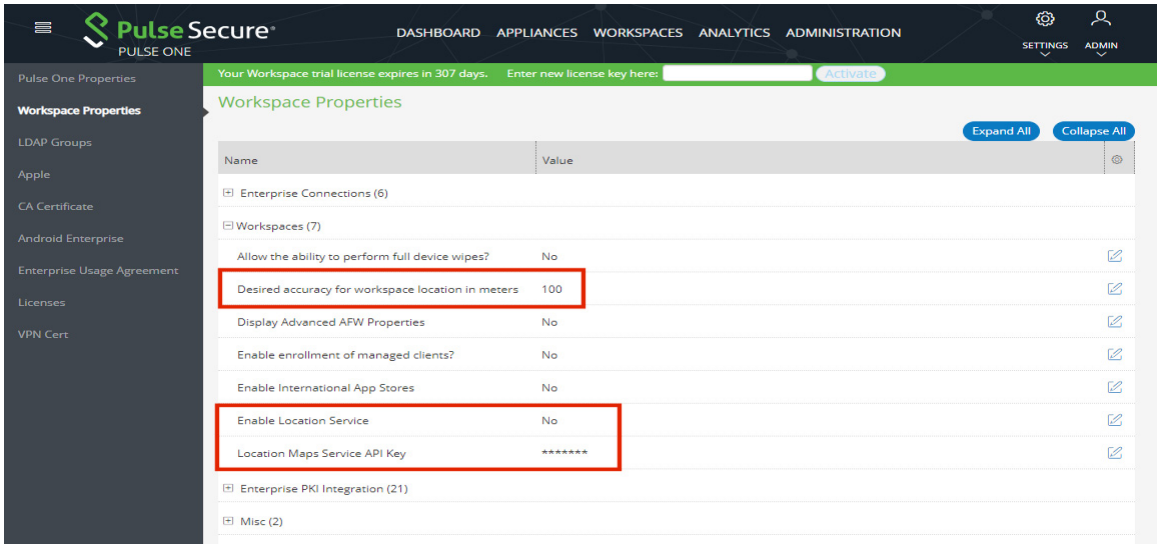
   

   The **Workspace Properties** page appears.

© 2019 Pulse Secure, LLC.

3. Expand the **Workspaces** group to view the **Enable Location Service** and **Location Maps Service API Key** properties. For example:

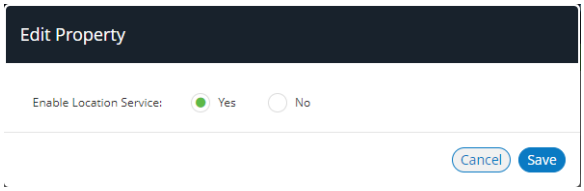
FIGURE 206 Workspace Properties



4. Click the **Edit** button for the **Enable Location Service** property.

   The **Edit Property** dialog appears.

FIGURE 207 Enable Location Service Workspace Property

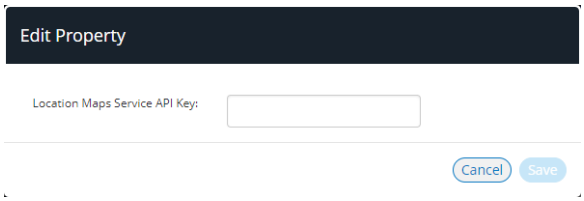


5. In the **Edit Property** dialog, set **Enable Location Service** to *Yes* and then click **Save**.

6. (Optional) If you have a Google API Key (see **"Creating a Google API Key" on page 166**, click the **Edit** button for the **Location Maps Service API Key** property.

   The **Edit Property** dialog appears.

FIGURE 208 Location Maps Service API Key Property



   In this dialog, enter the **Location Maps Service API Key** and then click **Save**.

© 2019 Pulse Secure, LLC.

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 **"Managing Policies" on page 132** and **"Workspaces" on page 149**.

   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 174**.

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.

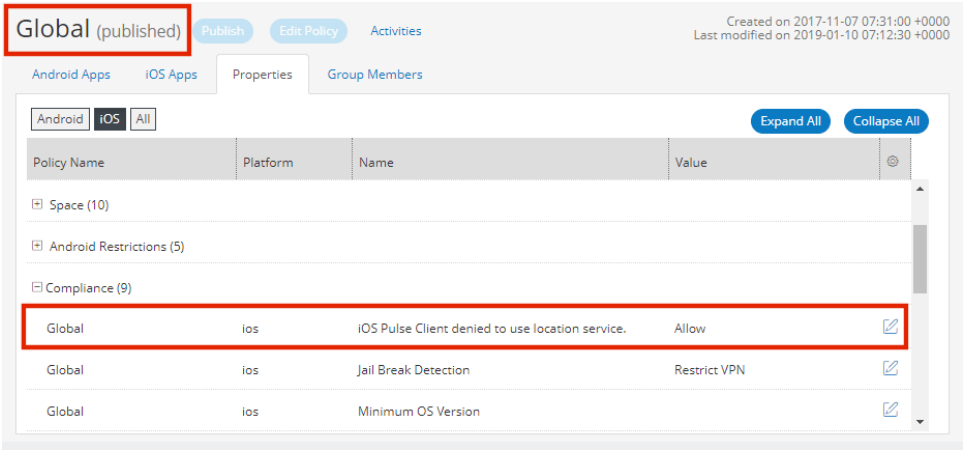
© 2019 Pulse Secure, LLC.

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:

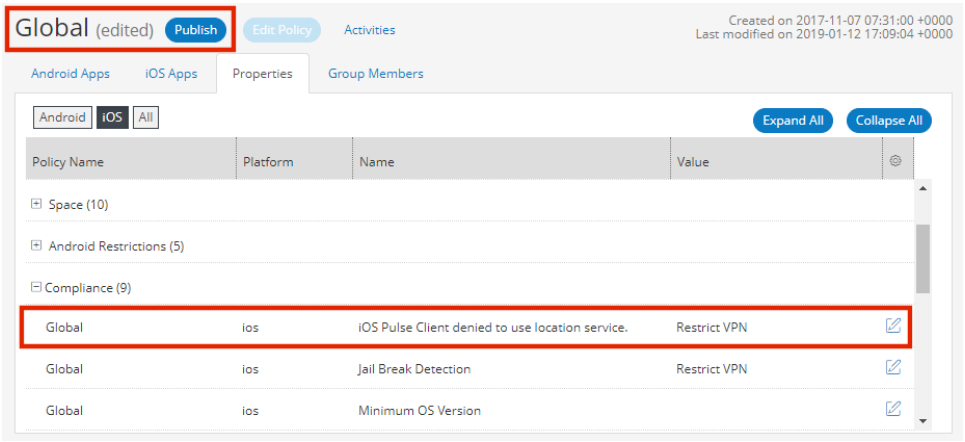
   FIGURE 209 iOS Denied To Use Location Service Property



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 210 Updated iOS Denied To Use Location Service Property



9. **Publish** the updated policy to implement it on all devices that use the policy.

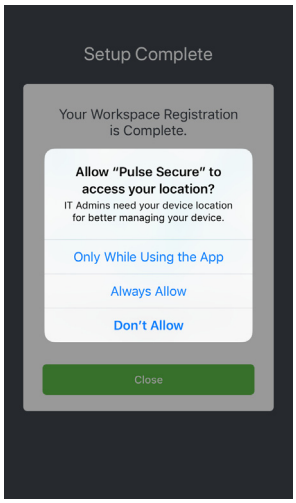
The configuration of the policy is complete. The feature must then be enabled manually on each device that uses the policy, see **"Configuring a Device After Device Location is Enabled" on page 176**.

© 2019 Pulse Secure, LLC.

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 211 Pulse Secure Device Location



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 174**.

- *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.

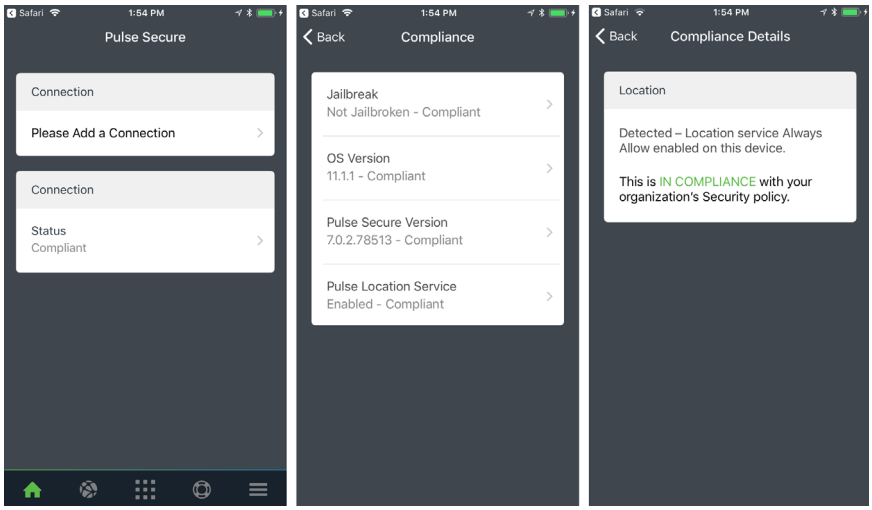
After a device user has confirmed that they allow the retrieval of their device location, Pulse Workspace can request the device location at any time, see **"Locating a Device" on page 179**.

© 2019 Pulse Secure, LLC.

The device location compliance status can be seen from the device:

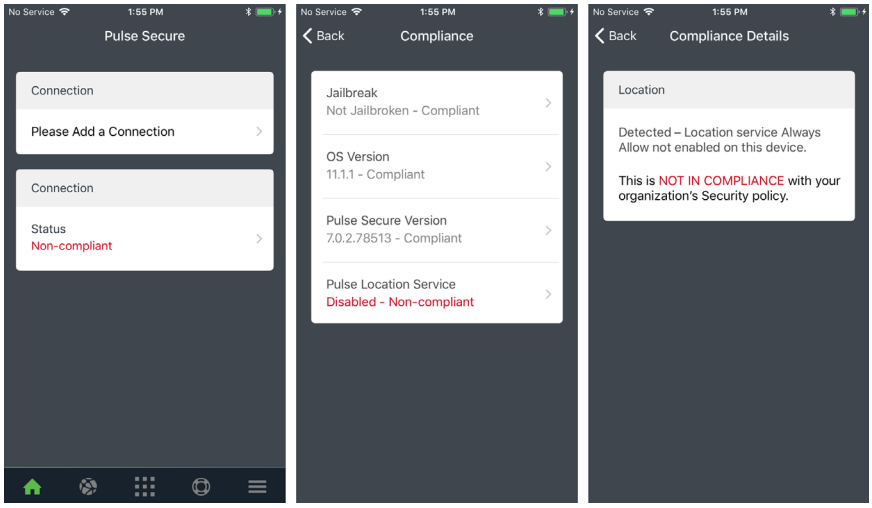
- A compliant device (in this example, an iOS device) is shown below:

  FIGURE 212 Pulse Secure Device Location Compliance



- A non-compliant device (in this example, an iOS device) is shown below:

  FIGURE 213 Pulse Secure Device Location Non-Compliance

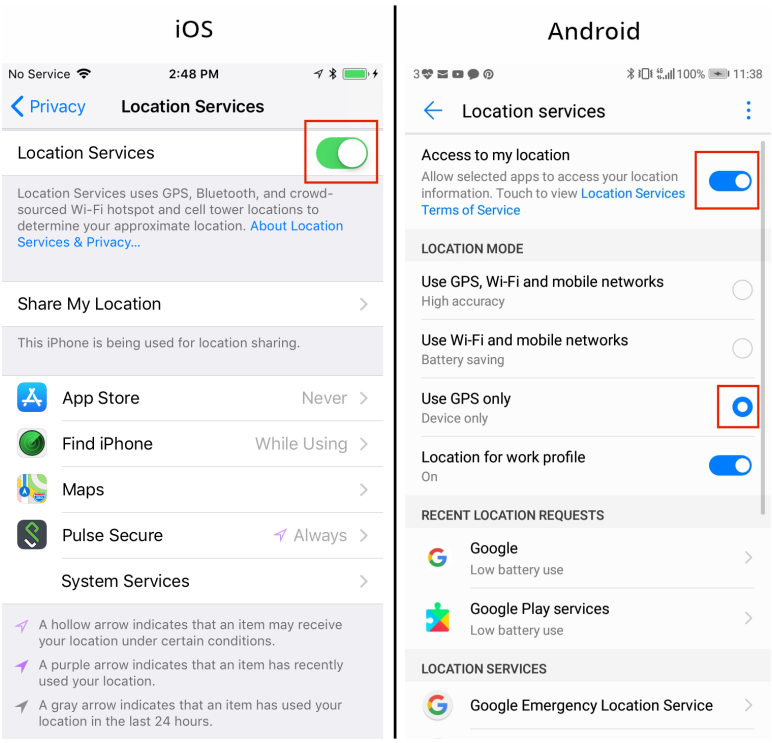


To enable/disable the Device Location feature:

- 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.

© 2019 Pulse Secure, LLC.

FIGURE 214 iOS and Android Device Location Services Switch



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.

© 2019 Pulse Secure, LLC.

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.

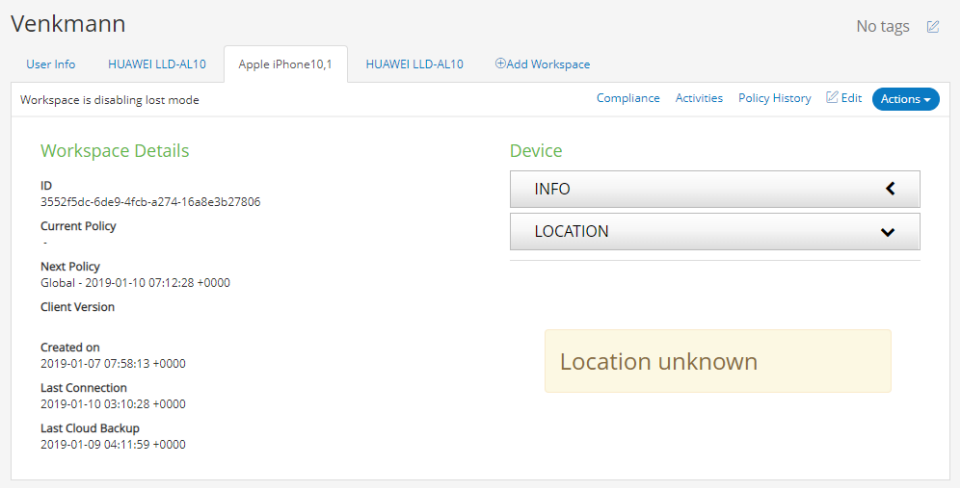
Note: Device location requires iOS v10 or later, or Android 8.0 or later.

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 215 iOS Device Location Unknown



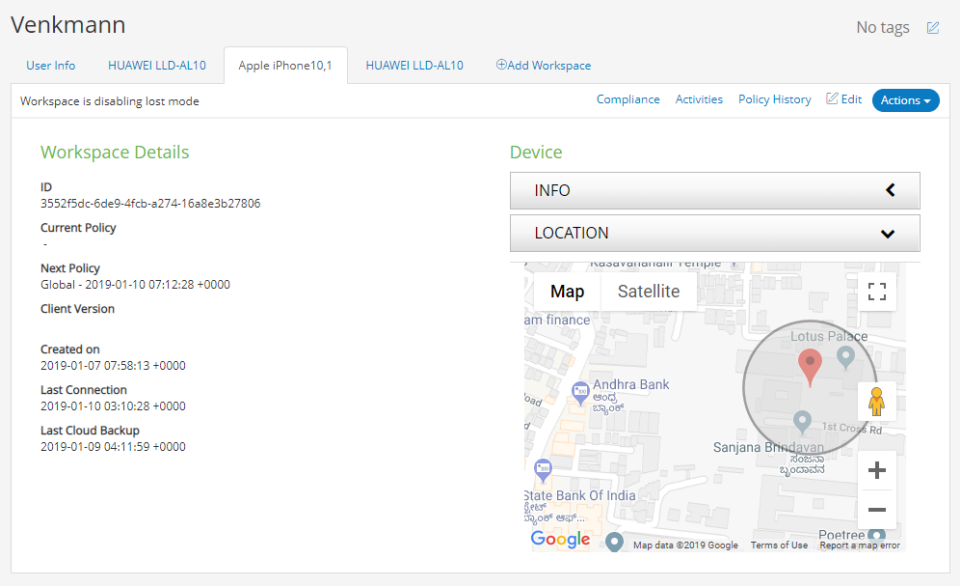
   In this example, no device location has yet been retrieved.

5. Click the **Actions** pull-down menu and select **Update Location**.

© 2019 Pulse Secure, LLC.

The device location request is sent. After it is retrieved, the device location appears. For example:

FIGURE 216 iOS Device Location Retrieved



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:

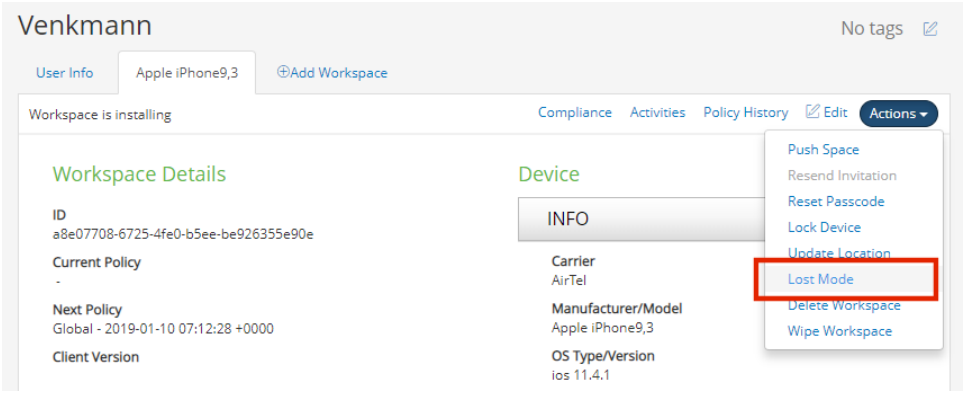
1. Log into Pulse Workspace.
2. Select the **Workspaces** menu.
3. Select the **Devices** tab.
4. Select the required user and device.

   The **Workspace Details** for the device appears.

© 2019 Pulse Secure, LLC.

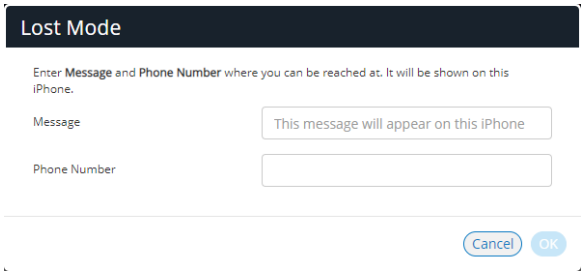
5. In the **Actions** pull-down menu for the device, select **Lost Mode**:

FIGURE 217 iOS Device Actions Lost Mode



The **Lost Mode** dialog appears:

FIGURE 218 Lost Mode



6. Enter a **Message** and a **Phone Number** to be displayed on the lost device, and click **OK**.

   A confirmation message appears.

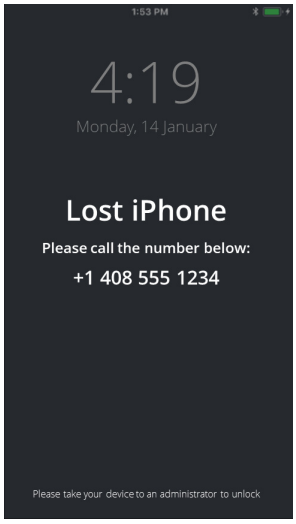
7. Confirm the confirmation message.

   The device enters Lost Mode.

© 2019 Pulse Secure, LLC.

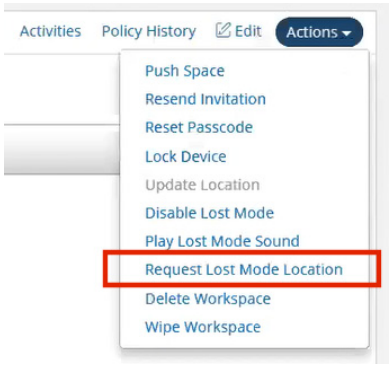
The lost device becomes locked, and displays the **Message** and **Phone Number**. For example:

FIGURE 219 Lost iPhone Message



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 220 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**.

© 2019 Pulse Secure, LLC.

Viewing Analytics

- Viewing the Login Attempts Report 183
- Viewing the Appliance Health Report 184
- Viewing the Appliance Activities Report 185
- Viewing the App Visibility Report 186
- Viewing Log Aggregation and Analysis 187

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 221 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.

© 2019 Pulse Secure, LLC.

Viewing the Appliance Health Report

To view the **Appliance Health** report:

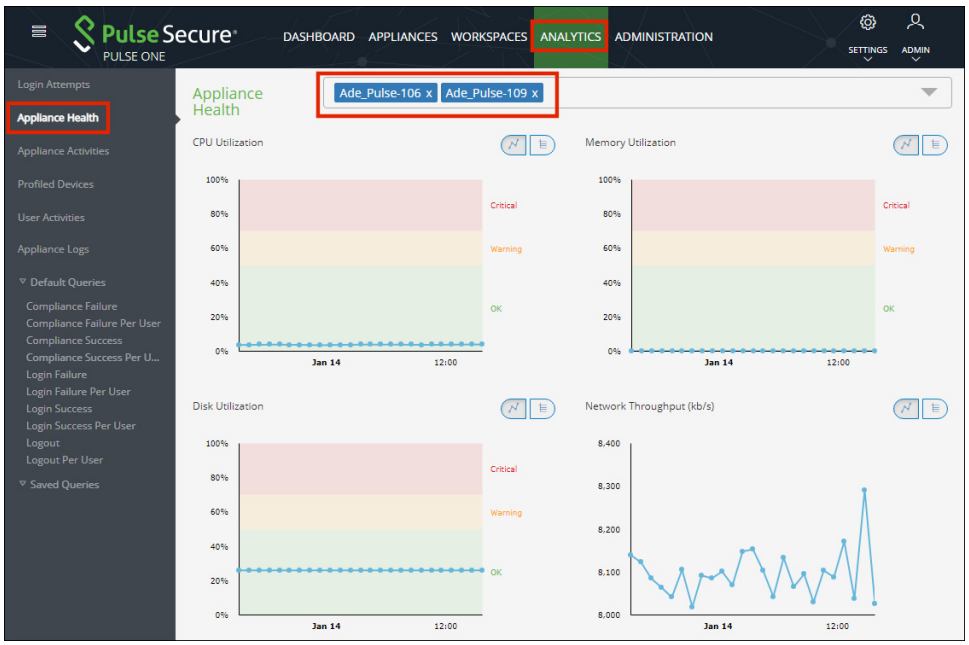
1. Select the **Analytics** menu.
2. Select **Appliance Health**.
3. From the **Appliance Health** drop-down, select one or more appliances for the report.

   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 222 Appliance Health Report



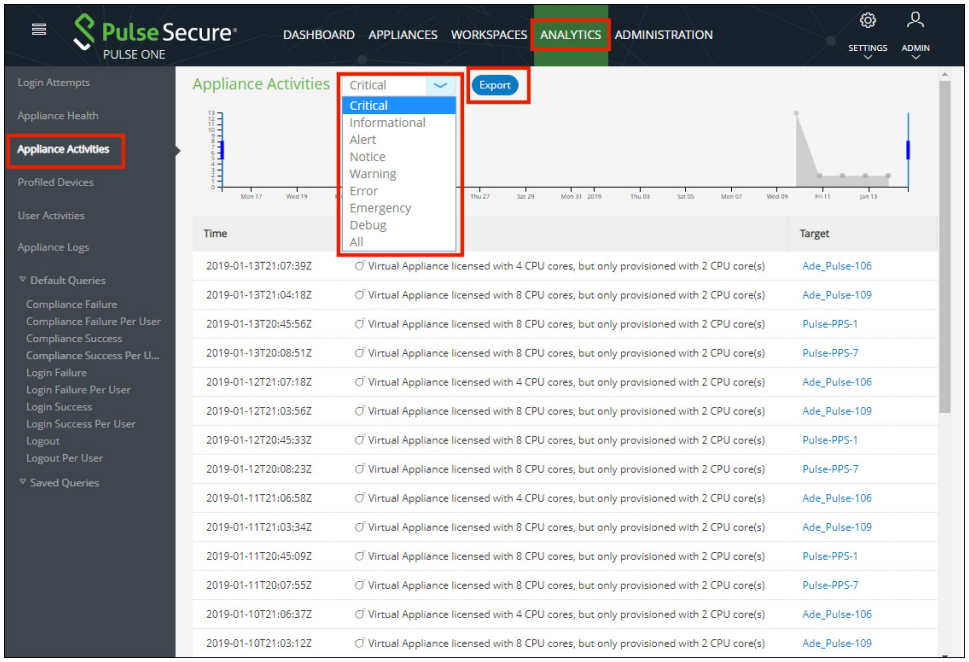
© 2019 Pulse Secure, LLC.

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 223 Appliance Activities



4. (Optional) Click **Export** to download displayed information as a *.csv* format file.

Viewing the App Visibility Report

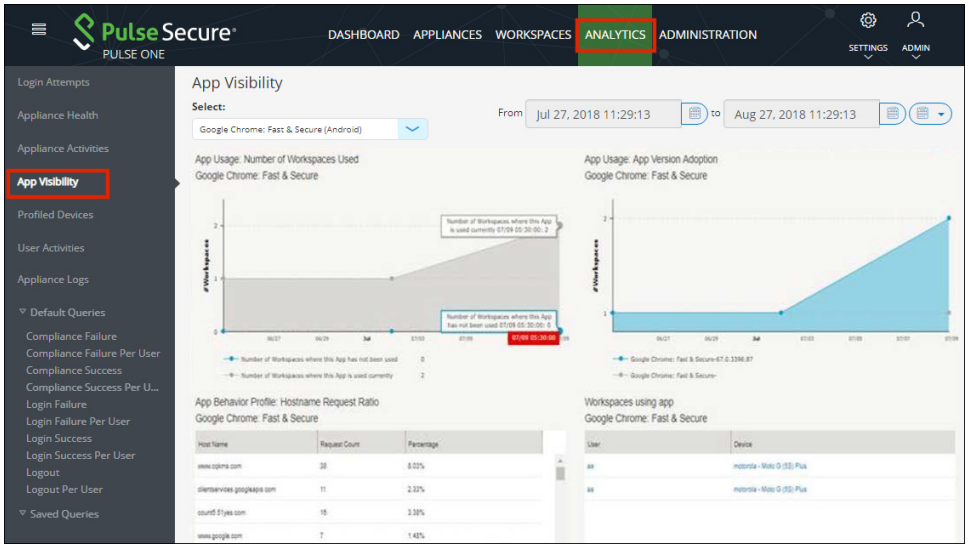
To view the **App Visibility** report:

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 224 App Visibility Report

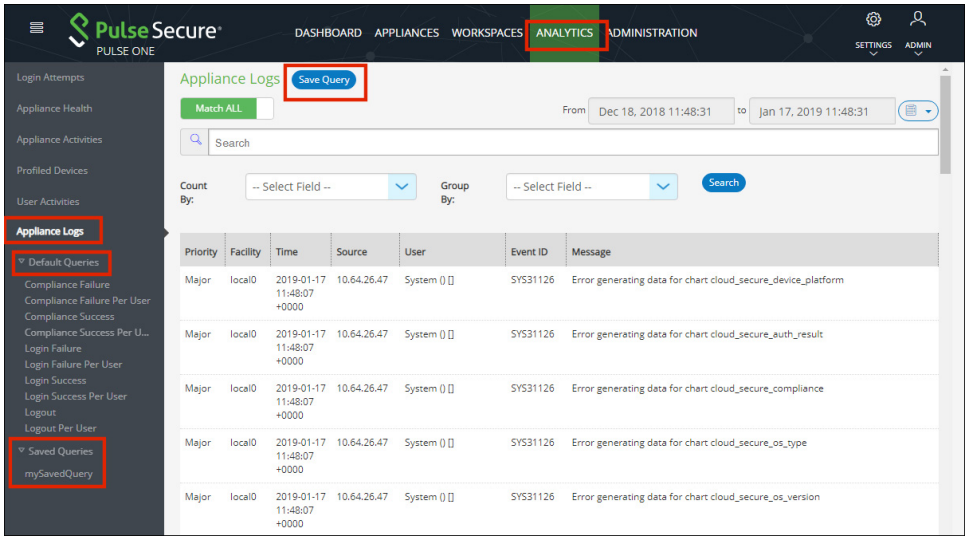


© 2019 Pulse Secure, LLC.

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.

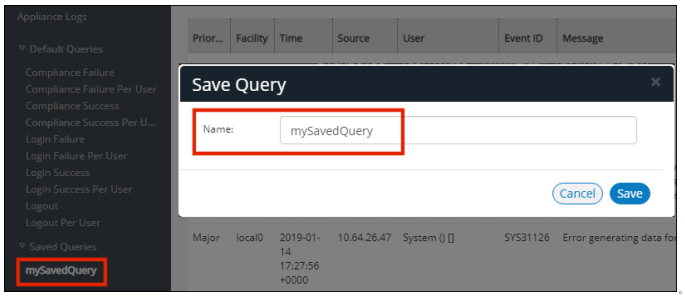
FIGURE 225 Appliance Logs



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 226 Save Query



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.

© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

User Administration

- Adding an Admin User 189
- Modifying User Details 190
- Removing an Admin User 190
- Resetting a User Password 191
- Suspending a User. 192

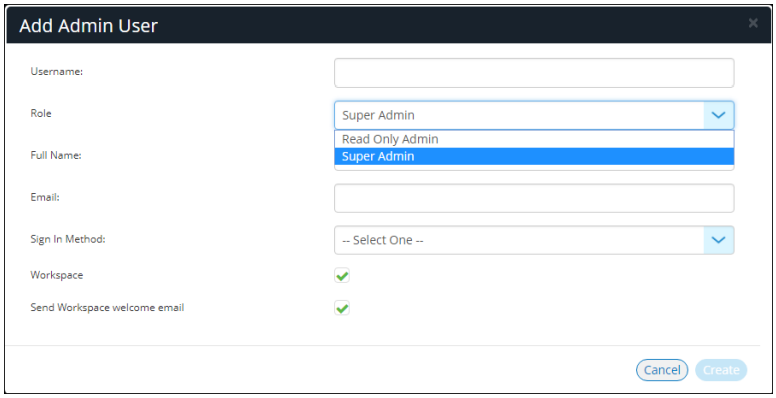
Adding an Admin User

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 227 Add Admin User



Note: If Role is set to **Read Only Admin**, then the user will not be given the permissions to create/update/delete functions.

© 2019 Pulse Secure, LLC.

Modifying User Details

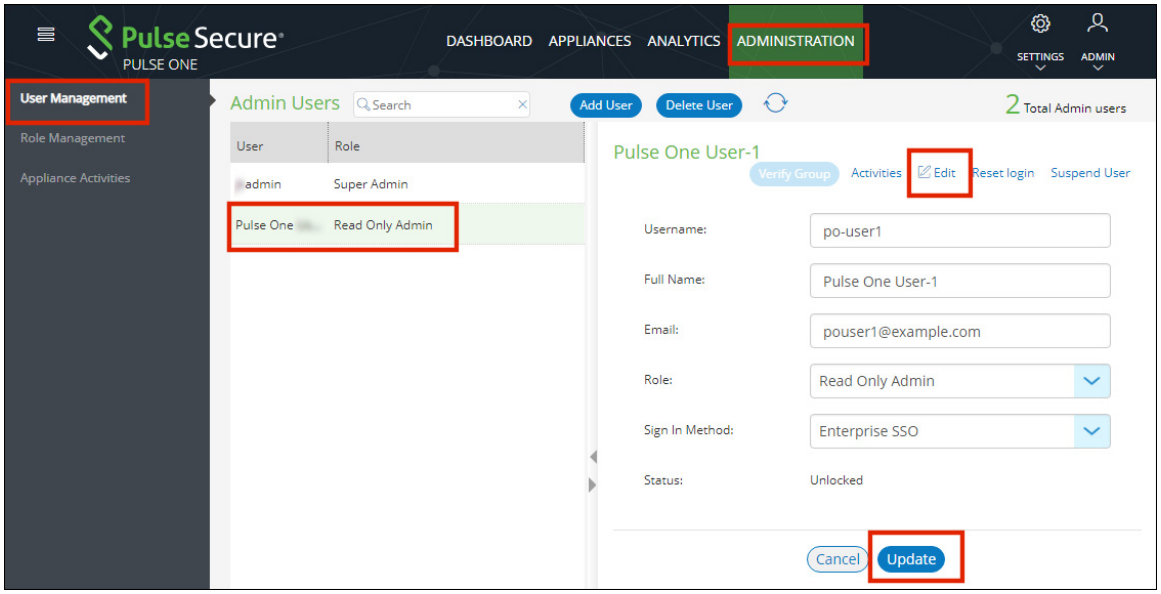
To modify an admin user's details:

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 228 Edit User Details



Removing an Admin User

To remove an admin user:

1. Select the **Administration** menu.
2. Select **User Management**.

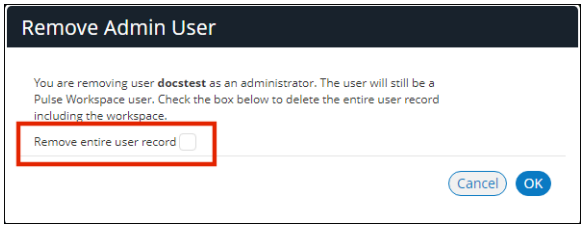
   A list of existing admin users is displayed.
3. Select the user from the list and click **Delete User**.

   The **Remove Admin User** dialog appears. By default, this dialog will enable you to remove a user from the list of admin users.

© 2019 Pulse Secure, LLC.

4. (Optional) In order to remove the user from Pulse Workspace completely, select the **Remove entire user record** check box.

   FIGURE 229 Remove Admin User



5. Click **OK.**

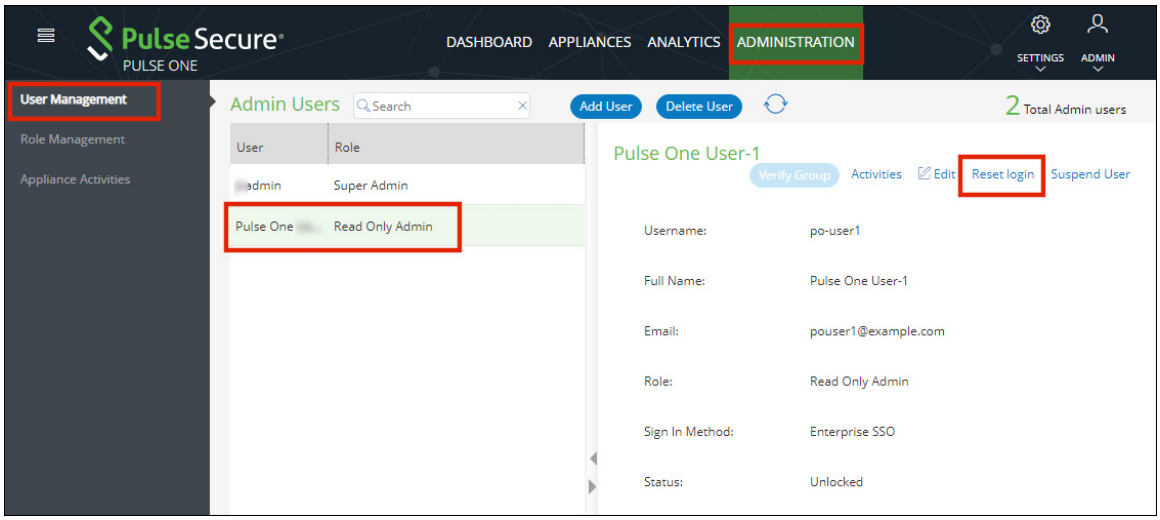
Resetting a User Password

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 230 Reset Login



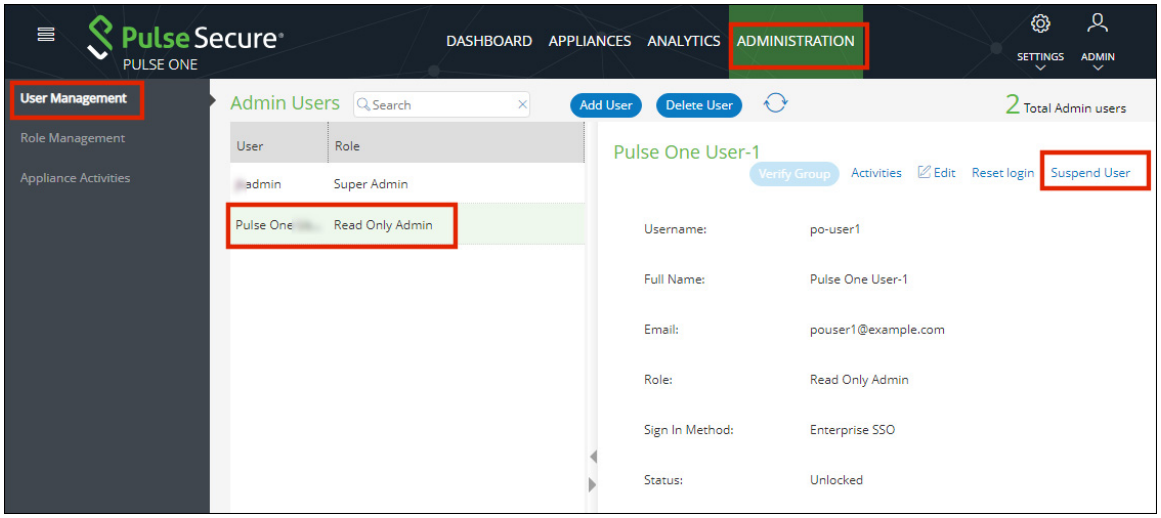
© 2019 Pulse Secure, LLC.

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 231 Suspend User



© 2019 Pulse Secure, LLC.

Role Management

- Adding Admin-Defined Roles. 193
- Modifying Admin-Defined Roles 196
- Removing Admin-Defined Roles 196
- Managing Pulse One Properties 197

Adding Admin-Defined Roles

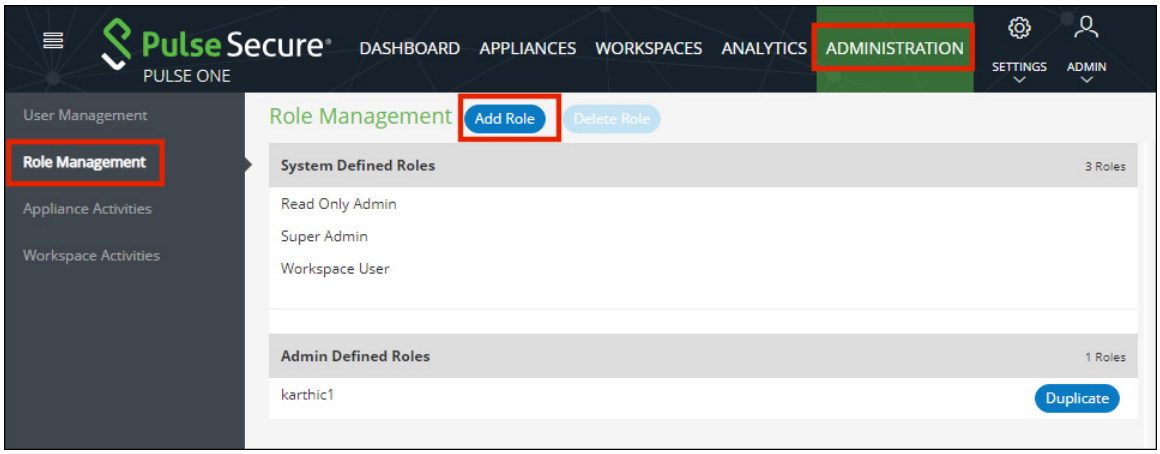
An admin-defined role can be created manually, or by duplicating an existing role.

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.

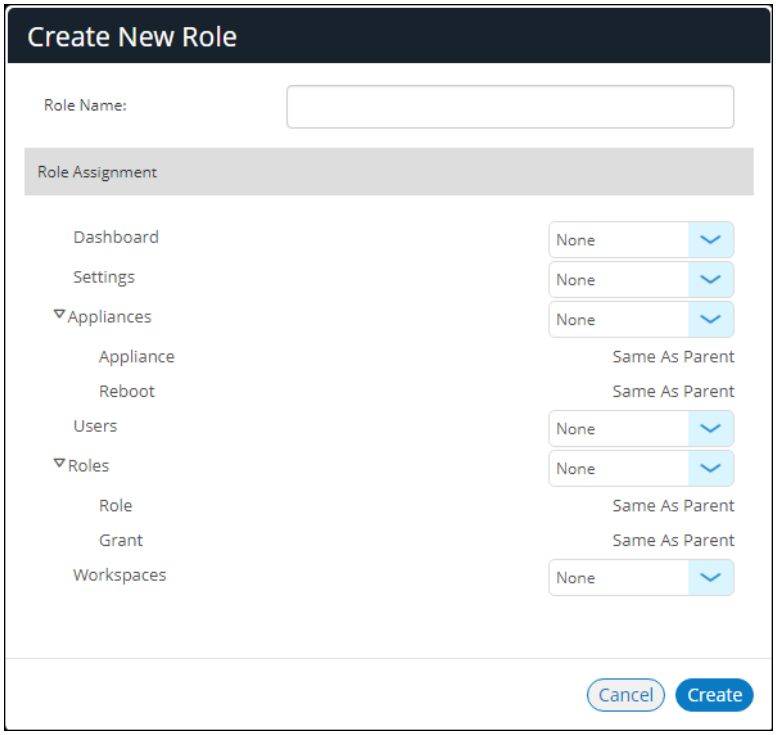
   FIGURE 232 Add Role



© 2019 Pulse Secure, LLC.

The **Create New Role** dialog appears.

FIGURE 233 Create New Role



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:

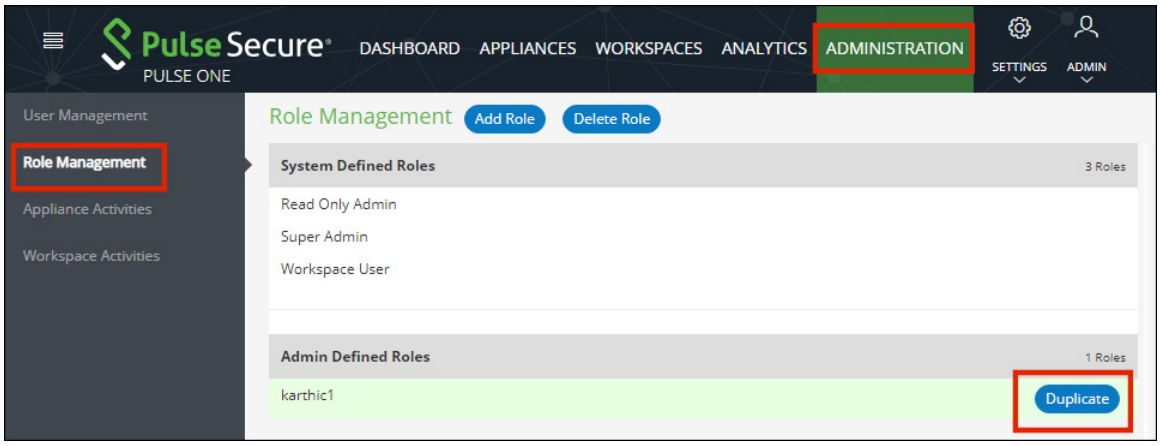
1. Select the **Administration** menu.
2. Select **Role Management**.

   A list of system defined roles appears.

© 2019 Pulse Secure, LLC.

3. Click **Add Role** to add a new admin defined role.
4. Click **Duplicate Role** to add a new admin defined role.

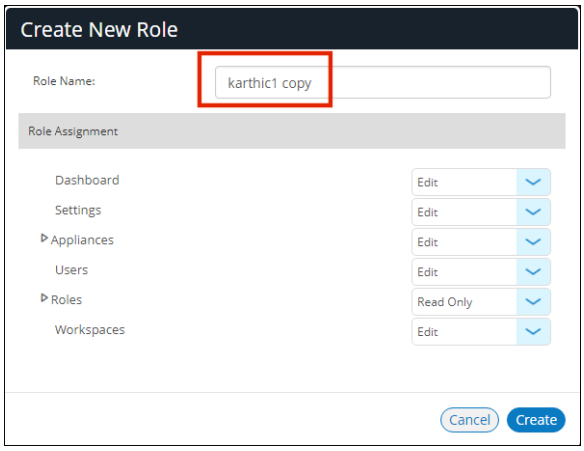
FIGURE 234 Duplicate a Role



The **Create New Role** dialog appears. In this dialog:

- A duplicate name is used.
- All permissions match the original admin role.

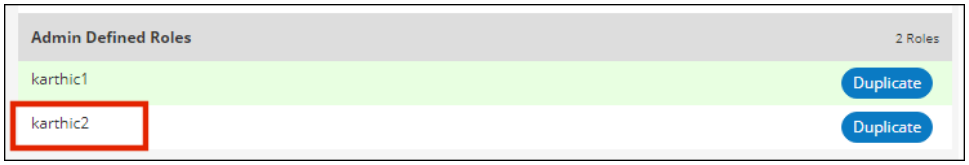
FIGURE 235 Create Duplicate Role



5. Make any required changes and click **Create**.

The duplicated admin role is added to the list of admin roles.

FIGURE 236 Duplicated Role



© 2019 Pulse Secure, LLC.

Modifying Admin-Defined Roles

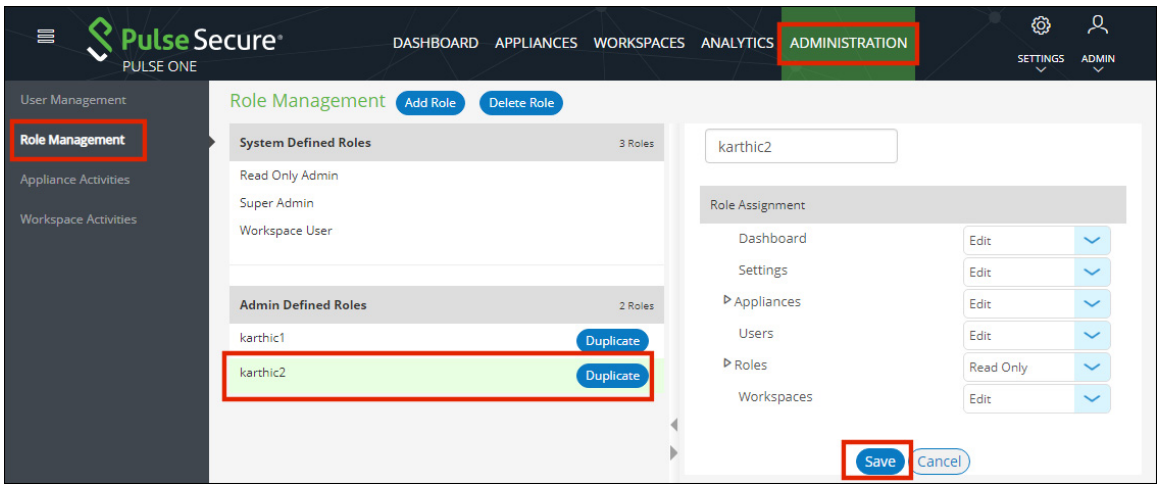
You can modify only the admin defined roles.

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 237 Modify Role



Removing Admin-Defined Roles

You can remove only the admin defined roles.

To remove an admin defined role:

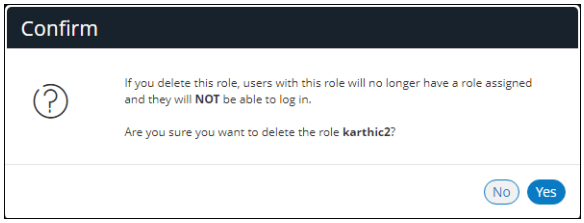
1. Select the **Administration** menu.
2. Select **Role Management**.

   A list of system defined roles appears.
3. Select the role from the list and click **Delete Role**.

© 2019 Pulse Secure, LLC.

4. In the Confirmation message box, click **Yes** to remove the selected role.

FIGURE 238 Confirm Delete Role



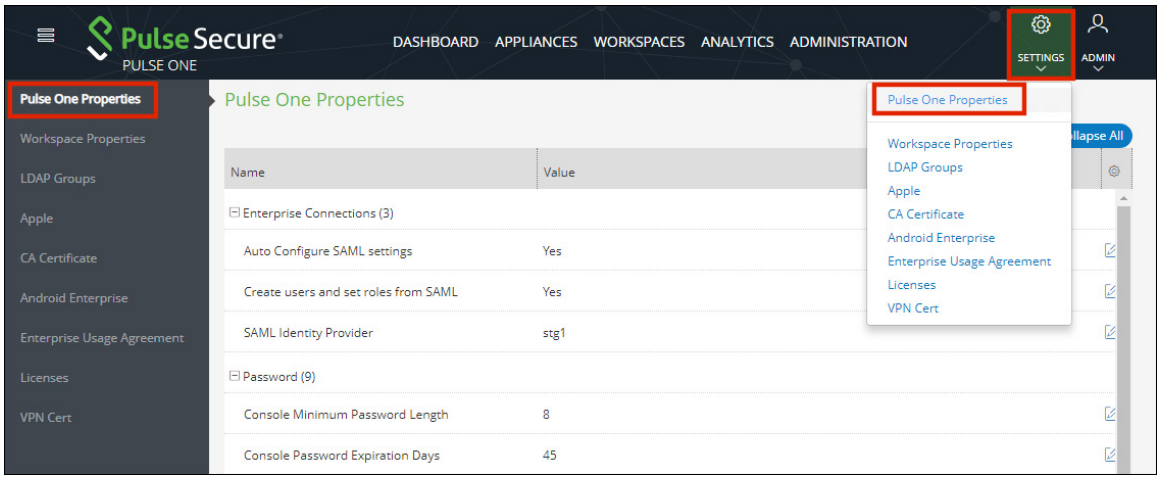
Managing Pulse One Properties

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.

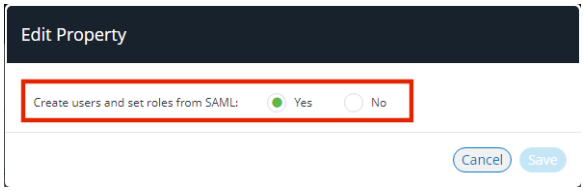
FIGURE 239 Pulse One Properties



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 240 Edit Property



© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

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.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Working with the MSSP Management Console

- Introduction 201
- Preparing to Provision an MSSP Management Console 201
- Creating an MSSP Management Console 202
- Accessing the MSSP Management Console. 203
- Managing Users of the MSSP Management Console 204
- Managing Customer Domains on the MSSP Management Console 208
- Accessing a Customer Domain 220

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 210**.

© 2019 Pulse Secure, LLC.

- 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 201**.
- 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.

© 2019 Pulse Secure, LLC.

- 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

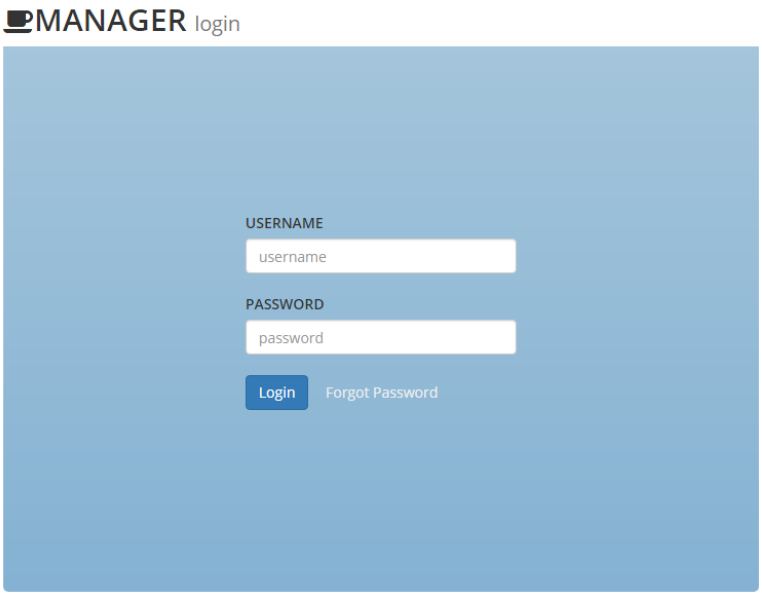
To access the MSSP management console:

1. Open a browser and enter the URL for the management console. For example:

   demo.customer.com

   The login page appears. For example:

   FIGURE 241 MSSP Management Console Login



2. Log in using the administration user declared when the MSSP management console was provisioned. For example:

   admin123

© 2019 Pulse Secure, LLC.

The default home page (Domains) appears:

FIGURE 242 MSSP Management Console Home Page

From this page, you can:

- (Optional) Create additional users to the MSSP management console, see **"Managing Users of the MSSP Management Console" on page 204**.
- Create customer domains, see **"Managing Customer Domains on the MSSP Management Console" on page 208**.

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 204**.
- **"Editing an MSSP Management Console User" on page 206**.
- **"Deleting an MSSP Management Console User" on page 207**.

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 220**.

To add a user to the MSSP management console:

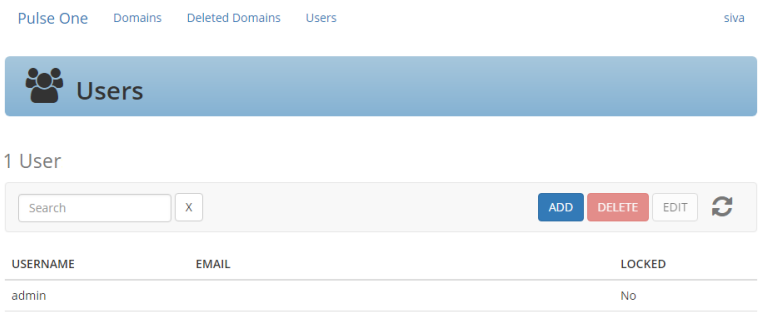
1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
2. Click the **Users** tab.

   The **Users** page appears.

   Note: When the MSSP management console is started for the first time, only the defined administrator user is present.

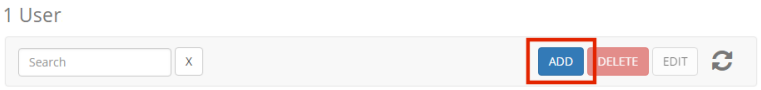
© 2019 Pulse Secure, LLC.

FIGURE 243 Users Page



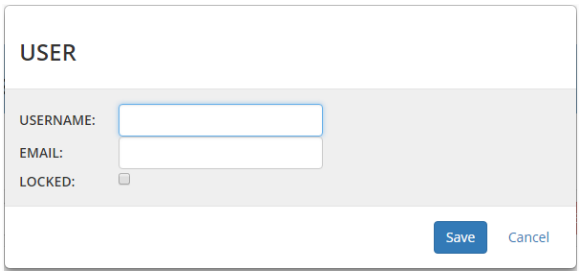
3. Above the table of users, click **Add**.

FIGURE 244 Adding a User



The **User** dialog appears.

FIGURE 245 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 206**.

7. Click **Save**.

   The new user is added to the **Users** page. For example:

   FIGURE 246 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.

© 2019 Pulse Secure, LLC.

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 203**.
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 247 Edit a User

   The **User** dialog appears.

   FIGURE 248 Edit User

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 207**.
5. Click **Save**.
6. The table of users on the **Users** page updates.

© 2019 Pulse Secure, LLC.

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.

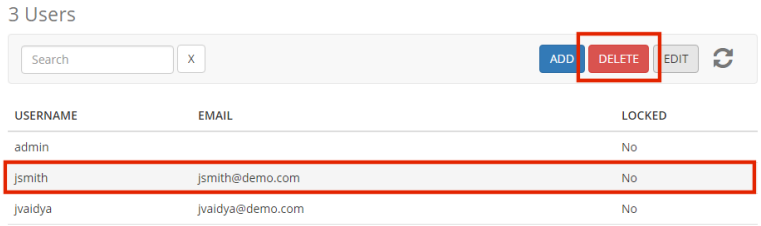
Note: If you want to temporarily prevent a user from accessing the console, you can edit the user to lock the account, see **"Editing an MSSP Management Console User" on page 206**.

To delete a user:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
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 249 Delete User

   A confirmation dialog appears.
4. Click **OK** to confirm the deletion.

   The user is removed from the table of users.

© 2019 Pulse Secure, LLC.

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 208.
- "Licensing a Customer Domain" on page 210.
- "Adding an Email Domain to a Customer Domain" on page 215.
- "Editing a Customer Domain" on page 216.
- "Managing Customer Domains" on page 217.

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 203.
2. Click the **Domains** tab.

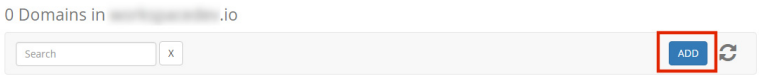
   The **Domains** page appears.

   FIGURE 250 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**.

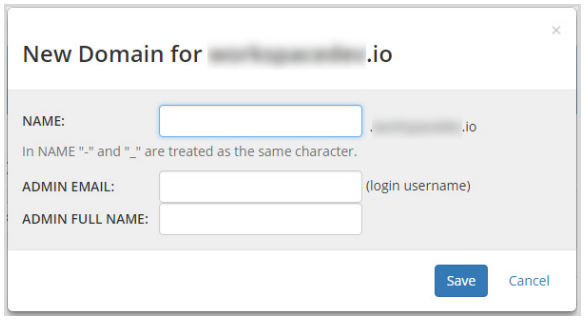
   FIGURE 251 Add Customer Domain

© 2019 Pulse Secure, LLC.

The **Domain** dialog appears.

FIGURE 252 New Domain Dialog



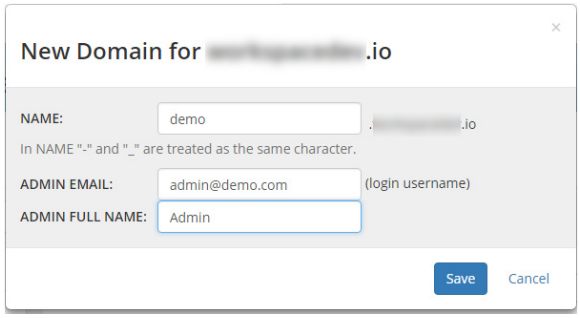
4. Enter a **Name** for the domain. This will be used in the URL for the domain.

   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 253 New Domain Dialog

   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**.

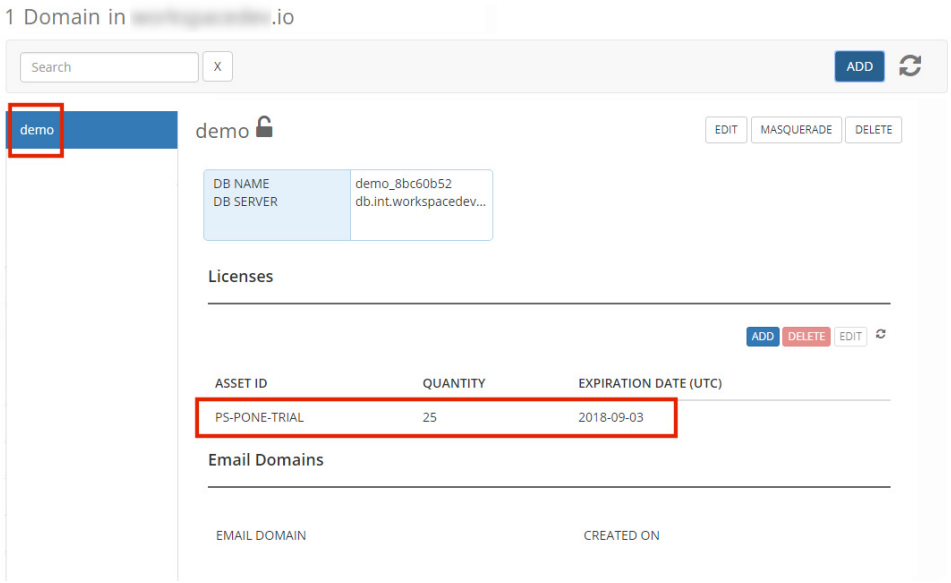
   The new domain is added to the **Domains** page.

   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.

© 2019 Pulse Secure, LLC.

When this domain is accessed for the first time, a *PS-ONE-TRIAL license* is applied automatically. For example:

FIGURE 254 Domains Page Addition



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 210**.

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 211**.
- **"Adding Customer Domain Licenses" on page 211**.
- **"Editing a License for a Customer Domain" on page 214**.
- **"Deleting a License from a Customer Domain" on page 214**.

© 2019 Pulse Secure, LLC.

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:

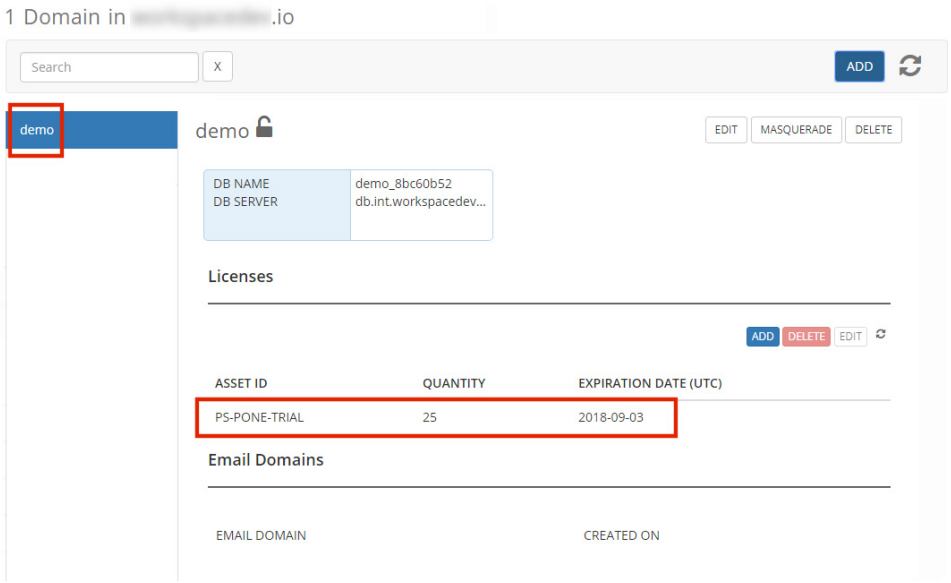
1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
2. Click the **Domains** tab.

   The **Domains** page appears.
3. Select the required customer domain.

© 2019 Pulse Secure, LLC.

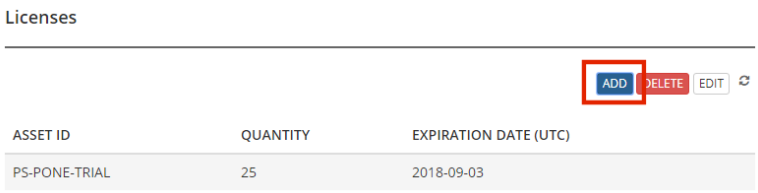
The **Domains** page updates to show details of the selection, including any default trial license that are in place. For example:

FIGURE 255 Customer Domain Trial License



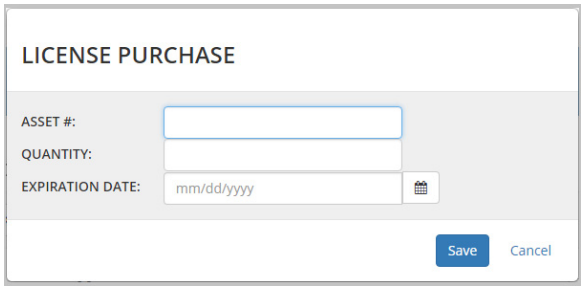
4. Above the table of licenses, click **Add**.

FIGURE 256 Add Customer Domain License



The **License** dialog appears.

FIGURE 257 License Purchase



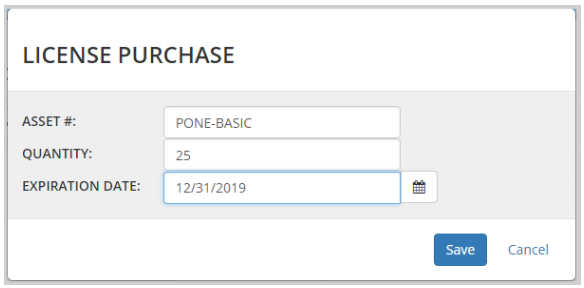
5. Enter the required license type as the **Asset #**. For example: *PONE-BASIC* or *PWS-TRIAL*.
6. Enter the required **Quantity** of this license.

© 2019 Pulse Secure, LLC.

7. Enter the required **Expiration Date** for this license.

   For example:

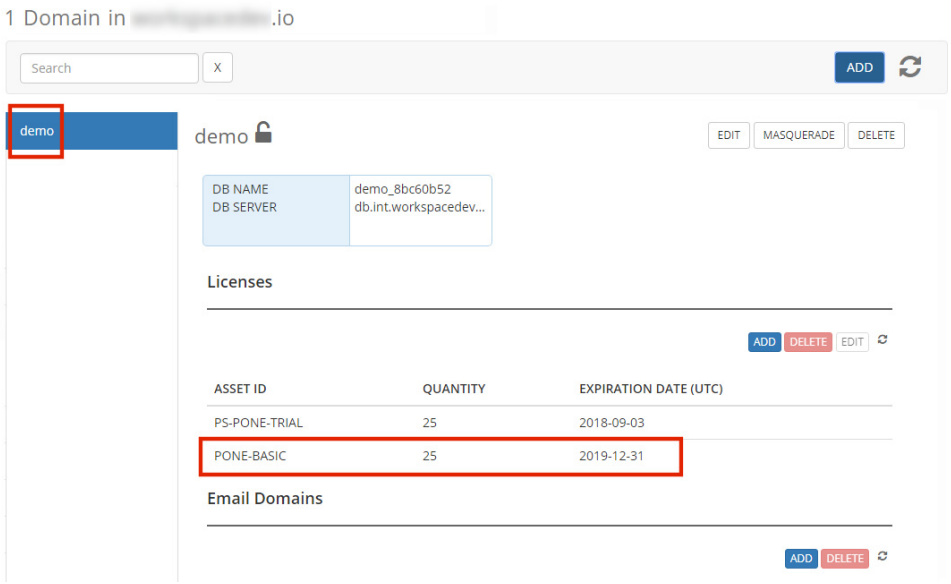
   FIGURE 258 Required License Details



8. Click **Save**.

   The license is added to the customer domain details.

   FIGURE 259 License Added



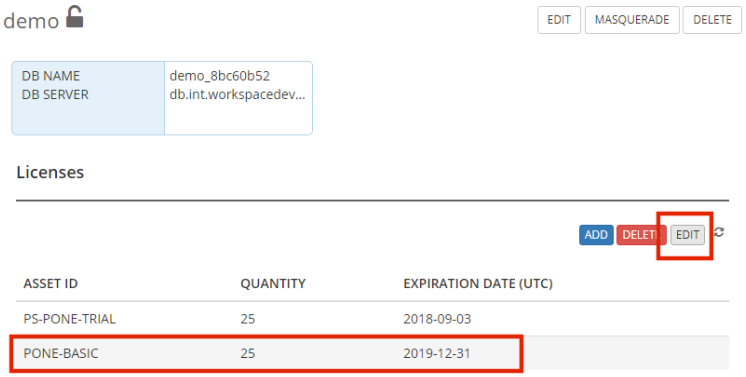
© 2019 Pulse Secure, LLC.

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 260 Edit a License



   The **License Purchase** dialog appears.

3. Update the required details for the license.
4. Click **Save**.

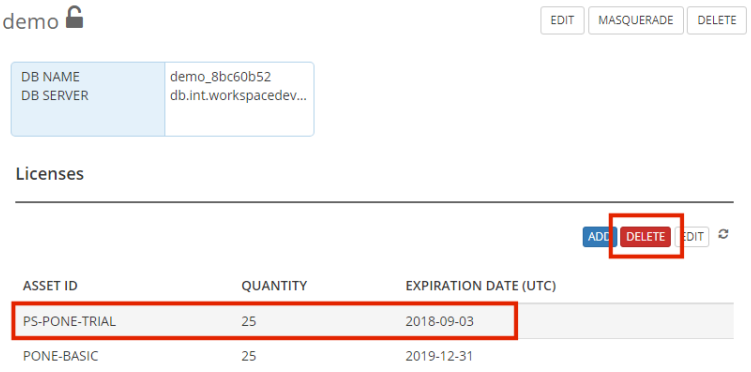
   The license details are updated.

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 261 Delete a License



   A confirmation dialog appears.

© 2019 Pulse Secure, LLC.

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.

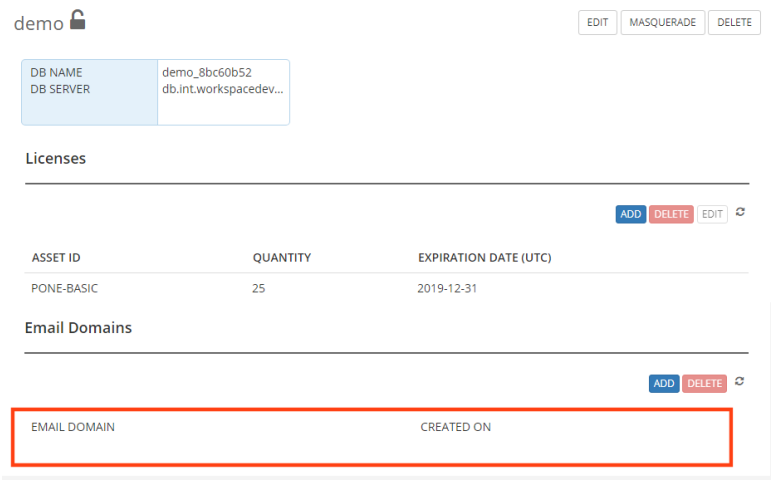
To add an email domain to a customer domain:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
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 262 Customer Domain



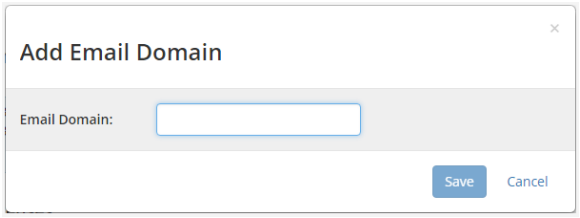
   In this example, there is no defined email domain for the demo customer domain.
4. Above the (initially empty) table of email domains, click **Add**.

   FIGURE 263 Add Email Domain

© 2019 Pulse Secure, LLC.

The **Email** dialog appears.

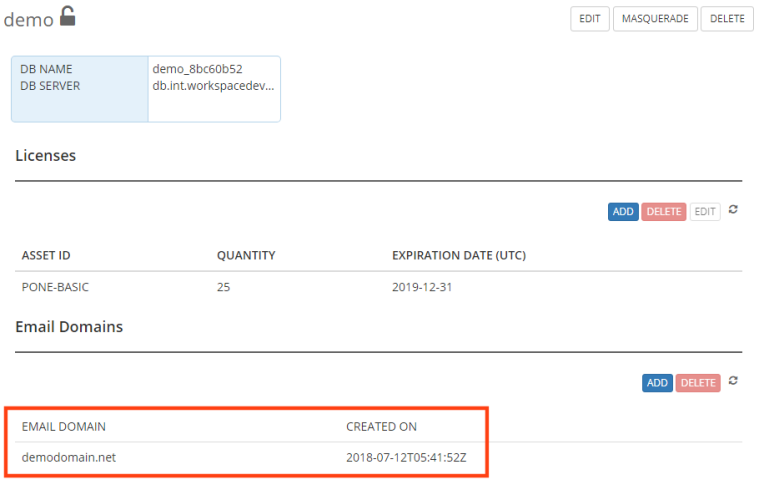
FIGURE 264 Add Email Domain Dialog



5. Enter the required **Email Domain**. For example: *demodomain.net*.
6. Click **Save**.

   The email domain is added to the customer domain details.

FIGURE 265 Email Domain Added



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 203**.
2. Click the **Domains** tab.

   The **Domains** page appears.
3. In the table of domains, select the required customer domain.

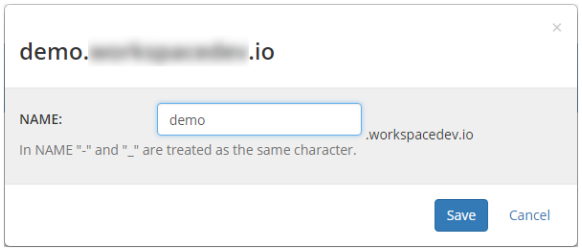
© 2019 Pulse Secure, LLC.

4. Above the table, click **Edit**.

FIGURE 266 Edit a Customer Domain

A customer domain dialog appears. For example:

FIGURE 267 Customer Domain



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 217.
- "Viewing Deleted Customer Domains" on page 218.
- "Recovering a Deleted Customer Domain" on page 219.

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 218.

You can log into a deleted customer domain if required.

© 2019 Pulse Secure, LLC.

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 219**.

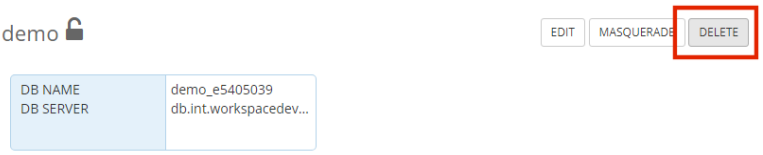
After the retention period, the deleted customer domain and all configuration and data is permanently deleted automatically.

To delete a customer domain:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
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 268 Delete a Customer Domain

   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 218**.

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.

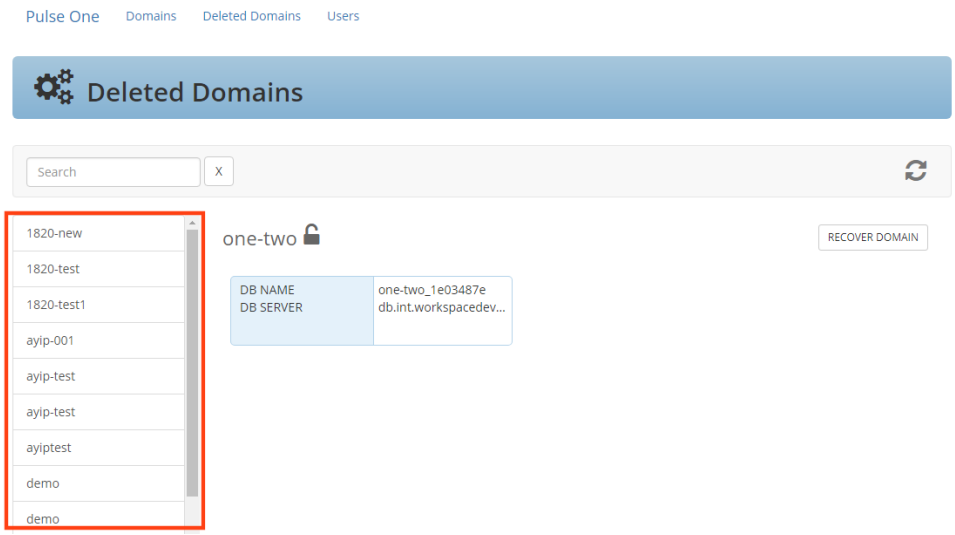
To view deleted customer domains:

1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
2. Click the **Deleted Domains** tab.

© 2019 Pulse Secure, LLC.

The **Deleted Domains** page appears. This includes a list of customer domains that have been deleted during the last 30 days.

FIGURE 269 Deleted Domains



You can recover a listed deleted customer domain if required, see **"Recovering a Deleted Customer Domain" on page 219**.

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:

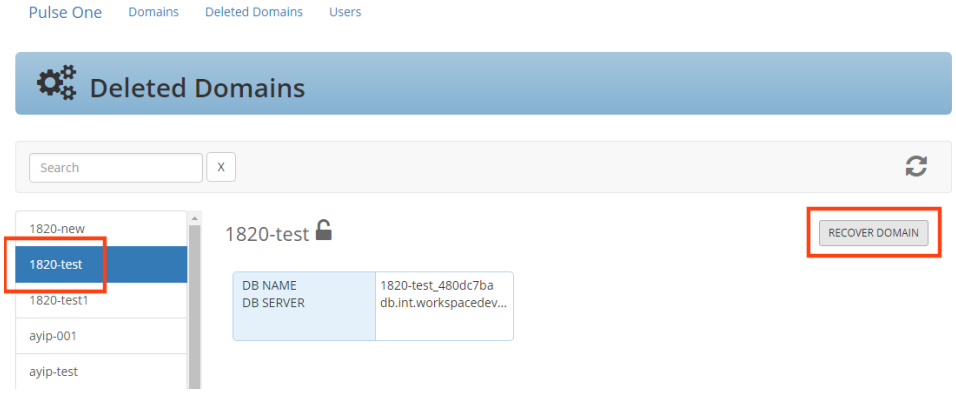
1. Log into the MSSP management console as an administrator, see **"Accessing the MSSP Management Console" on page 203**.
2. Click the **Deleted Domains** tab.

   The **Deleted Domains** page appears.
3. In the table of deleted domains, select the customer domain that you want to recover.

© 2019 Pulse Secure, LLC.

4. Above the table, click **Recover Domain**.

   FIGURE 270 Recover a Deleted Customer Domain



   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 220**.

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.

© 2019 Pulse Secure, LLC.