Contents

1 Introduction to the VMware Pulse IoT Center Mobile Application 4
   Mobile OS Support 4
   User and Password Requirements 5
   Terminology 5

2 Installing the VMware IoT Center Mobile Application 7
   Set Up the Mobile Application on an iOS Device 7
   Set Up the Mobile Application on an Android Device 8

3 Using the VMware Pulse IoT Center Mobile Application 9
   Log In to VMware Pulse IoT Center Mobile Application 9
   Whitelist or Unwhitelist a Device 10
   Enroll a Whitelisted Device 11
Introduction to the VMware Pulse IoT Center Mobile Application

The VMware Pulse IoT Center onboards, configures, manages, monitors, and secures unmanned IoT devices and objects at scale.

You can use this solution to:

- Pre-register and bulk onboard IoT devices.
- Manage alerts and notifications.
- Troubleshoot the devices.
- Change the configuration of devices.
- View audit logs.
- Perform compliance management operations through over the air updates.

The VMware Pulse IoT Center Mobile application provides the capability to whitelist any gateway that is enabled to be whitelisted in the VMware Pulse IoT Center. To use this mobile application, you must be a registered user of the VMware Pulse IoT Center 2.0.

For information about how VMware handles information collected through the VMware Pulse IoT Center Mobile application, go to https://www.vmware.com/help/privacy.html

This chapter includes the following topics:

- Mobile OS Support
- User and Password Requirements
- Terminology

Mobile OS Support

The VMware Pulse IoT Center Mobile application supports the following Android and iOS versions:

Table 1-1. Supported Mobile OS Platforms and Versions

<table>
<thead>
<tr>
<th>Mobile OS</th>
<th>Minimum Version</th>
<th>Maximum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Jelly Bean (API 16)</td>
<td>Pie (API 28) - Latest</td>
</tr>
<tr>
<td>iOS</td>
<td>iOS 11.0</td>
<td>iOS 12.14 - Latest</td>
</tr>
</tbody>
</table>
User and Password Requirements

The users of the VMware Pulse IoT Center Mobile application must be the registered users of VMware Pulse IoT Center.

To add a new user, contact your VMware Pulse IoT Center system administrator. To know about the password policy for the VMware Pulse IoT Center Mobile application, see Password Requirements in *VMware Pulse IoT Center User Guide*.

Terminology

This section provides the information about the terminology that is frequently used in this guide.

**Gateway**

A gateway is a physical device that serves as a connection point between the cloud (public or on premises) and controllers, sensors, and intelligent devices. All data moving to and from the cloud goes through the gateway. The VMware Pulse IoT Center IoTC Agent runs and collects information on behalf of other connected Thing devices through the gateway.

**Connected Device or Thing Device**

A connected device or a Thing device is a nonstandard computing device that can transmit data and is connected to a gateway. The Thing device connects to a gateway and sends information to the VMware Pulse IoT Center through the VMware Pulse SDK client that is running on the gateway.

**Registered Device**

A registered device is a virtual gateway that is created on the VMware Pulse IoT Center. A registered device does not have a physical gateway associated with it.

**Whitelisted Device**

A whitelisted device is a virtual gateway that is created on the VMware Pulse IoT Center. A registered device having permission to enroll is a whitelisted device. A whitelisted device does not have a physical gateway associated with it yet. You can whitelist or unwhitelist a device to control whether it is permitted to enroll or not.

**Unwhitelisted Device**

An unwhitelisted device is a virtual gateway that is created on the VMware Pulse IoT Center. This device is already registered but not whitelisted.

**Enrolled Device**

An enrolled device is a registered gateway or a device with a physical gateway associated with it.
Unenrolled Device

An unenrolled device is a device or a virtual gateway which is not registered and enrolled.
Installing the VMware IoT Center Mobile Application

If you have an Android device, you can install the VMware Pulse IoT Center Mobile application from the Google Play Store. If you have an iOS device, you can install the VMware Pulse IoT Center Mobile application from the App store.

For information about mobile OS requirements, see Table 1-1. Supported Mobile OS Platforms and Versions

This chapter includes the following topics:

- Set Up the Mobile Application on an iOS Device
- Set Up the Mobile Application on an Android Device

Set Up the Mobile Application on an iOS Device

Install the security certificate by following the instructions for the iOS application:

**Prerequisites**

Download the security certificate file on your iOS mobile device. Use only Safari browser for downloading and installing the certificate. Other browsers are not supported and display an error message.

**Note** These steps are only for on-premises VMware Pulse IoT Center. For SaaS, you can skip these steps.

**Procedure**

1. Install the mobile application from the App store.
2. To get the necessary certificate, contact the VMware Pulse IoT Center administrator.
3. On your mobile device, click the downloaded file and tap **Install**.

   **Note** iOS displays a warning message that installing the profile changes the settings on your iPhone.

4. Tap **Install Now**.
   After the installation is complete, a certificate screen is displayed.
5. Tap **Done** in the top right corner to exit from the screen.
6 Open the **Settings App**, open **Settings > General > About > Certificate Trust Settings** to enable the SSL trust.

7 Tap **toggle** next to the installed certificate.

8 Tap **Continue** and **Finish**.

You have successfully installed the mobile application and security certificate on your iOS device.

**Set Up the Mobile Application on an Android Device**

Install the security certificate and mobile application on the Android device.

**Prerequisites**

Download the certificate on your Android device. To get the necessary certificate, contact the VMware Pulse IoT Center administrator.

**Note** These steps are generic for an Android device. It can vary from device to device.

**Procedure**

1 Install the mobile application from the Google play store.

2 On your mobile device, go to the **Settings app**.

3 Select **Security**.

4 Select **Install from Storage**.

5 Select the certificate file from your local repository and install.

You have successfully installed mobile application on your Android device.
Using the VMware Pulse IoT Center Mobile Application

The VMware Pulse IoT Center Mobile application allows you to whitelist and un-whitelist a device.

This chapter includes the following topics:

- Log In to VMware Pulse IoT Center Mobile Application
- Whitelist or Unwhitelist a Device
- Enroll a Whitelisted Device

Log In to VMware Pulse IoT Center Mobile Application

The VMware Pulse IoT Center Mobile application allows you to whitelist and unwhitelist a gateway or a device. The mobile application whitelists a gateway which enables the gateway to enroll automatically once whitelisted. It also unwhitelists a gateway which does not allow the gateways to get enrolled or onboarded.

Prerequisites

- A valid VMware Pulse IoT Center URL and credentials to log in.
- If you do not have a VMware Pulse IoT Center URL, user name or password, contact your VMware Pulse IoT Center system administrator.
- If self-signed certificates are used for the VMware Pulse IoT Center on-prem deployment, obtain the CA certificate from the VMware Pulse IoT Center administrator.

Procedure

1. On your mobile device, log in to VMware Pulse IoT Center. Enter the VMware Pulse IoT Center URL, user name, and password.

2. Tap Sign in.

   The VMware Pulse IoT Center Mobile application displays a dashboard with the total devices, number of devices that are whitelisted, enrolled, registered, and unenrolled.
Note: After logging in, if a user wants to change the password, contact the VMware Pulse IoT Center administrator.

3 Tap **Scan** to scan and whitelist a device.

**Whitelist or Unwhitelist a Device**

A whitelisted device is a virtual gateway that is registered but not enrolled and does not have a physical gateway associated with it.

To whitelist a device, you must scan the QR code on the VMware Pulse IoT Center Mobile application.

**Prerequisites**

- A valid VMware Pulse IoT Center URL and credentials to log in.
- The device should be registered in the VMware Pulse IoT Center administrator.
- The QR code value is already added to the device property `qr-code` in the VMware Pulse IoT Center.

**Procedure**

1 Open the VMware Pulse IoT Center Mobile application on your device.
2 Log in to the VMware Pulse IoT Center Mobile application and tap **Scan**.

When you open the application for the first time, a pop-up window requesting permissions to access the camera is displayed.

3 Tap **OK**.

4 Tap **OK**.

5 Scan the QR code on the gateway.

Once the QR code is scanned, gateway details such as gateway name and the status are displayed.

6 Tap **Whitelist the device** to whitelist the gateway.

Your device is whitelisted. When you scan the same device again, it shows that the device is whitelisted.

7 On the confirmation window, if you want to whitelist another device, click **Yes** and scan the QR code.

The whitelisted device details are displayed.

8 Tap **Un-Whitelist Device** to unwhitelist a device.

**Note** Scanning a device that is already enrolled displays an error that the device is already enrolled and cannot be whitelisted.

**Enroll a Whitelisted Device**

A device or a gateway is enrolled when a physical gateway is associated with it. A whitelisted device is enrolled automatically. For information about enrolling whitelisted devices, see the *VMware Pulse IoT Center User Guide*.