You can find the most up-to-date technical documentation on the VMware website at: https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to docfeedback@vmware.com
Contents

1 Introduction ............................................................................................................................................. 5
  1.1. Browser Support ............................................................................................................................. 5
  1.2. Terminology ...................................................................................................................................... 6
  1.3. Administrators ................................................................................................................................. 6

2 Workflows .............................................................................................................................................. 8
  2.1 System Administrator Workflow ...................................................................................................... 8
  2.2 Pulse Administrator Workflow ......................................................................................................... 15
  2.2.1 User Management ......................................................................................................................... 16
  2.2.2 Client Package Configuration ....................................................................................................... 19
  2.3 Alert Administrator Workflow .......................................................................................................... 19
  2.3.1 Monitoring the Health of the IoT Infrastructure ............................................................................. 20
  2.3.2 Triage Specific Resources ............................................................................................................ 22
  2.4 Console Administrator Workflow .................................................................................................... 23
  2.4.1 Defining Alerts and Notifications ............................................................................................... 23
  2.4.2 Product Dashboard ....................................................................................................................... 27
  2.4.3 Device Group Management .......................................................................................................... 27
  2.4.4 Product Creation and Assignment ............................................................................................... 28
  2.5 Gateway Installation Administrator (Technician) ............................................................................ 34

3 Device Offline Alert .................................................................................................................................. 35
  3.1 Requirement of Device Offline .......................................................................................................... 35
  3.2 Understanding When the Device (Gateway/Sensors) Goes Offline .................................................... 35
  3.3 Creation of an Offline Alert ............................................................................................................... 35
  3.4 Generation of an Offline Alert .......................................................................................................... 36

4 Pulse IoT Center Client OTA Provisioning on Dell Gateways with Ubuntu Core 16 ......................... 37
  4.1 Prerequisites ...................................................................................................................................... 37
  4.2 OTA Provisioning Through the Pulse AirWatch Console .................................................................. 37

5 Pulse IoT Center Client SNAP Management on Dell Gateways with Ubuntu Core 16 ................. 39
  5.1 Snap Management ............................................................................................................................. 39
  5.2 Prerequisites ...................................................................................................................................... 39
  5.3 SNAP Management Using Product Provisioning through the Pulse AirWatch Console .............. 39
5.3.1 Supported Snap Management Commands ................................................................. 41

6 Pulse Client Upgrade through Product Provisioning Using the AirWatch Console .......... 45
  6.1 Prerequisites ............................................................................................................. 45
  6.2 Generating a Staging Package using the APF File ................................................... 45
  6.3 Upgrading the Pulse Client Snap Through OTA Provisioning ................................. 47
1 Introduction

VMware Pulse IoT Center provides a solution to monitor and manage the Enterprise IoT infrastructure and drives its operational efficiency. You can use the VMware Pulse IoT Center as an on-premise solution to begin with and as a hosted solution in subsequent releases. You can use this solution to access a collection of edge services that includes a combination of device management, security, identity, ability to upgrade, and networking capabilities. VMware Pulse IoT Center supports workflows for five different personas that are as follows.

1. System Administrator
2. Pulse Administrator
3. Console Administrator
4. Alert Administrator
5. Gateway Installation Administrator or Technician User

1.1. Browser Support

This VMware Pulse IoT Center release supports all current and popular web browsers such as Mozilla Firefox, Google Chrome, Safari, Microsoft Edge. Pulse Console has been tested with the latest versions of the following browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Platform</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Microsoft Windows 10, Mac OS Sierra</td>
<td>58.x – 62.x</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Microsoft Windows 10, Mac OS Sierra</td>
<td>53.x – 56.x</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Microsoft Windows 10</td>
<td>Edge</td>
</tr>
<tr>
<td>Safari</td>
<td>Mac OS Sierra</td>
<td>11.x</td>
</tr>
</tbody>
</table>

Note: Internet Explorer is not supported in this release of VMware Pulse IoT Center.

**The latest release Firefox Quantum (v 57.x) by Mozilla is not certified for use because it has inconsistencies with the Pulse Console."
1.2. Terminology

Management Console: Advanced device management solution that provides several advanced capabilities like OTA (over-the-air) updates, enrollment, and device health reporting.

Operational Analytics: Helps IT administrators monitor, troubleshoot, and manage the health and capacity of IoT infrastructure.

VMware Identity Manager: An identity provider from VMware.

SMTP Server: The email server that VMware Pulse uses to send email notifications to administrators.

1.3. Administrators

VMware Pulse IoT System allows five types of users. They are as follows:

System Administrator: The system administrator is the administrator who manages the whole system. The system administrator is responsible for configuring the system and testing the compatibility of the setup from an integration standpoint. The system administrator also has permission to perform any action on the Pulse Console. Super admin users are not visible to other roles in the system.

Pulse Administrator: The pulse administrator is responsible for admin user and technician user credential management. The pulse administrator can create administrator users, create technician user credentials, reset the password, and unlock users who are locked. The pulse administrator is used by customers to manage the Pulse Console. However, the pulse administrator does not have permission to make changes to the infrastructure setup.

Console Administrator: The console administrator uses the Pulse system for staging, provisioning (advanced management capabilities), creating organization groups, creating alert definitions, notifications, and other operational analytic activities. The console administrator is familiar with logical flows of the IoT setup that needs to be created to efficiently manage the IoT infrastructure.

Alert Administrator: The alert administrator can view alerts, acknowledge them, and perform manual or automatic solutions to fix the problem. The alert administrator interacts with the Pulse system on a day-to-day basis and maintains the infrastructure with the help of the console administrator, if required. The alert administrator cannot create rules and notifications for generating alerts. The alert administrator must engage with the console administrator for this task.
**Gateway Installation Administrator (technician user):** This is a new role introduced from VMware Pulse IoT Centre 1.1. The gateway installation administrator performs seamless enrollment without manually generating on-boarding credentials on the Pulse Console and manually typing long credentials on the gateway for enrollment. The process authenticates the technician user against a new server endpoint (enrollment service) and retrieves a system generated unique user name and password for use on the gateway. The technician user can access the console only to accept the EULA. After the technician user accepts the EULA, the technician user is not allowed to access the console.
2 Workflows

There are several workflows that are explained from the perspective of different administrators. Each workflow defines a sequence of operations that an administrator with the specified role can perform.

2.1 System Administrator Workflow

System administrators can configure the system so that other roles such as pulse administrators, console administrators, alert administrators, and gateway installation administrators can use the system. In addition, after the backend services are integrated, the staging packages that are pushed to the gateways are also configured by system administrators.

The system administrator performs some of the following functions:

- Provides the password during installation.
- Updates the password on first login.
- Ensures that all the server endpoints are connected, and a set of users are created with accurate roles.
- Creates organization groups in the Management Console to organize the IoT devices.
- Grants system administrator rights to other users.

Some of the workflow procedures include:

- Logging in to the Pulse IoT Center
- Resetting the Password
- Accepting the EULA
- System Management

Logging in To the VMware Pulse IoT Center
2.1.1 Procedure

- Enter the username and password. For example, enter sysadmin as the user name and enter the provided password.

Reset the Password
2.1.2 Procedure

• Enter a new password. You must modify the password when you log in. A typical password must meet the following requirements:
  o The password must be at least 8 characters long.
  o The password must have at least one upper case letter.
  o The password must have at least one special character ($#!@*^&^).
  o The password must have at least one number (0-9).
Accept the EULA

2.1.3 Procedure

Accept the End User License Agreement.

2.1.4 System Configuration

Set up interaction points with the Management Console, the Operation Analytics application, VMware Identity Management application, SMTP, and Google Maps API.

- System configuration is a multi-step process.
- The administrator must Save and Continue at each step.
- Skipping a page will not save any changes made on that page.
- As an administrator, you can save the details for one or two configuration screens and leave the rest to come back again and complete.

2.1.5 Procedure

1. Enter the following details to configure the interaction between the Pulse system and the Management Console. You can update the configurations later, at any stage, as applicable. All the fields are mandatory.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console URL</td>
<td>The public URL of the Management Console Server.</td>
</tr>
<tr>
<td><strong>API URL</strong></td>
<td>The public URL of the Management API Server.</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td><strong>Group ID</strong></td>
<td>The organization group ID in the Management Console. This is the highest level of OG (Organization Group) to which the Pulse system has access to. This is the Group ID field in the Pulse IoT Management Console.</td>
</tr>
<tr>
<td><strong>Group Index</strong></td>
<td>This is the Organization Group (OG) index that the VMware Pulse Device Management Suite maintains internally. You can obtain the index from the URL when you open the Organization Group page.</td>
</tr>
<tr>
<td><strong>API Key</strong></td>
<td>The API enablement key from the Management Console. From the Management Console, navigate to <strong>Groups and Settings &gt; All Settings &gt; Advanced &gt; API &gt; REST API &gt; Enable API Access</strong> button.</td>
</tr>
<tr>
<td><strong>User + Password</strong></td>
<td>The user created in the Management Console. The user must be assigned the role of an administrator or a higher role in the Management Console. You can use this user for the API calls and the sync services in the Pulse system. The admin user must be created for the given customer organization group. The user must have only one role for the customer organization group such as the system administrator or the AirWatch administrator.</td>
</tr>
</tbody>
</table>
2. Enter the configuration details for the interaction between the Pulse system and the Operational Analytics system deployment. All the fields are mandatory on this page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suite API URL</td>
<td>The API server URL for the Operational Analytics Server.</td>
</tr>
<tr>
<td>Username + Password</td>
<td>The basic user created on the Operational Analytics server. This user is used for API calls and sync services in the Pulse system.</td>
</tr>
</tbody>
</table>

VMware Identity Manager is used to manage users and provide Single Sign-On to other systems such as the Management Console. Enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server URL</td>
<td>The hosting public URL of VMware Identity Manager.</td>
</tr>
</tbody>
</table>
### Service Client ID
The admin account for managing the VMWare Identity Manager tenant. On the VMWare Identity Manager remote access screen, create this client with Service Client privileges.

### Service Client Secret
The secret/password for the Service Account

### User Access Client ID
The Pulse API server also acts as an OAuth consumer. You must create a remote client with User Access token privileges.

### User Access Client Secret
The user access account secret/password

### SAML IDP Metadata
The SAML Identity Provider metadata that you download from the VMware Identity Provider Console.

### SAML Server Provider Signing Certificate
A certificate used for communication between IDP and Pulse. You must generate the certificate manually and then upload it.

3. Enter the SMTP settings.
4. Select either SSL or TLS as the type of secure connection.

5. Select the check box to enable Google Maps.
VMware Pulse uses Google Maps to display the location of the resources, if available. Provide the mandatory API key for Google Maps to work. The API key can be obtained from the Google Developer Console or from the Google Enterprise Licensing. Typically, the API key is provided for every deployment of VMware Pulse. You can also obtain the API key by completing the steps at Google Docs: Get API Key.

After configuration is complete, you will be asked to log out and log in again. This is required for the Pulse system to reload all the configurations and start the background processes with the latest configuration. This step completes the configuration of the system. As a system administrator, you can now use the system. You must create users who can log in and use the system.

2.2 Pulse Administrator Workflow
The pulse administrator is responsible for managing the administrator account and for creating technician user credentials for gateway enrollment. The pulse administrator does not have access to the Settings pane that helps to integrate different components of the Pulse System. The pulse administrator must communicate with the super administrator
for any change that is required to set up the infrastructure. The super administrator validates and tests the environment.

### 2.2.1 User Management

There are two different kinds of users such as the basic user and the SAML user.

**Basic users**: You create and manage basic users in VMware Pulse IoT Center as part of the user administration workflow. By default, all basic users have the Alert Admin role assigned to them. You can update the role updated by the system administrator post installation. Basic users do not have access to the AirWatch user interface without an additional login. These users are not created and managed in VMware Identity Manager.

**SAML users**: You create and manage SAML users in VMware Identity Manager. By default, all SAML users are assigned the Console Admin role in addition to the Alert Admin role privileges. SAML users can access AirWatch without an additional login.

### Managing Users

#### 2.2.1.1 Procedure

- To manage users, select the **Admin** tab from the User Accounts page. You are directed to the User Accounts page.

### View Users in the System

#### 2.2.1.2 Procedure
• As a systems administrator, click the Admin Users tab on the left. The page displays a list of administrators such as, basic and SAML.

Delete a User

2.2.1.3 Procedure

• Click the delete icon on the right side of the row that is active. The icon appears when the pointer hovers over a user row.

Create a User

2.2.1.4 Procedure

1. Select the Create User button on the top right side of the page. Enter details in the following fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The user name to be used by the user for logging into the system.</td>
</tr>
</tbody>
</table>
**Password**

The password for the user. A typical password must meet the following requirements:
- The password must be at least 8 characters long.
- The password must have at least one upper case letter.
- The password must have at least one special character ($!@&^{*}@$).
- The password must have at least one number/digit (0-9).

**Full Name**

The first, middle, and the last name of the user that you create.

**Group name**

The name of the organization group to which the user belongs.
- The user can access the resources and data in and below this organization group.

**Email Address**

The email address of the user.

**Phone Number**

The phone number of the user preferably with an extension code.

**Prompt User to change the password on the first login**

Since the current password is provided by the system administrator, update the password for security and privacy reasons.

---

2. Click **Save**.

**Change the Role of the User**

**2.2.1.5 Procedure**

1. Click the **Edit** icon that appears when you hover the pointer on the right of the row that is active.
2. Select **Pulseadmin**, **Consoleadmin**, **Alertadmin** or **Technician**.
3. Click **Update** to update the role of the user.

**Reset or Unlock the Password**

**2.2.1.6 Procedure**

- As a pulse administrator, click the **Key** icon that appears in the row of the user whose password you want to reset.
2.2.2 Client Package Configuration

To configure the client package, refer to the *VMware Pulse IoT 1.1 Center Client Installation Guide* for more information and complete the following steps. The client package configuration is used to create a client package that is installed by the technician on the IoT gateways. The process is explained in the Client Installation guide as specified above.

A high-level summary of steps is provided in the steps below:

- Download the VMware Pulse IoT Center Client packages from the customer download portal.
- Upload VMware Pulse IoT Center Client package to the VMware Pulse IoT Center Server.
- Create VMware Pulse IoT Center Client Sideload package on the VMware Pulse IoT Center Server.
- Download VMware Pulse IoT Center Client Sideload Staging package from the VMware Pulse IoT Center Console.

2.3 Alert Administrator Workflow

A basic user created by the system administrator is assigned the alert administrator role. A VMware Identity Manager user can also be assigned an alert administrator role. A user with the alert administrator role can view and acknowledge all the alerts granted in the system at the relevant level in the hierarchy. A user with the alert administrator role can
use the VMware Pulse IoT Center dashboard using the filters and search capabilities provided. In addition, a user with the alert administrator role can view the alert and notification definitions but cannot edit them.

2.3.1 Monitoring the Health of the IoT Infrastructure

2.3.1.1 View Alert and Resource Summary

You can view the alert and resource summary at a global level. You can view the number of edge systems and connected devices in addition to the different categories of alerts and their counts. You can also obtain information about alert trends, locations of the alerts, and their resources from the VMware Pulse IoT Center Dashboard page.
You can narrow down the view of the IoT infrastructure to a specific level in the hierarchy by selecting the required organizational group from the organizational group drop-down menu.

### 2.3.1.2 Filter Alerts

You can filter by one or more parameter values, alert categories, or by specific custom alerts. You can filter by criteria specific to an edge system or a connected device.

- Select the filter symbol next to the Dashboard label in the VMware Pulse IoT Center Dashboard page to filter the alerts that are displayed.

There are several possible property values that the alert pages can be filtered on, based on the property values that are set for the edge system during the on-boarding process and the metrics that are gathered by Liota. The properties can range from metrics gathered such as CPU, disk utilization, network bytes received in case of an edge system, to metrics such as temperature, pressure in case of an edge device. The properties can also be the values assigned to the edge system or the child device during onboarding, such as the geographic location, latitude, longitude, building, city, state, and zip. You
can search through the alerts using the search box. The system auto prompts for matching search resources available.

2.3.2 Triage Specific Resources

You can view the details of the resources using the resource details pages, that includes properties, metrics, trends, locations, and topology.

Triage Specific Alerts

2.3.2.1 Procedure

- Click on one of the alerts to view the alert details. A sample alert screenshot is displayed above.
2.4 Console Administrator Workflow

The console administrator has all the capabilities of an alert administrator in addition to product creation capabilities and alert and notification management capabilities such as, create, edit, alert, and notification definitions.

2.4.1 Defining Alerts and Notifications

Alerts specify the conditions under which an alert is triggered, such as symptoms of a device and if the temperature exceeds a certain limit. VMware Pulse IoT Center provides a comprehensive set of features to define alerts and the conditions under which the alerts are triggered.

Notifications are a list of actions such as email, that occur based on a set of criteria. Whenever an alert is triggered based on a set of criteria that the notification matches, then the notifications are sent out.

Wait cycles and cancel cycles must be defined when you define an alert/symptom. A wait cycle is the number of cycles the system waits for, before raising an alert. A cancel cycle is the number of cycles the system waits for, before canceling an alert.

Alerts are generated when the condition set in the symptom definition along with the wait cycles of the symptom and alert definitions are met.
Example: If the metric interval is 30 seconds and the wait cycle defined in the alert definition is 3, and wait cycle defined in the symptom definition is 2, then the alert will be generated after 180 seconds \((30 \times 3 \times 2)\), where 30 is metric interval, 3 is alert definition wait cycle, and 2 is symptom definition wait cycle.

Alert Definitions
You can view the list of alert definitions but cannot edit them. You can access the Alert Definitions page from the VMware Pulse IoT Center.

2.4.1.1 Filtering Alerts

Use the filter to narrow down the list of alert definitions.

2.4.1.2 Manage Alert Definitions

Navigate to the Alert Definitions tab and complete the following steps:

1. Click the Add New button at the top right of the page to add alerts.
2. Enter the metadata for the alert definition and click Next.
3. Select the symptoms to trigger an alert.
4. Click Create Symptom to create a new symptom.
5. Enter the metadata for the alert definition and click **Next**.
6. Specify the recommendations to remedy the situation of the alerts in this category.
7. Review and **Save** the alert.

### 2.4.1.3 Notification Definitions

You can view the list of alert notifications from the Notifications page of the VMware Pulse IoT Centre.

You can hover over a notification and click on **Details** icon to view the details.

### Filtering Notifications

#### 2.4.1.4 Procedure

- Use the filter field to narrow down the list of notifications.
2.4.1.5 Manage Notification Definitions

A notification is an action that is independently created. Notifications are based on alert definitions that match the criteria of the notification.

2.4.1.6 Add or Edit Notifications

Navigate to the Notifications tab and enter details for the notifications like the name, description, resource kind, severity of the alert, and the email IDs to which the notification must be sent. Multiple email IDs can be added by clicking the + sign.

2.4.1.7 Procedure

1. Select the Notifications tab on the left pane of the VMware Pulse IoT Centre.
2. Enter the metadata and click Save.
2.4.2 Product Dashboard

Product provisioning allows you to create, using AirWatch, products that contain profiles, applications, and files/actions based on the platform you use. These products follow a set of rules, schedules, and dependencies as guidelines to ensure that your devices remain up to date with the content they need. The screenshot provides an overview of the products that are in the system.

2.4.3 Device Group Management

An assignment group is based on certain criteria satisfied by devices. Any device that satisfies the criteria specified by the assignment group becomes a part of the group. An assignment group is used to move the product to a group of devices.
The screenshot displays the set of criteria possible for any group. Using the criteria, the product can be moved to a group of devices or gateways. The grouping helps you to have greater control on the devices the product can be moved to.

### 2.4.4 Product Creation and Assignment

A product comprises of content or files along with the associated actions that must be sent to the edge systems or devices. You can view all the products and the various states of deployment of these products among the devices.

#### Create a New Product

1. Click **Add Product** to create a new product.
2. Select the platform to which you want to add the product. It could be a Linux or an IoT device.

3. Enter the metadata for the product along with the assignment group.
The following screenshots illustrate the **File** and **Manifest** tabs defined in the Files/Action window, in an Edge system. You can download the file to the `/tmp` folder of the Gateway.
4. To change the permission of `<file_name>`:
   a. Click **Add Action** and select **Run**.
   b. Enter the following command:
      \[
      \text{chmod 777 /tmp/<file_name>}
      \]

5. To run the python file:
   a. Click **Add Action** and select **Run**.
   b. Enter the following command:
      \[
      \text{python /tmp/<file_name> (if file_name is a python file)}
      \]

6. Enter the following command to run the shell file:
   \[
   \text{sh /tmp/<file_name> (if file_name is a shell file)}
   \]

Similarly, the following screenshots illustrate the **Manifest** tab for connected devices defined in the Files/Action window:
7. To create a directory <Directory-1> within the cache path:
   a. Click Add Action and select Run.
   b. Run the following command:
      ```bash
      mkdir -p
      %cache_path%/%uuid%/%attr_IoTDeviceType%/<Directory>
      </Directory-1>
      ```
      • This creates a directory <Directory-1> inside the path as mentioned above.
      • The cache path is /opt/ice-client/data/Cache/Downloads/<Product-number>/<Product-version>
      • The uuid is the unique identity for that connected device.
      • attr_IoTDeviceType is the object type (Edge system/IOT device)

8. To create an empty file inside the directory:
   a. Click on Add Action and select Run.
   b. Run the following command:
      ```bash
      touch
      %cache_path%/%uuid%/%attr_IoTDeviceType%/<Directory>
      </file_name>
      ```
      • This creates an empty file <file_name> inside the <Directory>

9. To copy the file <file_name> to directory <Directory-1> which is present in another directory <Directory>:
   a. Click Add Action and select Run.
   b. Run the following command:
      ```bash
      cp
      %cache_path%/%uuid%/%attr_IoTDeviceType%/<Directory>
      </file_name>
      %cache_path%/%uuid%/%attr_IoTDeviceType%/<Directory>
      </Directory-1>
      ```
      c. This copies the file <file_name> to directory <Directory-1> which is present in another directory <Directory>.

10. Enter the manifest details. The manifest consists of a set of files or actions and the order of their execution.
11. Enter the download and execution conditions such as the state of the device. For example, if the Wi-Fi is turned on. This feature is currently not used in product provisioning in Pulse.

12. Specify when the product is activated or deactivated.
13. Specify the base packages the product depends on. Download and activation are not triggered on devices that do not contain the packages specified on this page. This feature is not used in product provisioning in Pulse.

After the product is created and associated with assignment groups, the policy-driven execution engine ensures that all devices are compliant with respect to the product.

**2.5 Gateway Installation Administrator (Technician)**

The gateway installation administrator is the technician who carries out installations on the gateway with a simplified enrollment procedure. This is new in VMware Pulse IoT Center 1.1. For information about the gateway installation workflow with this new role, refer to the section called *Install VMware Pulse IoT Center Client Sideload Staging package on the Edge System* in the [VMware Pulse IoT 1.1 Center Client Installation Guide](#). Besides the enrollment functionality, this user only accepts the EULA on initial creation of the user.
3 Device Offline Alert

3.1 Requirement of Device Offline

In VMware Pulse IoT Center 1.0, there was no provision to know if the devices (gateways/sensors connected to gateways) are actively communicating with the Pulse IoT Center Server or not. In VMware Pulse IoT Center 1.1, a new type of availability metric has been introduced that is available by default for all the managed objects. Administrators can define offline alerts based on that metric value.

3.2 Understanding When the Device (Gateway/Sensors) Goes Offline

A device (gateway/sensors connected to a gateway) is considered offline under the following cases:

For gateways:

1. When the metrics stop flowing from the device because there is a loss of connection between the gateway and the MQTT broker due to a network error.
2. The metrics stop flowing from the device when the metric package is unloaded.

For sensors connected to gateways:

1. When the gateways through which the sensors are connected goes offline.
2. When the metrics stop flowing from the sensor for some time when the metrics package is unloaded.

3.3 Creation of an Offline Alert

Create an alert as described in the section called Defining Alerts and Notifications under Console Administrator Workflow.

In the symptom definition, set the condition as Availability < 0.0. This is the metric that indicates whether the gateway or the connected device is actively communicating to the server. If the value is -1, it indicates that the device is not communicating to the server.
3.4 Generation of an Offline Alert

Whenever a new device is enrolled, initially the device will be in offline mode and so, an offline alert will be triggered. Until the device publishes metrics, it will be considered offline. However, after five minutes, the device will be online with the Availability metric reflecting an online status and the offline alert generated right after enrollment, is cancelled.

The availability status of the device switches to offline if no metrics flow through the device for a period of one hour. The Availability metric will display as offline and an offline alert is generated. When metrics flow from the device, it will remain online. If the metrics stop flowing because of a network issue or because of unloading the metrics package, the device is displayed as offline and offline alerts are generated.

After the metrics start flowing, the device (edge system/sensors connected to edge system) will appear online and alerts are cancelled.

**Case 1:** If all the metrics have the same interval (for example 5 minutes) and if no metrics are flowing through the device (edge system/connected devices) by unloading the metrics package, then the device will appear offline after an interval of 25 mins (if 5 metrics are present with an interval of 5 mins).

The state of the Availability metric changes based on the metric flow interval of the various metrics of a resource. The default Availability metric monitoring interval is five minutes. If all metrics intervals are below the default monitoring interval, the default monitoring interval of the Availability is adhered.

**Case 2:** If there are 5 metrics and if the interval between the metrics is different for each metric, for example 5 mins, 6 mins, 7 mins, 8 mins, 9 mins, and 10 mins, then the device (edge system/connected devices) will appear offline after an interval of 10 mins. This is the maximum interval among all the metrics if no metrics are flowing through the device by unloading the metrics package.
4 Pulse IoT Center Client OTA Provisioning on Dell Gateways with Ubuntu Core 16

4.1 Prerequisites

1. Ensure that the Pulse Client device is enrolled successfully on the Dell gateway.
2. Ensure that there is proper connectivity between the AirWatch console and the Dell gateway.

4.2 OTA Provisioning Through the Pulse AirWatch Console

Traditional files/actions including download, copy, move, delete, and run, are restricted and can be performed only on writable areas within the snap confinement. Snap applications expose writable areas in the form of environment variables. Files/actions can be performed in the writable areas by specifying the exposed environment variables as macros (%<env-variable>%).

Each snap has the following writable areas:

- `SNAP_DATA` - /var/snap/<snap>/<revision>
- `SNAP_COMMON` - /var/snap/<snap>/common
- `SNAP_USER_DATA` - <user_home>/snap/<snap>/<revision>
- `SNAP_USER_COMMON` - <user_home>/snap/<snap>/common

**Note:** `SNAP_USER_DATA` and `SNAP_USER_COMMON` will be writable only under root user home because of the processes running under root user context.

**Procedure**

1. Login to the AirWatch console using the following link with an appropriate user name and password.
   
   https://<Airwatch_IP>

2. From the device management console, navigate to Files/Actions. Click Add Files/Actions.
   
   **Note:** Select the same OG (organization group) under which the Pulse client device was enrolled: Devices > Staging & Provisioning > Components.

3. Select Linux. In the General section, provide a name and description.

4. In the Manifest section, click the Add Action button.

5. Under Add Manifest, select Run as the Action(s) to perform.

6. Under Command Line and Arguments to run enter the provisioning commands you would like to perform. For example, create a directory, create a file, copy a file from one path to another path under the Snap confinement area as given below:

   ```
   mkdir -p %SNAP_DATA%/test_provision
   ```
touch %SNAP_DATA%/test_provision/mysnapfile.txt

cp %SNAP_DATA%/test_provision/mysnapfile.txt %SNAP_COMMON%/mysnapcopyfile.txt

7. Click Save.
9. Under the General section, provide the Name and Description of the product.
10. Next, under the Assignment groups, select Create Assignment Group.
11. Under Create New Smart Group section, select Select Devices or Users.
12. Under Devices, select the enrolled edge system on which you want to perform product provisioning and click Add.
13. The selected device will appear under the Devices in Smart Group section. Enter a user defined name and click Save.
14. Navigate to the Manifest section and click Add.
15. Under Action(s) to Perform, select Install Files/Actions and under the Files/Actions option, select the appropriate files/actions that you created in the previous steps from the drop-down menu and click Save.
16. Activate the product by clicking the red circle button. A message is displayed stating: Are you sure you wish to continue? Click OK and verify if a green circle appears.
17. Click the search button on the right of the product and monitor the status of your job. The status displayed should be Compliant and the last job status should be Completed.
18. Now, login to the Dell gateway using putty and navigate to the path and confirm that the files are copied suitably as per the provisioning.

Note: If a job fails, verify the logs at the following paths:

/var/snap/ice-client/common/logs/ice-client/AWProcessCommands.0.txt
/var/snap/ice-client/common/logs/ice-client/AWProductManager.0.txt

19. Similarly, perform all the other files/action operations like download, copy, move, delete, run and so on and confirm that the product provisioning works properly without any problems.
5 Pulse IoT Center Client SNAP Management on Dell Gateways with Ubuntu Core 16

5.1 Snap Management

Snap confinement restricts the execution of the snap commands (install, refresh, remove, and so on) from within the snap application. To run the snap commands, invoke the snap manager utility exposed by the client, with the required snap commands through product provisioning.

Snap manager utility transforms these commands into appropriate REST calls and communicates with the Snap Daemon, which in turn executes the command. An additional interface snapd-control must be connected with the client to allow the client to communicate with the snap daemon.

5.2 Prerequisites

1. Ensure that the Pulse Client device is enrolled successfully on the Dell gateway.  
2. Ensure that there is proper connectivity between the AirWatch console and the Dell gateway.

5.3 SNAP Management Using Product Provisioning through the Pulse AirWatch Console

Procedure

1. Login to the AirWatch console using the following link and enter the relevant user name and password.

   https://<Airwatch_IP>

2. rom the device management console, navigate to Files/Actions. Click Add Files/Actions.
   
   Note: Select the OG (organization group) that was used to enroll your Pulse client device in Devices > Staging & Provisioning > Components.

3. Select Linux. In the General section, provide a name and description.

4. In the Manifest section, click Add Action. Under Add Manifest, select Run as the Action(s) to perform.
   
   Under Command Line and Arguments to run, enter the snap management provisioning command you would like to perform. For example, install a snap from the store or local file system.  
   In this example we are trying to install a snap VLC from store.
Here, \texttt{%SNAPM\%} is an environmental variable which points to \texttt{/snap/<snap name>/<revision>/script/snapmanager}.

This \texttt{%SNAPM\%} variable communicates to the snap daemon on the Dell gateway.

\texttt{%SNAPM\%} install vlc (installs vlc snap from global store)

Positional arguments:
- \texttt{Snapname}: Snap package to be installed.

Optional arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{--channel}</td>
<td>Snap channel to be used.</td>
</tr>
<tr>
<td>\texttt{--edge}</td>
<td>Install from the edge channel.</td>
</tr>
<tr>
<td>\texttt{--candidate}</td>
<td>Install from the candidate channel.</td>
</tr>
<tr>
<td>\texttt{--stable}</td>
<td>Install from the stable channel.</td>
</tr>
<tr>
<td>\texttt{--devmode}</td>
<td>Puts snap in development mode.</td>
</tr>
<tr>
<td>\texttt{--jailmode}</td>
<td>Puts snap in enforced confinement mode.</td>
</tr>
<tr>
<td>\texttt{--classic}</td>
<td>Puts snap in classic mode.</td>
</tr>
<tr>
<td>\texttt{--dangerous}</td>
<td>Snap is not verified, no signatures.</td>
</tr>
<tr>
<td>\texttt{--sideload}</td>
<td>Installs snap from the local path.</td>
</tr>
<tr>
<td>\texttt{--beta}</td>
<td>Install from the beta channel.</td>
</tr>
</tbody>
</table>

5. Click \texttt{Save}.
   Click \texttt{Add Product} and select \texttt{Linux}.
7. Under the \texttt{General} section, enter the \texttt{Name} and \texttt{Description} of the product.
8. Under the \texttt{Assignment groups}, place your cursor and select \texttt{Create Assignment Group}.
9. Under \texttt{Create New Smart Group} section, select \texttt{Select Devices or Users}.
10. Under \texttt{Devices}, select the enrolled edge system on which you want to perform product provisioning and click \texttt{Add}.
11. The selected device appears under the \texttt{Devices in Smart Group} section. Enter a user defined name and \texttt{Save}.
12. Navigate to the \texttt{Manifest} section and click \texttt{Add}. Under \texttt{Action(s) to Perform}, select \texttt{Install Files/Actions}.
13. Under \texttt{Files/Actions}, select the appropriate files/actions you created in the previous steps from the drop-down menu and click \texttt{Save}.
14. Activate the product by clicking the red circle button. It displays a message that states: \texttt{Are you sure you wish to continue?} Click \texttt{OK} and verify that a \texttt{green} circle appears.
15. Click the search button on the extreme right of the product and monitor the status of your job. The status displayed should be \texttt{Compliant} and the last job status should be \texttt{Completed}.
16. Now, login to the Dell gateway using putty and ensure that the files are copied accurately as per the provisioning. Run the following command to verify that the vlc snap was installed successfully and listed under the list of snaps that are installed.
sudo snap list

Note: If the job fails, verify the logs at the following paths:

/var/snap/ice-client/common/logs/ice-client/AWProcessCommands.0.txt

/var/snap/ice-client/common/logs/ice-client/AWProductManager.0.txt

/var/snap/ice-client/common/logs/ice-client/snapmanager.log

17. Similarly, perform all other snap management operations like remove, refresh, revert, enable, disable, connect, and disconnect through product provisioning.

5.3.1 Supported Snap Management Commands

Pulse Client exposes the snap manager utility through an environment variable SNAPM.
Snap management can be achieved by invoking the snap manager utility (using the macro %SNAPM%) with the appropriate snap command using 'Run' Files/Actions. The following snap commands are supported.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>remove</td>
<td>Removes snap from the system.</td>
<td>%SNAPM% remove snapname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%SNAPM% remove hello</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To verify snap removal, run the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sudo snap list</td>
</tr>
<tr>
<td>refresh</td>
<td>Refreshes (updates) a snap from the store based on the availability of the update.</td>
<td>%SNAPM% refresh snapname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%SNAPM% refresh (Refreshes all snaps)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%SNAPM% refresh hello (Refresh hello snap)</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Command</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>revert</td>
<td>Reverts (downgrades) a snap to its previous state.</td>
<td>%SNAPM% revert snapname</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the snap. The binaries and services of the snap will no longer be available, but all the data will still be available.</td>
<td>%SNAPM% disable snapname</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the previously disabled snaps.</td>
<td>%SNAPM% enable snapname</td>
</tr>
<tr>
<td>connect</td>
<td>Connects a snap plug to the exposed interface slot. Interfaces allow snaps to communicate or share resources.</td>
<td>%SNAPM% connect plug slot</td>
</tr>
</tbody>
</table>

To verify snap refresh, run the following command from the store:
```
sudo snap list --all
```

Example:
```
%SNAPM% revert vlc
```

To verify snap revert, run the following command from the store:
```
sudo snap list --all
```

Example:
```
%SNAPM% disable ice-client
```

To verify snap disable, run the following command:
```
sudo snap list
```

Example:
```
%SNAPM% enable ice-client
```

To verify snap enabled, run following command:
```
sudo snap list
```

Positional arguments:
```
plug Snap plug to be connected, <snap>::<plug>
```
according to the protocol established by the interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect</td>
<td>Connects a plug to an interface slot.</td>
<td>%SNAPM% connect hello:process-control core:process-control</td>
</tr>
<tr>
<td>interfaces</td>
<td>Verifies if the snap plug is connected to the exposed interface.</td>
<td>sudo snap interfaces</td>
</tr>
</tbody>
</table>

Example:

To verify snap, connect to the exposed interface slot and run the following command. Verify if the snap plug is connected to the exposed interface.

```
sudo snap interfaces
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>disconnect</td>
<td>Disconnects a plug from an interface slot.</td>
<td>%SNAPM% disconnect plug slot</td>
</tr>
</tbody>
</table>

Positional arguments:

- **plug**: Snap plug to be disconnected, `<snap>:<plug>`
- **slot**: Snap slot to be disconnected, `<snap>:<slot>`

Example:

```
%SNAPM% disconnect hello:process-control core:process-control
```

To verify that the snap plug is disconnected from the interface slot, run the following command:

```
sudo snap interfaces
```

Provide an ability to set a snap action timeout using the command line
The timeout option is mainly intended for the snap manager. The snap manager waits for the snap daemon to return a response after a particular snap action is completed. For example: installing a snap from store.

The default timeout is 20 mins. This is an optional parameter that can be set while configuring the snap management commands during product provisioning in the AirWatch console.

Consider that a snap download takes one-hour or 30 minutes, snap manager will never know how long it must wait for the snap daemon to complete the action so that it can return the status back to the server through the client. The default wait time is 20 mins. If the action is not completed in 20 mins, it is treated as a failure, but the action might have succeeded in the device. To overcome this scenario, timeout has been added.

Timeout is an optional value and you can define any value based on your requirement. If you do not define the timeout value, then the default timeout will be 20 minutes.

Syntax:

```
%SNAPM% install [--timeout TIMEOUT] snapname
```

```
--timeout TIMEOUT Snap action timeout value in secs
```

Example:

```
%SNAPM% install --timeout 1800 wifi-ap
```

In this example, the timeout parameter is 1800 seconds which means that the snap manager will wait for 30 minutes and return the status only after 30 minutes based on whether install was successful or has failed.

**Note:** You can find additional information related to snaps at the following links:

- [https://docs.snapcraft.io/?_ga=2.73722514.1648244170.1520753094-1716090929.1519737331](https://docs.snapcraft.io/?_ga=2.73722514.1648244170.1520753094-1716090929.1519737331)
- [https://docs.snapcraft.io/reference/snap-command](https://docs.snapcraft.io/reference/snap-command)
6 Pulse Client Upgrade through Product Provisioning Using the AirWatch Console

You can upgrade a client snap through OTA provisioning by creating a product manifest in the AirWatch server. The Agent Upgrade action in the product manifest cannot be utilized because of restrictions imposed by snap confinement. Instead, the product manifest should contain a Run action to trigger the snap manager which in-turn communicates with the snap daemon to install the client snap.

6.1 Prerequisites

1. Ensure that Pulse Client device is enrolled successfully on the Dell Gateway.
2. Note the Pulse Client version installed on the gateway.
3. Ensure that there is proper connectivity between the AirWatch console and the Dell Gateway.

6.2 Generating a Staging Package using the APF File

- Download the `ice-client-<version>.zip` that needs to be upgraded from packages folder.
- Unzip the `ice-client-<version>.zip` file.
- Get the `ice-client-snapbin-x86_64-version.apf` APF file which contains client binaries and snap packages using the following steps:

Procedure

Login to the AirWatch console. Navigate to the device management console. Ensure that you are under the global organization group or the customer type organization group.

1. Navigate to Devices > Staging & Provisioning > Components > Agent packages.
2. Click Add AirWatch Agent.
3. Select Linux.
4. Upload the `ice-client-snapbin-x86_64-version.apf` APF package you wish to upgrade.
5. Click Save.

Create Files/Actions Components Containing Liota Registration Packages

Procedure

1. From the device management console, navigate to Devices > Staging & Provisioning > Components > Files/Actions. Click Add Files/Actions.
2. Select Linux.
3. In the Files section, click the Add Files button and upload the Liota user package required for registration of the gateways:
- iotcc_mqtt.py
- general_edge_system.py

**Note:** Any manifest added in the staging package is not applied while upgrading the snap.

4. Click **Save**.
5. Provide the download path on the gateway for all the Liota user package files as %SNAP_DATA%/liota-packages
6. From the device management console, navigate to **Devices > Staging & Provisioning > Staging**.
7. Click **Add Staging** and then **Linux**.
8. Under the **General** section, enter a user name and description for staging.
9. From the **Agent** option, select the pulse client agent that was uploaded as specified in section 6.2.
   ice-client-snapbin-x86_64-version.apf.
10. Click **Manifest**:
    - Click **Add > Install Profile**. Select the valid MQTT cert and click **Save**.
    - Click **Add > Install Profile**. Select the valid AirWatch cert and click **Save**.
    - Click **Add > Install Profile**. Select the valid API cert and click **Save**.
    - Click **Add > Install Files/Actions**. Select the files/actions created in the previous steps and click **Save**.
11. Double-click the **Sideload Staging** button on the right side of the intended sideload package.
12. Ensure that the organization group displayed is correct.
13. Ensure that the universal flag is not selected.
14. Enter a passphrase for the sideload package.
15. Click **Download**.

A sideload staging package file called SideLoadStaging_<string based on package name, version, organization group>.tar.gz is downloaded

**Generating a Snap on a Linux Host Machine**

**Procedure**

1. Copy the **SideLoadStaging** package that was downloaded to your local machine, to the home directory of the Linux host machine using WinSCP or FileZilla.
2. After the **SideLoadStaging** package is copied to your Linux host machine, extract the contents by running the following command:

   ```bash
tar -xvzf SideLoadStaging_string based on package name_version_organization group.tar.gz
   ```

3. After extraction, the following files are created:
   - advancestaging enrollment settings
agent PFILES SideLoadStaging_string based on package name_version_organization group.tar.gz

4. To extract client binaries, navigate to the agent directory and run the embedded shell script as given below:
   sudo ./ice-client-snapbin-x86_64-apf_version.sh

5. To generate a snap, run the build-snap script that was extracted under the agent folder using the following command:
   
sudo ./build-snap.sh

   The ice-client snap package is generated along with the script connect-interfaces that contains a list of interfaces to connect. Verify that the ice-client snap is generated successfully without any errors.

6. The following files are created under the /agent/packages directory
   connect-interfaces ice-client_apf_version_amd64.snap
   Copy this ice-client snap to your local machine using any of the scp clients like WinSCP or FileZilla.

6.3 Upgrading the Pulse Client Snap Through OTA Provisioning

Upload the generated client snap to the product manifest in AirWatch.

Procedure

1. Login to the AirWatch console using the following link and enter the relevant user name and password.
   https://<Airwatch_IP>

2. From the device management console, navigate to Files/Actions. Click Add Files/Actions.

   Note: Select the same OG (organization group) under which your Pulse client device was enrolled: Devices > Staging & Provisioning > Components.

3. Select Linux. In the General section, enter a name and description.

4. In the Files section, click Add File and upload the snap that was downloaded on to your machine from the Linux host machine. Under the download path, provide the path which will be used to copy the snap on the Dell gateway given below and click Save.
   %SNAP_COMMON%/downloads/

5. In the Manifest section, click Add Action. Under Add Manifest select Run as the Action(s) to Perform.

   Under Command Line and Arguments to run, enter the snap upgrade command.

   %SNAPM% install %SNAP_COMMON%/downloads/ice-client_version_amd64.snap --dangerous --sideload
7. Here `%SNAPM%` is an environmental variable which points to `/snap/<snap name>/<revision>/script/snapmanager`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--dangerous</code></td>
<td>The dangerous option is used as the Pulse client snap does not have signatures.</td>
</tr>
<tr>
<td><code>--sideload</code></td>
<td>Installs snap from local path</td>
</tr>
</tbody>
</table>

8. Click **Save**.

9. Navigate to **Devices > Staging & Provisioning > Product List View**. Click **Add Product** and select **Linux**.

10. Under the **General** section, enter the name and description of the product.

11. Under the **Assignment** groups, place your cursor and select **Create Assignment Group**.

12. Under the **Select New Smart Group** section, select **Users** or **Select Devices**.

13. Under **Devices**, select the enrolled edge system on which you want to perform product provisioning and click **Add**.

14. The selected device appears under **Devices** in the **Smart Group** section. Enter a user-defined name and click **Save**.

15. Navigate to the **Manifest** section and click **Add**.

16. Under **Action(s) to Perform**, select **Install Files/Actions** and under **Files/Actions**, select the appropriate **Files/Actions** that you created in the previous steps from the drop-down menu and click **Save**.

17. Activate the product by clicking the red circle. A message is displayed: **Are you sure you wish to continue?** Click **OK** and verify that a green circle appears.

18. Click the search symbol on the extreme right of your product and monitor the status of your job. The status displayed must be **Compliant** and the last job status displayed must be **Completed**.

19. Login to the Dell gateway using putty and run the following command to verify that the pulse client snap was upgraded successfully and listed under the list of snaps that are installed.

```
sudo snap list -all
```

The ice-client snap upgrade should be successful. Verify the logs at the following paths:

```
/var/snap/ice-client/common/logs/ice-client/AWProcessCommands.0.txt
/var/snap/ice-client/common/logs/ice-client/AWProductManager.0.txt
/var/snap/ice-client/common/logs/ice-client/snapmanager.log
```