VMware Workspace ONE
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-01</td>
<td>May 2019</td>
<td>Arpit Bhatt</td>
<td>Initial Release</td>
</tr>
<tr>
<td>2019-02</td>
<td>October 2019</td>
<td>Danny Jump</td>
<td>Minor Functional Updates</td>
</tr>
</tbody>
</table>

Copyright

©Copyright 2019 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.
Contents
Introduction and Overview ......................................................................................................................... 5
Pictorial View of the Integration .................................................................................................................. 6
Software Requirements.................................................................................................................................... 6
Installation and Deployment Guide ............................................................................................................. 6
Access to the Extension Store .................................................................................................................... 6
New Extension Support in ClearPass 6.7+ ..................................................................................................... 7
  Extensions and IP address configuration support ..................................................................................... 7
  Extensions and web proxy support ........................................................................................................... 7
Configuration Steps ....................................................................................................................................... 9
  Step I: Register and Request for a Skyhook Tenant ID ............................................................................... 9
  Step II: Configuring Workspace ONE (Airwatch) for ClearPass Integration ............................................... 12
    Getting API Credentials ......................................................................................................................... 12
    Getting REST API key ............................................................................................................................. 14
    Configuring Event Notifications .......................................................................................................... 15
  Step III: Airwatch Extension Installation and Configuration ...................................................................... 18
Examples: .................................................................................................................................................... 23
  Device Registration .................................................................................................................................... 23
  Compliance Status Change ....................................................................................................................... 24
  MDM Unenroll ............................................................................................................................................ 26
  Device Deletion ......................................................................................................................................... 27
Appendix A – Additional Diagnostics and Support ..................................................................................... 30
  The Extensions Service ............................................................................................................................ 30
  Extension logs and debugging ................................................................................................................... 30
  Accessing extension logs within ClearPass ‘Collect Logs’ ........................................................................ 31
Figures
Figure 1: Pictorial view of ClearPass Policy Manager integration with VMware Workspace ONE ........................................... 6
Figure 2: Entering HP Passport credentials .................................................................................................................. 7
Figure 3: Extension framework GUI ........................................................................................................................... 8
Figure 4: Defining the base IP SUBNET and LOCALHOST for the Extensions framework ........................................ 8
Figure 5: Skyhook tenant registration email ID ........................................................................................................... 9
Figure 6: Skyhook tenant registration application to integrate ........................................................................................ 10
Figure 7: Skyhook tenant registration company identifier ............................................................................................. 10
Figure 8: Sample email response upon registration ................................................................................................ 11
Figure 9: Create an Admin user ................................................................................................................................... 12
Figure 10: Add Admin User details ............................................................................................................................. 13
Figure 11: Admin User Role .......................................................................................................................................... 14
Figure 12: REST API key ................................................................................................................................................ 15
Figure 13: Event Notification rule ............................................................................................................................... 15
Figure 14: Event Notification URL .................................................................................................................................. 16
Figure 15: Enable Notification Events ........................................................................................................................ 17
Figure 16: Extensions framework GUI .......................................................................................................................... 18
Figure 17: GUI Extension search ..................................................................................................................................... 18
Figure 18: GUI Extension Install ...................................................................................................................................... 19
Figure 19: GUI Extension configuration at install time ................................................................................................... 19
Figure 20: Extension configuration parameters ........................................................................................................... 20
Figure 21: Creating an Admin user on ClearPass ........................................................................................................ 21
Figure 22: GUI review and setting the Extension configuration .................................................................................. 22
Figure 23: Log validation .................................................................................................................................................. 22
Figure 24: Attributes added to Endpoint repository .................................................................................................... 25
Figure 25: Attributed changed by Extension .................................................................................................................. 27
Figure 26: Toggle Known to Unknown on delete action ................................................................................................. 28
Figure 27: Sample Enforcement Policy ........................................................................................................................ 29
Figure 28: Checking on the extensions service and how to start/stop the service ......................................................... 30
Figure 29: Using the GUI to change the DEBUG level .................................................................................................. 30
Figure 30: Extension logs location in 'Collect Logs' diagnostic GZ file .......................................................................... 31
Introduction and Overview

Workspace ONE, formerly known as VMware Airwatch is the unified digital workspace platform that simplifies and secures app access and IT management for the modern workforce.

ClearPass Policy Manager integration with Airwatch existed since a long time. This integration leverages the Endpoint Context Servers. Here is the link to this guide which talks about this integration in detail: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=33307

That obviously brings us to the question of what’s different here? The integration previously leveraged a polling mechanism to fetch information associated with endpoints from the Airwatch server using the Endpoint Context Servers. The new integration however receives in real time rather than relying on a poll interval. Hence, upon device enrollment/unenrollment, Workspace ONE triggers a webhook which will be consumed by a ClearPass service running in the cloud. The extension installed within ClearPass for this integration maintains a persistent connection with this service and immediately writes the updated information in the ClearPass endpoint repository. This integration is an enhancement that leverages an extension. The events for which the real time updates can be sent via webhook are configurable in Workspace ONE. Following are a list of the events we support today.

1. Device enrollment
2. Device unenrolled/ Enterprise wipe
3. Device compromised/ Status changed
4. Device Delete

To summarize, the endpoint repository continues to be used an Authorization source but the information is updated in real time hence allowing an administrator to create more accurate policies. Without integration with the extension, ClearPass would only get the latest information based on the polling interval. The default value of this polling interval is 60 minutes. It could be set to a lower value (under guidance from Aruba) depending on the number of endpoints to be fetched and varies based on the environments.

An important point to note is that, this integration enhances the existing integration we have with Airwatch. Hence this should be used after the configuration of the existing integration using the Endpoint Context Servers. In order to get the most of the integration with Workspace ONE/Airwatch, add the real time update capabilities by integrating with the extensions which is covered in detail in this guide.
Pictorial View of the Integration

The diagram below shows a pictorial overview of the components and how they interact with each other.

Figure 1: Pictorial view of ClearPass Policy Manager integration with VMware Workspace ONE

The ClearPass Airwatch Extension establishes a persistent connection with a tenant in Aruba Skyhook. As soon as a webhook event is pushed from Airwatch, it is consumed immediately by the Extension.

Software Requirements

The minimum software version required for ClearPass is 6.7.2. At the time of writing, ClearPass 6.8.0 is the latest available and recommended release. Any subsequent ClearPass software release will support this integration. ClearPass runs on either hardware appliances with pre-installed software, or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.5, 6.0, 6.5, 6.6 or higher
- Microsoft Hyper-V Server 2012 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 or 2016 R2
- KVM on CentOS 7.5

The Workspace ONE UEM version used to verify the interoperability for this guide was 19.04.0.0.

Installation and Deployment Guide

This document assumes your ClearPass environment is already configured and operational. If you require assistance with basic deployment, refer to the following deployment guide:

Access to the Extension Store

Access to the extension store to download extensions is simplified starting version ClearPass 6.7. The ability to download extensions from the store and to validate support entitlement for access to the Software Updates Portal (e.g. Posture & Profile Data Updates, Software Updates, & Skins) now uses the HPE Passport account credentials that are associated with the customers’ ClearPass licenses. This is configured where previously the subscription-id was defined, under **Administration -> Agents and Software Updates -> Software Updates** as shown below. Ensure you enter your HPE Passport credentials to enable extension download capabilities.

![Figure 2: Entering HP Passport credentials](image)

New Extension Support in ClearPass 6.7+

With the release of 6.7, several new features have been added to enhance the functionality of the extension framework. Previously, all extension installation and operation tasks required use of the API Explorer to interoperate with the extension and the underlying framework. Now this functionality has been exposed with a new GUI. The GUI is accessed from within the Guest UI and is shown below, **Administration -> Extensions**.

Extensions and IP address configuration support

The other major additions in the 6.7 release are the ability to define the extension framework base IP network and statically define the IP address of the individual extensions. The latter being useful when deploying extensions in a cluster and the requirement for a fixed IP address for the same extension across a cluster regardless of which ClearPass node or nodes it is installed on.

Extensions and web proxy support

Prior to 6.7 support for web proxy was limited to the installation of the extensions. Starting in ClearPass 6.7, extensions now support communications with 3rd parties via a web proxy. This adds incremental web proxy functionality. If a web proxy is defined in ClearPass Policy Manager, then an extension will use that configuration.

The Policy Manager web proxy configuration is ONLY read by the extension at installation time. If the web proxy configuration is changed in Policy Manager, then the extension must be re-installed so the new settings are re-read and bonded to the extension.
Figure 3: Extension framework GUI

Configuring the base extension IP subnet, this is defined within Policy Manager as shown below under Administration > Server Manager > Server Configuration [chose your node] Service Parameters [ClearPass system service]. The default is 172.17.0.1/16, this address is the non-routed address of the ClearPass node itself. The IP addresses range for the extensions are based upon the network prefix used.

Note that the subnet defined here for the extension framework must be one of the following 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16.

Figure 4: Defining the base IP SUBNET and LOCALHOST for the Extensions framework

Changing the extension base IP address will require the extension service to be restarted.

Changing the “Extensions Network Address” range is necessary if either the MGMT or DATA interface are also using an address in the extension default range of 172.17.x.x/16. Set the new network address range as needed and restart the extension service for this to take effect.
Configuration Steps

There are primarily 3 steps involved in getting this integration configured.

1. Register and request for a Skyhook tenant
2. Configuration of VMware Workspace ONE UEM/Airwatch for Integration
3. Installation and Configuration of the Workspace ONE extension using the GUI in ClearPass 6.7.X

Step I: Register and Request for a Skyhook Tenant ID

- Register on the URL https://peoplemove.typeform.com/to/Z80ezD
  Follow the instructions on the form to request for the Skyhook tenant ID. This ID is unique per customer.
- Read the instructions carefully and ensure you use your company email address only.

Figure 5: Skyhook tenant registration email ID
• Select Airwatch for our integration

Figure 6: Skyhook tenant registration application to integrate

2. Please select the App you wish to integrate with using Skyhook?

- Envoy
- SinePoint Pro
- Teamgo (GoReception)
- Teem LobbyConnect
- VMware Workspace ONE (previously AirWatch)

• Choose a unique company identifier for your skyhook app. Kindly read the instructions carefully and avoid spaces or special characters

Figure 7: Skyhook tenant registration company identifier

3. Please enter company name associated with this Skyhook registration?

Cpmlab

• Accept Terms and Conditions and Submit the request.

You will receive a response within 24-48 hours upon submitting a request.
Following is a sample response with the desired details.

**Figure 8: Sample email response upon registration**

---

Thanks for your interest in our integration between VMware WorkSpace ONE (formerly Airwatch) and ClearPass. Please find below your registered tenant details for our Skyhook platform which will enable your ClearPass deployment to receive real-time events from the VMware WorkSpace ONE cloud platform.

You can find documentation steps for the VMware WorkSpace ONE integration [here](#), please note that at this time we are recommending a minimum version of ClearPass Policy Manager 6.7.2, however the most recent version is 6.7.9 which is the recommended version.

Below are your Skyhook tenant mapping details as requested:

```
"skyhookTenant": "311a47292e9",
"dbAccessToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJpZiIsIm5hbWUiOjEwMDYsImlhdCI6MTY3MTQ4MzU4OCwiZXhwIjoxNjY5NjIyOTA4fQ.yhYs5vTSdOtvIz2B8_4WJv9hpgV6zgQCSJcS3icbildw"
```

Use the following Target URL when configuring Event Notifications inside WorkSpace ONE:

```
https://skyhook.clearpassbeta.com/api/skyhook/airwatch/311a47292e9
```

The extension id required to download the latest build of the VMware WorkSpace ONE integration is as follows:

```
"storeId": "865529a0-c1ac-4d6f-81b5-418c24c56e72"
```

Alternately, if you are running 6.7.2 or later as recommended, you can search the Extension Store by name.

Regards

-d

**DANNY JUMP, PRODUCT MANAGER – CLEARPASS**

Aruba, a Hewlett Packard Enterprise company

---

Kindly copy the `skyhookTenant`, `dbAccessToken` and the Target URL in the highlighted area in a text file. This will be used for configuration of the extension in ClearPass Policy Manager as well as configuring the tenant details on Workspace ONE UEM.
Step II: Configuring Workspace ONE (Airwatch) for ClearPass Integration

Setup and configuration of Workspace ONE UEM is beyond the scope of this guide. Here we specify the steps necessary to configure the integration.

Below are the configuration steps to follow.

**Getting API Credentials**

Login to the Workspace ONE UEM tenant, using your administrator credentials.

Create a new administrator account for this integration.

Navigate to **Accounts > Administrator > List View > Add > Add Admin.**

*Figure 9: Create an Admin user*
Specify the mandatory fields below and create a user. It is not recommended to use the default admin account for this integration for security reasons.

**Figure 10: Add Admin User details**

<table>
<thead>
<tr>
<th>Add/Edit Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Type</strong></td>
</tr>
<tr>
<td><strong>User name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
</tr>
<tr>
<td><strong>Require password change at next login</strong></td>
</tr>
<tr>
<td><strong>First Name</strong></td>
</tr>
<tr>
<td><strong>Middle Name</strong></td>
</tr>
<tr>
<td><strong>Last Name</strong></td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
</tr>
<tr>
<td><strong>Locale</strong></td>
</tr>
<tr>
<td><strong>Initial Landing Page</strong></td>
</tr>
</tbody>
</table>

> Two-Factor Authentication Method

> Notification
When creating this user, one can specify the role associated with the user. Use “Device Manager” role or any custom role that gives device information access via the REST API.

**Figure 11: Admin User Role**

<table>
<thead>
<tr>
<th>Organization Group</th>
<th>Role</th>
<th>Passcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE dellvejump</td>
<td>Device Manager</td>
<td></td>
</tr>
</tbody>
</table>

The credentials of the account created can be used as "airWatchUser" and "airWatchPassword" in the ClearPass extension configuration.

**Getting REST API key**

Go to “Groups & Settings” > All Settings.

Navigate to System > Advanced > API > REST API.

To add a new API service.

a. Select “Override” as the Current Setting.

b. Set “Enable API Access” to “Enabled”.

c. Click on +ADD box to add a new service account. This should generate the API Key.

   i. Set the Service name to something that can be identified later like “ClearPass Extension”.
   
   ii. Set the Account Type to “Admin”.

   iii. Copy the API Key. This will be used as “airWatchApiKey” for the ClearPass extension configuration.

d. Ensure you Save your changes.
Configuring Event Notifications

Go to “Groups & Settings” > All Settings.

Navigate to System > Advanced > API > Event Notifications.

Click on + ADD RULE to add the events that the ClearPass skyhook needs to be notified for.

The Event Notification window helps to specify the Target Name and the Target URL. The Target URL contains the skyhook tenant that was granted to you at the time of the request in “Step I: Register and Request for a Skyhook Tenant ID”. The email received should consist of the Target URL to be used.

The Username and Password field could be left blank.
Select the **Format** as **JSON**.

**Figure 14: Event Notification URL**

- **Target Name**: CP-skyhook
- **Target URL**: https://skyhook.clearpassbeta.com/qa/skyho
- **User name**: 
- **Password**: Show
- **Confirm Password**: Show
- **Format**: JSON

The attempt to “TEST CONNECTION” is unsuccessful in this scenario.

Finally, scroll down under the **“Events”** section and specify the events for which we require a real time update from Airwatch.

Currently ClearPass has added support for the following events.

- Device Enrollment
- Device Unenrolled Enterprise Wipe
- Device Wipe
- Device Compromised Status Change
- Device Compliance Status Change
- Device Delete
- Device Attribute Change - Ownership

These are essentially the events which are leveraged within ClearPass Policy Manager to define policies and hence requires a real time update for accurate policy enforcement.
Once the required events are Enabled, Save the changes.
Step III: Airwatch Extension Installation and Configuration

Starting in ClearPass 6.7, a Graphical User Interface (GUI) was introduced to make the process of interacting with the extension framework easier. To access the extension GUI, from the Guest System, under Administration find the Extension user interface as shown below.

**Figure 16: Extensions framework GUI**

From here, click on ‘Install Extension’, and the search box below appears. Enter the keyword “Airwatch” and click on Search.

**Figure 17: GUI Extension search**

Starting 6.7, in a cluster environment an extension can be installed on the subscriber nodes directly.
Click on the Extension and then the **Install option**

**Figure 18: GUI Extension install**

Set a specific IP address for the extension if required. It will automatically pick an IP address if not assigned. Also, it can be changed later if required.

**Figure 19: GUI Extension configuration at install time**

After the extension has been installed, review the configuration and adjust as needed. Notice the options to Start, Delete, Reinstall or Show Logs and the option to edit and set the extension configuration.
The default configuration used for the extension is below

```json
{
    "logLevel": "INFO",
    "verifySSLCerts": true,
    "cppmUser": "admin.user",
    "cppmPassword": "********",
    "skyhookTenant": "aruba",
    "dbAccessToken": "********",
    "airWatchHost": "airwatch.domain.local",
    "airWatchUser": "user.name",
    "airWatchPassword": "********",
    "airWatchApiKey": "********",
    "enrollmentRetries": 3,
    "enrollmentWaitTimer": 5,
    "toggleEndpointStatus": false
}
```

Each of the attributes are explained in the table below in detail.

**Figure 20: Extension configuration parameters**

<table>
<thead>
<tr>
<th>Configuration attribute</th>
<th>Description</th>
<th>Example/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>logLevel</td>
<td>Logging level for troubleshooting</td>
<td>&quot;DEBUG&quot;, &quot;INFO&quot;, &quot;WARN&quot;, &quot;ERROR&quot;</td>
</tr>
<tr>
<td>verifySSLCerts</td>
<td>The host name or IP address of your Airwatch system.</td>
<td>Example: 192.168.1.10 or abcdef.airwatchportals.com</td>
</tr>
<tr>
<td>cppmUser</td>
<td>The user name of an Admin user in ClearPass. This is used for device profiling.</td>
<td>Administrator username</td>
</tr>
<tr>
<td>cppmPassword</td>
<td>The password for the user entered in cppmUserName</td>
<td>Administrator password</td>
</tr>
<tr>
<td>skyhookTenant</td>
<td>The Skyhook tenant ID received in the registration email.</td>
<td>c7xxxxx8-b2b6-4125-9741-cxxxxxxx38a6</td>
</tr>
<tr>
<td>dbAccessToken</td>
<td>The access token for Skyhook received in the registration email.</td>
<td>Long Random string like 7INXYr1YUixxxxxv...</td>
</tr>
<tr>
<td>airWatchHost</td>
<td>The URL/FQDN for airwatch instance</td>
<td>xxx.airwatchportals.com</td>
</tr>
<tr>
<td>airWatchUser</td>
<td>The airwatch account username who has access to the device information using the APIs.</td>
<td>Airwatch API username</td>
</tr>
<tr>
<td>airWatchPassword</td>
<td>The airwatch account password for the user who has access to the device information using the APIs.</td>
<td>Airwatch API password</td>
</tr>
<tr>
<td>airWatchApiKey</td>
<td>Allows access to Airwatch REST APIs.</td>
<td>huzBl-xxx-xxxxx-xxxxx</td>
</tr>
<tr>
<td>enrollmentRetries</td>
<td>During the enrollment process, if there is no MAC Address found, retry X number of times to wait for a MAC Address.</td>
<td>3 {Default}</td>
</tr>
<tr>
<td>enrollmentWaitTimer</td>
<td>The delay between retries when attempting to get a MAC Address.</td>
<td>5</td>
</tr>
<tr>
<td>toggleEndpointStatus</td>
<td>When a device is unenrolled, if set to true, the endpoints status will be set to &quot;Unknown&quot;.</td>
<td>false / true</td>
</tr>
</tbody>
</table>
The **cppmUserName** and **cppmPassword** should be for an Administrator account. The device profiling attributes obtained from Airwatch need to be written into the endpoint repository leveraging the REST APIs which requires an Administrator account.

A ClearPass administrator account can be created under **Administration > Users and Privileges > Admin Users.** Click on **Add.** A user with the following **Privilege Level** needs to be created.

**Figure 21: Creating an Admin user on ClearPass**

A Network Administrator privilege level is sufficient for the action of adding device profiling information into the endpoint database of ClearPass.

A copy of the VMware Airwatch Extension with the desired configuration is shown below, this has to be modified for your deployment. Include the **skyhookTenant, dbAccessToken, airWatchHost, airWatchApiKey, airWatchUser, airWatchPassword, cppmUserName and cppmPassword** that will be specific to your environment.

In the V2 of the VMware Airwatch Extension support was added to modify the **enrollmentRetries** and the **enrollmentWaitTimer,** if during the enrollment process events are being received into ClearPass with a mac-address of 000000000000, an automatic retry mechanism was added. If endpoints continue to not be added, the retry parameters may need to be modified to cater for this by adding extra delay or more retries.

In the V3 of the VMware Airwatch Extension support was added for **toggleEndpointStatus,** this switch enables the Known/Unknown status to be modified on a ClearPass Endpoint. During the process of a Device being Unenrolled in Airwatch you possibly might want the status to be set to Unknown such that standard ClearPass housekeeping can additionally tidy up and remove these endpoints from the ClearPass EndpointDb.

Change or include any other values based on the description of each in the above table

Select **Restart** and click on **Save Changes** to restart the extension.
Figure 22: GUI review and setting the Extension configuration

After the configuration and the restart of the extension, click on Show Logs

Figure 23: Log validation

The above log states that the extension has established a successful connection to skyhook and ready to ingest events from Airwatch in real time.
Examples

In this section we look at some sample events. The logs have been enabled in DEBUG mode for details.

Device Registration

As soon as a device enrolls with Airwatch, it triggers a webhook which is consumed by ClearPass using extensions. In this scenario the Event Type triggered is ‘MDM Enrollment Complete’.

Once the extension gets the device ID using webhook, it will trigger an API call into Airwatch to get all details associated with the device since the webhook triggered does not send all the details. These details are then copied into the endpoint database in ClearPass. Notice the MAC address received in the logs. Since the MAC address is absent during the Device Enrollment event, the error can be ignored.

In this scenario, Airwatch may not have gathered the MAC address of the device hence an API call gives us information with MAC address = 000000000000. ClearPass requires a MAC address for the entry to be added in the endpoint repository. Take note to the note above of the retry capabilities added to the Airwatch extension to cater for this missing mac-address.

```
[2019-05-13T17:17:42.830] [DEBUG] AirWatch - New event received (-Leo7of0NJa4kCUIR1Vu).
[2019-05-13T17:17:42.850] [DEBUG] AirWatch - Event Details:
[2019-05-13T17:17:42.851] [DEBUG] AirWatch - {
  "EventId": 148,
  "EventType": "MDM Enrollment Complete",
  "DeviceId": 23697,
  "DeviceFriendlyName": "iPad3,5-a9db198fa8be40cebf44b7e3d60d4a38a27d1eac",
  "EnrollmentEmailAddress": "abhatt@arubanetworks.com",
  "EnrollmentUserName": "enrol",
  "EventTime": "2019-05-14T02:17:41.0804739Z",
  "EnrollmentStatus": "Enrolled",
  "CompromisedStatus": "",
  "CompromisedTimeStamp": "2019-05-14T02:17:41.9052133Z",
  "ComplianceStatus": "NotAvailable",
  "PhoneNumber": "",
  "Udid": "a9db198fa8be40cebf44b7e3d60d4a38a27d1eac",
  "SerialNumber": "DMPJL6F6F18D",
  "MACAddress": "000000000000",
  "DeviceIMEI": "013367007879628",
  "EnrollmentUserId": 75198,
  "AssetNumber": "a9db198fa8be40cebf44b7e3d60d4a38a27d1eac",
  "Platform": "Apple",
  "OperatingSystem": "10.3.3",
  "Ownership": "CorporateDedicated",
```
**Compliance Status Change**

This event is triggered immediately after a device is enrolled and performs its first compliance check. It is also triggered if AirWatch detects a change in the compliance status of the device. Again, the webhook sends us the Device ID which is used by the extension to trigger an API call on AirWatch and get more information about the device. Once the device lookup is completed, the extension writes the attributes into the ClearPass endpoint repository.
Once the compliance check on the device is finished, the endpoint table on ClearPass gets updated with the device information as shown below.

**Figure 24: Attributes added to Endpoint repository**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Compliance</td>
<td>Compliant</td>
</tr>
<tr>
<td>2. Compromised</td>
<td>false</td>
</tr>
<tr>
<td>3. Data Encryption YN</td>
<td>Y</td>
</tr>
<tr>
<td>4. Device Friendly Name</td>
<td>AB iPad</td>
</tr>
<tr>
<td>5. Enrollment Email Address</td>
<td><a href="mailto:abhatt@arubanetworks.com">abhatt@arubanetworks.com</a></td>
</tr>
<tr>
<td>6. Enrollment Status</td>
<td>Enrolled</td>
</tr>
<tr>
<td>7. Enrollment User Name</td>
<td>enrol</td>
</tr>
<tr>
<td>8. Group ID</td>
<td>9835</td>
</tr>
<tr>
<td>9. Group Name</td>
<td>HPE dannyjump</td>
</tr>
<tr>
<td>10. IMEI</td>
<td>013367007879628</td>
</tr>
<tr>
<td>11. Is Activation Lock Enabled</td>
<td>true</td>
</tr>
<tr>
<td>12. Is Cloud Backup Enabled</td>
<td>false</td>
</tr>
<tr>
<td>13. Is Device DND Enabled</td>
<td>false</td>
</tr>
<tr>
<td>14. Is Device Locator Enabled</td>
<td>true</td>
</tr>
<tr>
<td>15. Is Network Tethered</td>
<td>false</td>
</tr>
</tbody>
</table>
MDM Unenroll

Once the Device Management profile is deleted from the managed endpoint, it would trigger a webhook for the event type captured below.

```
[2019-05-13T18:56:53.893] [DEBUG] AirWatch - Event Details:
  "EventId": 39,
  "EventType": "Break MDM Confirmed",
  "DeviceId": 23697,
  "DeviceFriendlyName": "AB iPad",
  "EnrollmentEmailAddress": "abhatt@arubanetworks.com",
  "EnrollmentUserName": "enrol",
  "EventTime": "2019-05-14T03:56:51.1141542Z",
  "EnrollmentStatus": "Enrolled",
  "CompromisedStatus": "",
  "CompromisedTimeStamp": "2019-05-14T03:56:51.1751679Z",
  "ComplianceStatus": "Compliant",
  "PhoneNumber": "",
  "Udid": "a9db198fa8be40ceb44b7e3d60d4a38a27deac",
  "SerialNumber": "DMPJL6F6F18D",
  "MACAddress": "98FE94714162",
  "DeviceIMEI": "013367007879628",
  "EnrollmentUserId": 75198,
  "AssetNumber": "a9db198fa8be40ceb44b7e3d60d4a38a27deac",
  "Platform": "Apple",
  "OperatingSystem": "10.3.3",
  "Ownership": "CorporateDedicated",
  "SIMMCC": "310",
  "CurrentMCC": "404",
  "OrganizationGroupName": "HPE dannyjump"
}
[2019-05-13T18:56:54.362] [DEBUG] AirWatch - Finished attempting to update device(s) with the ID 23697.
```
This results in change of the attribute ‘MDM Enabled’ to ‘false’. ‘Let’s look at the attributes changed for the endpoint in the endpoint database.

**Figure 25: Attributed changed by Extension**

![Figure 25: Attributed changed by Extension](Image)

The above attributes can be used in the ClearPass Policy Manager to ensure devices with “MDM Enabled = false” are either quarantined, or forced into a captive portal role or denied access.

**Device Deletion**

In this scenario, a device that was added previously by polling was deleted from Workspace ONE. This triggered a “Delete Device Requested” event.

```
[2019-05-13T19:12:51.235] [DEBUG] AirWatch - Event Details:
  "EventId": 662,
  "EventTypeName": "Delete Device Requested",
  "DeviceId": 23697,
  "EnrollmentEmailAddress": "abhatt@arubanetworks.com",
  "EnrollmentUserName": "enrol",
  "EnrollmentStatus": "Unknown",
  "CompromisedStatus": null,
  "CompromisedTime": "2019-05-14T04:12:50.2314048Z",
  "ComplianceStatus": null,
  "PhoneNumber": null,
```
This again results in change of the attribute "MDM Enabled" to false. Starting with V2 of the WorkspaceOne Extension a device deletion will also toggle the Known/Unknown status of the endpoint, the allows for ClearPass housekeeping to remove devices from the EndpointDb. This is an optional configuration switch.

Figure 26: Toggle Known to Unknown on delete action
A sample **Enforcement Policy** that can be used is shown here for reference. This may completely vary based upon the requirements of the customer.

**Figure 27: Sample Enforcement Policy**

```
<table>
<thead>
<tr>
<th>Conditions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Endpoint:Enrollment Status <strong>EQUALS</strong> Unenrolled)</td>
<td>Redirect to Enrollment page</td>
</tr>
<tr>
<td>(Endpoint:Data Encryption <strong>EQUALS</strong> N)</td>
<td>Send Email</td>
</tr>
<tr>
<td>(Endpoint:Owner <strong>NOT_EQUALS</strong> Corporate)</td>
<td>Guest-Public Guest Profile</td>
</tr>
<tr>
<td>(Endpoint:Compliance <strong>NOT_EQUALS</strong> Compliant)</td>
<td>Quarantine Role</td>
</tr>
<tr>
<td>(Endpoint:OS Version <strong>CONTAINS</strong> iOS)</td>
<td>Old-OS-ArubaRole</td>
</tr>
<tr>
<td>AND (Endpoint:OS Version <strong>NOT_CONTAINS</strong> 11.)</td>
<td></td>
</tr>
<tr>
<td>(Endpoint:Compromised <strong>EQUALS</strong> true)</td>
<td>Quarantine Role</td>
</tr>
</tbody>
</table>
```
Appendix A – Additional Diagnostics and Support

The Extensions Service

The ClearPass extension is supported by a new system service that was initially added in 6.6. This service should be running. Note that restarting this service will affect all deployed and running extensions.

To check on the state and to restart the service, go to Administration > Server Manager > Server Configuration [select a ClearPass node] > Service Control. From here start/stop the extension service. By default, this service is started.

Figure 28: Checking on the extensions service and how to start/stop the service

Extension logs and debugging

Referencing the configuration previously used, adjust the logLevel to ‘DEBUG’. In the new 6.7, GUI change the configuration and restart the extension as shown below. Logs can then be viewed from the ‘Show Logs’.

Figure 29: Using the GUI to change the DEBUG level

Remember after changing the logging level, the extension will need to be restarted for this change to take effect.
Accessing extension logs within ClearPass ‘Collect Logs’

In addition to the logging of messages that be examined in the extension as shown above, it’s possible to configure the extension to log messages so that they can be collected and examined via the Policy Manager ‘Collect Logs’ system function. This is extremely useful for Aruba TAC. The logs are available under Administration > Server Manager > Server Configuration > Collect Logs.

If there is a requirement for Aruba TAC to investigate a system issue, one of the items they regularly ask for is the system logs to aid with their diagnostic investigation. The ClearPass extension can write its logs such that they are available and can be collected with all other system diagnostics information when the ‘Collect Logs’ function is run. Remember that by default, the logLevel is set to INFO but TRACE, DEBUG, INFO, WARN, ERROR, FATAL can also be set. Any of the levels will display the information for the selected state and lower. For example, if INFO is selected, it will show messages for INFO, WARN, ERROR, FATAL.

After the logs have been collected and exported from the system, expand the GZ file and locate the extension logs in the following location ‘PolicyManagerLogs->extension’ as shown below.

Figure 30: Extension logs location in ‘Collect Logs’ diagnostic GZ file