MaaS360

a Hewlett Packard
Enterprise company

ClearPass

Integration Guide

Change Log

Version	Date	Modified By	Comments
2018-01	Sept-2018	Danny Jump	Initial release

Copyright

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

a Hewlett Packard Enterprise company

www.arubanetworks.com
3333 Scott Blvd
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550

Figures

Introduction

ClearPass Policy Manager has supported multiple MDM/EMM vendors for over 6 years. We continue to maintain and extend our technology lead with the major Enterprise Mobility Management (EMM) platforms, allowing Aruba ClearPass customers to extend the knowledge of managed device state (device type, policy compliance etc.) down to the business rules that govern their corporate network admission policies.

For example, if the EMM platform detects that a device is jailbroken, the EMM platform only has the option to attempt to enforce the business policy at the device level. By extending this policy state to ClearPass as the network policy definition point, the jailbreak status of a device can be used to deny access or quarantine this device the next time it attempts to connect to the secure network.

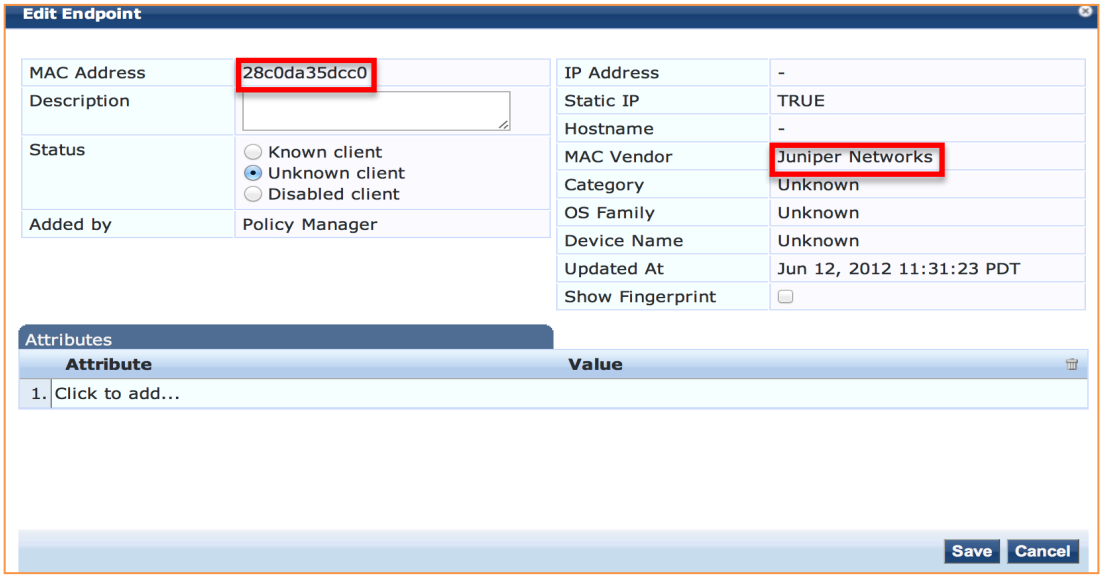
This walkthrough explains the details of the current integration, the configuration steps to establish the API relationship between ClearPass Policy Manager and the customer's chosen EMM platform and finally, the expected device inventory and policy compliance data expected from each EMM vendor.

Some familiarity with Mobile Device Management concepts and the use of ClearPass Policy Manager's network enforcement methodology are assumed throughout this Guide.

MDM/EMM Integration

ClearPass Policy Manager has an extensible database for tracking devices attempting to connect to secure corporate networks. The devices are stored within the Endpoints table that is indexed on a unique identifier for each device, its MAC Address.

Typically the Endpoints table stores only basic information about the device collected from RADIUS authentication transactions associated with its usage on the wired or wireless access networks as shown below on the right-hand-side. In-depth information relating to the device posture is not available as no Attribute data is shown and only basic information can be extracted such as the OUI (first 3-bytes of the mac) to identify the manufacturer.



The knowledge about this device is increased through the use of ClearPass Policy Manager's built-in device profiling capabilities by monitoring traffic patterns from the device as it attempts to connect to the network. Information extracted from DHCP, HTTP packets and other sources of context can help provide additional details about the manufacturer and class of device.

Figure 1 - Basic endpoint smart-device information

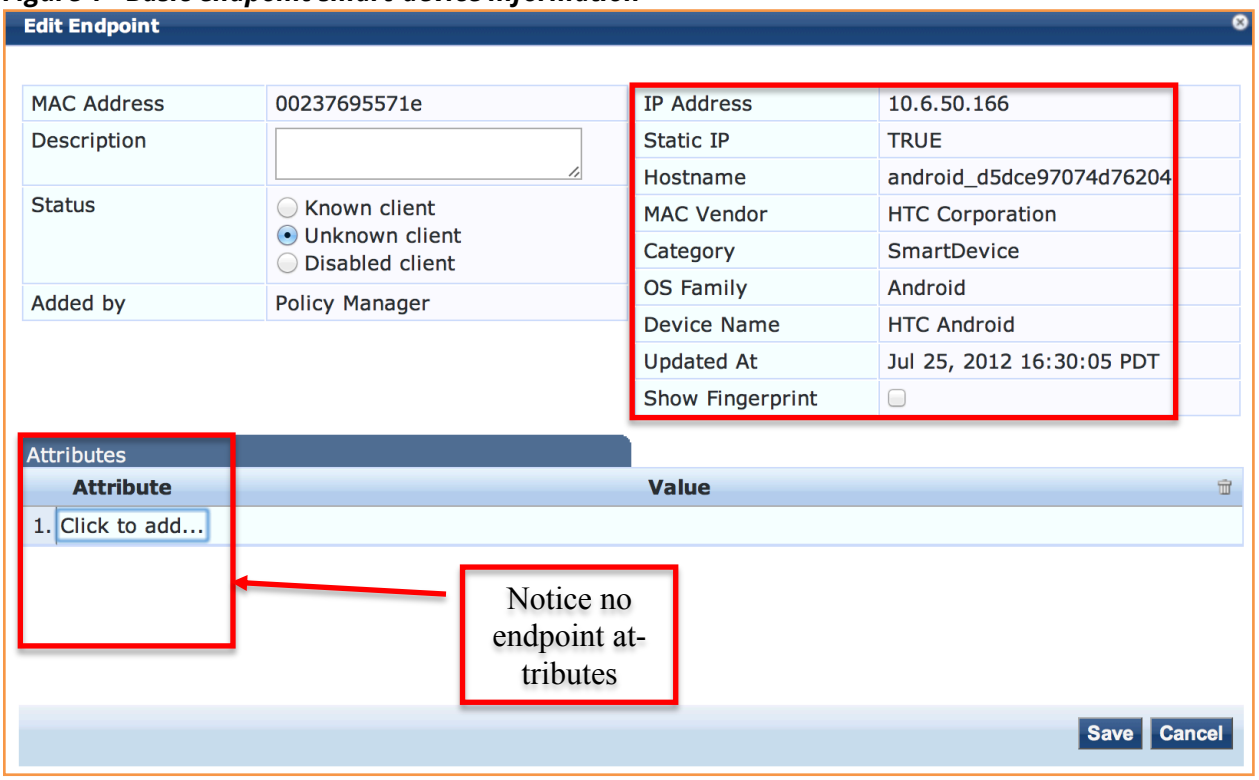


Figure 2 - Additional endpoint information retrieved thru DHCP fingerprinting

However, many customers have invested in EMM platforms to help them manage large rollouts of corporate issued smartphones or tablets. These EMM deployments can hold additional information about the device policy state that cannot be retrieved by passively monitoring network traffic as it enters the corporate network.

The EMM integration leverages the extensive dataset that each entry in the Endpoints table can hold, by adding a set of EMM normalized data tags. These additional data tags can then be referenced in enforcement policies to implement various business rules based on the device state information received from the EMM platforms.

Below we show an example of the additional attributes that can be integrated into the ClearPass Endpoint profiler database that could be received from an EMM vendor. Not all EMM vendors expose the same level of data, we normalize the information received and present it in a standard attribute template.

Figure 3 - Endpoint plus EMM attributes

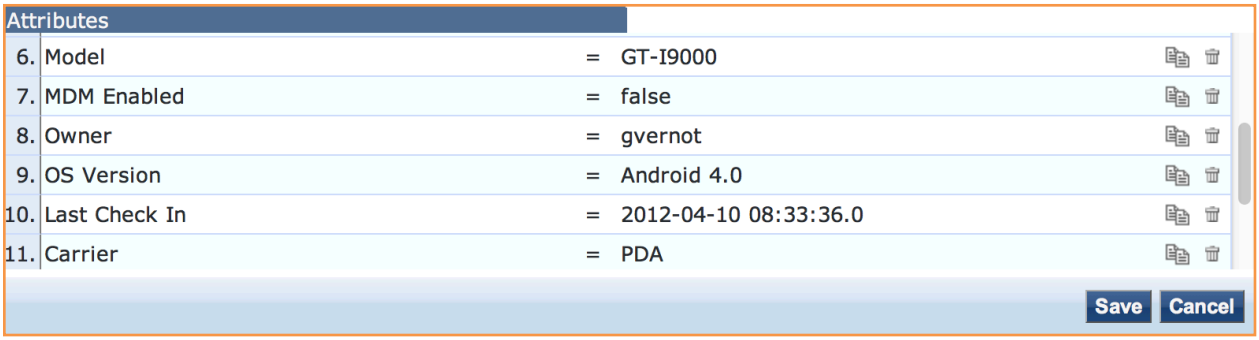


Figure 4 - More EMM attributes

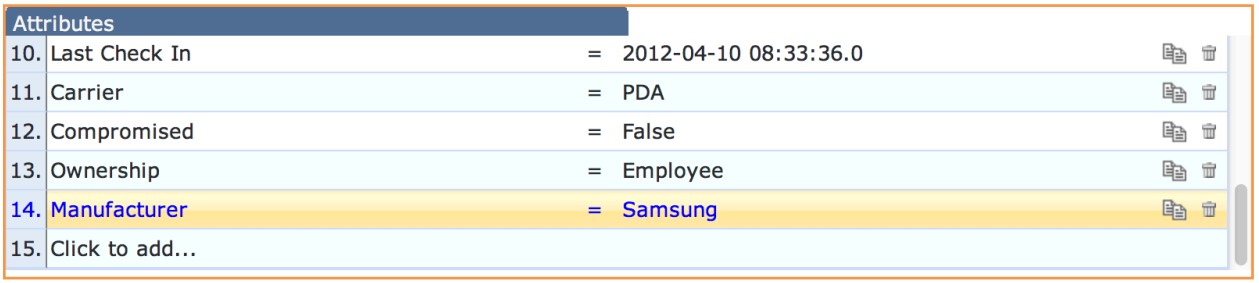


Figure 5 - Even more EMM attributes

Additionally, the ClearPass EMM integration updates the internal device Profile database with knowledge of the device type learned from the configured EMM platform. This valuable inventory data about the device manufacturer, its hardware platform type and software version are all recorded in the ClearPass Endpoint profiler database and provide the definitive knowledge of the device type that could not otherwise be collected from passive network monitoring. This level of detail is equivalent to the device information recovered from ClearPass' own Onboard device provisioning and OnGuard device posture assessment.

Configuration of EMM Vendors

From the Administration menu of ClearPass Policy Manager, a new menu option has been added under External Servers called Endpoint Context Servers. The configuration requires the menu option 'Add Context Server', under **Administration-> External Servers-> Endpoint Context Servers** a full list is shown below.

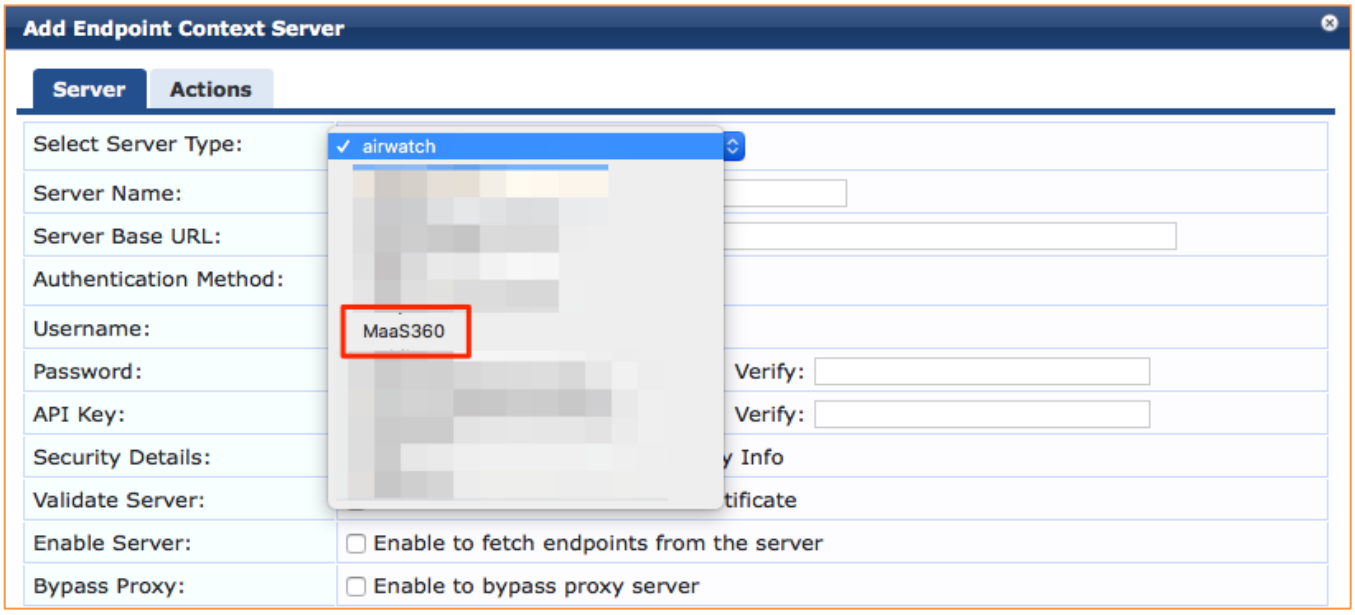


Figure 6 - Endpoint Context Server configuration for CPPM v6.4.0

Server Configuration varies slightly by vendor. But for all EMM partners some baseline parameter are required such as, Server Name, Server Base URL, User Name, and Password. Authentication is typically HTTPS authentication.

The Update Frequency option is defined in cluster-wide service parameter "Endpoint Context Servers polling interval". Go to **Administration > Server Manager > Server Configuration** -> **Cluster-Wide Parameters**.

Figure 7: Cluster-Wide Parameters

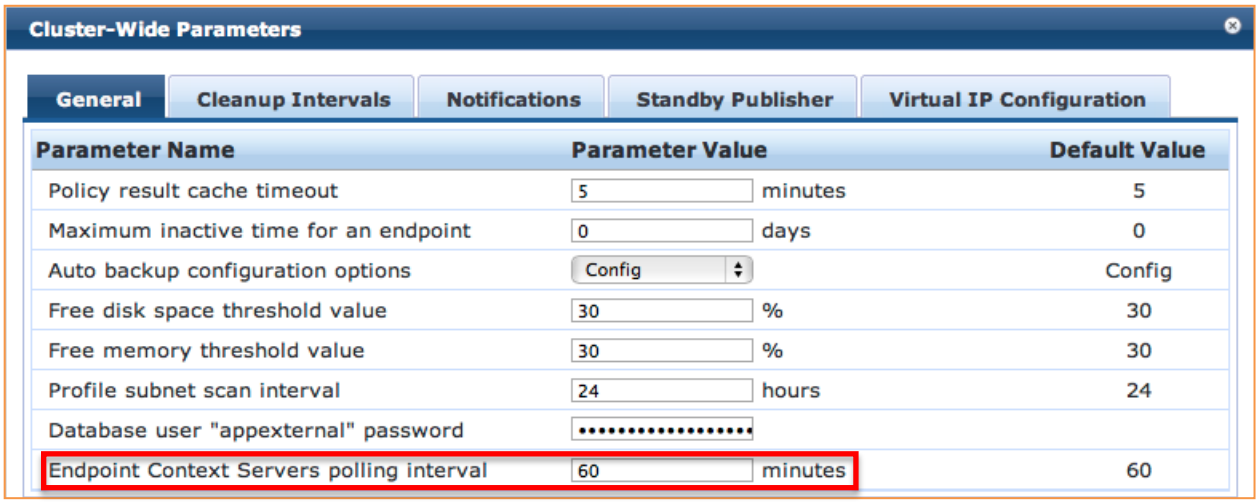


Figure 8 - Endpoint Context Servers polling interval – default 60 minutes

Typically the Update Frequency (Polling Interval) should be set relative to the device check-in interval configured on the EMM platform. This check-in interval is how often the EMM agent on the device itself connects back to the EMM server. For some platforms this could be 4 hours or longer, so there is no benefit to having an aggressive polling interval on ClearPass as the data returned will largely be the same.

Normalized Dataset

ClearPass Policy Manager communicates with the configured EMM platform via their published API interface. Typically these are HTTP Based API's - Typically these API communications are defined using RESTful API calls returning XML or JSON output. The ClearPass integration consumes these XML or JSON outputs, which are very specific to each EMM platform, and normalizes their output to a common set of Endpoint tags that can be added to the ClearPass database. By normalizing the output, common and easy to understand enforcement policies can be created within ClearPass without the need for the administrator to understand the semantics of the EMM API interface.

The following table shows the currently available normalized data set implemented by the ClearPass EMM Integration. Not all of these attributes will be available consistently from each EMM platform or for each device type within a chosen EMM platform. For example, the Carrier attribute will not be available for a WiFi only tablet as it does not have a cellular chipset.

In the event that an attribute is not available from the configured EMM platform or not supported on the returned device type, the ClearPass Endpoints table will not contain a value for that normalized attribute.

Endpoint Tag	Tag Type	Comments
Manufacturer	Inventory	Manufacture name such as Apple, Samsung, etc. For Activate will always be “Aruba Networks”
Model	Inventory	Model name such as iPad, DROID X, etc. with extraneous sub-model info removed.
OS Version	Inventory	Version number such as iOS 6.1, Android 4.0, etc. Minor version numbers are removed so that 6.1.1 becomes 6.1.
UDID	Inventory	Device unique identifier
Serial Number	Inventory	Device serial number
IMEI	Inventory	Cellular only devices
Phone Number	Inventory	Cellular only devices
Carrier	Inventory	Cellular only devices
Owner	Inventory	Registered enterprise username
Display Name	Inventory	Full name of registered owner
Description	Inventory	Display a description of the device.
Source	Inventory	Display which EMM vendor supplied the device details
Ownership	Inventory	“Corporate”, “Employee” perhaps “Personnel”
EMM Identifier	Inventory	Internal identifier used by EMM API interface. This varies between EMM vendors.
Compromised	Policy	“True” or “False”. Jail broken device or Root-kit detected.
Encryption Enabled	Policy	Device level encryption status
Blacklisted App	Policy	“True” or “False”. A blacklisted app is installed on the device.
Required App	Policy	“True” or “False”. A required corporate app is missing from the device.
EMM Enabled	Policy	“True” or “False”. The device is under EMM management.
Compliance	Policy	A summarized view of the endpoint
Last Check In	Policy	Last time the device last checked in to EMM server

Figure 9 - List of all possible normalized attributes

Using EMM Data for Network Enforcement

Once the EMM integration is configured and device data is being populated to the Endpoints and Profile databases within ClearPass, this information can be used to enforce various business rules on how these corporate managed devices are admitted on to the network.

Given EMM platforms are largely focused on smartphone and tablet devices, the network of interest is typically limited to WiFi connectivity. The following examples provide some guidance on how to leverage the EMM data to change the way these mobile devices are admitted onto a corporate WiFi network.

Endpoint Data

The data retrieved from the EMM platform and stored in the Endpoints table as additional tags contains both inventory data and policy state information. Therefore, an incredibly rich set of business rules can be enforced on the corporate network as it relates to the device type, ownership, compromised status, and the impact of Apps that are installed or missing, just to name a few. The following sample business rules included below illustrate how the EMM data included in the Endpoints table can be used to enforce network policy decisions and control the way these devices are admitted onto the network.

Jail broken or Rooted-Device Detected

A common used case of EMM platforms is to leverage the presence of the EMM agent (App) to attempt to detect if a device has been jail broken (Apple iOS devices) or a root-kit installed (Android). This status of the device being compromised is reported by the EMM agent back to the EMM server either during a regular check-in interval or as an alert message and will then be reflected in the ClearPass Endpoints table via the API integration.

A device being compromised will often result in the IT administrator being less trusting of the device and depending on the local security policy may result in a reduced level of network access or complete quarantining of the device. ClearPass' rich policy enforcement allows the administrator to choose how these compromised devices should be handled the next time the user attempts to connect to the enterprise network. The following enforcement policy example shows how the Endpoint *Compromised* data tag is being referenced whenever a device attempts to connect to the enterprise network.

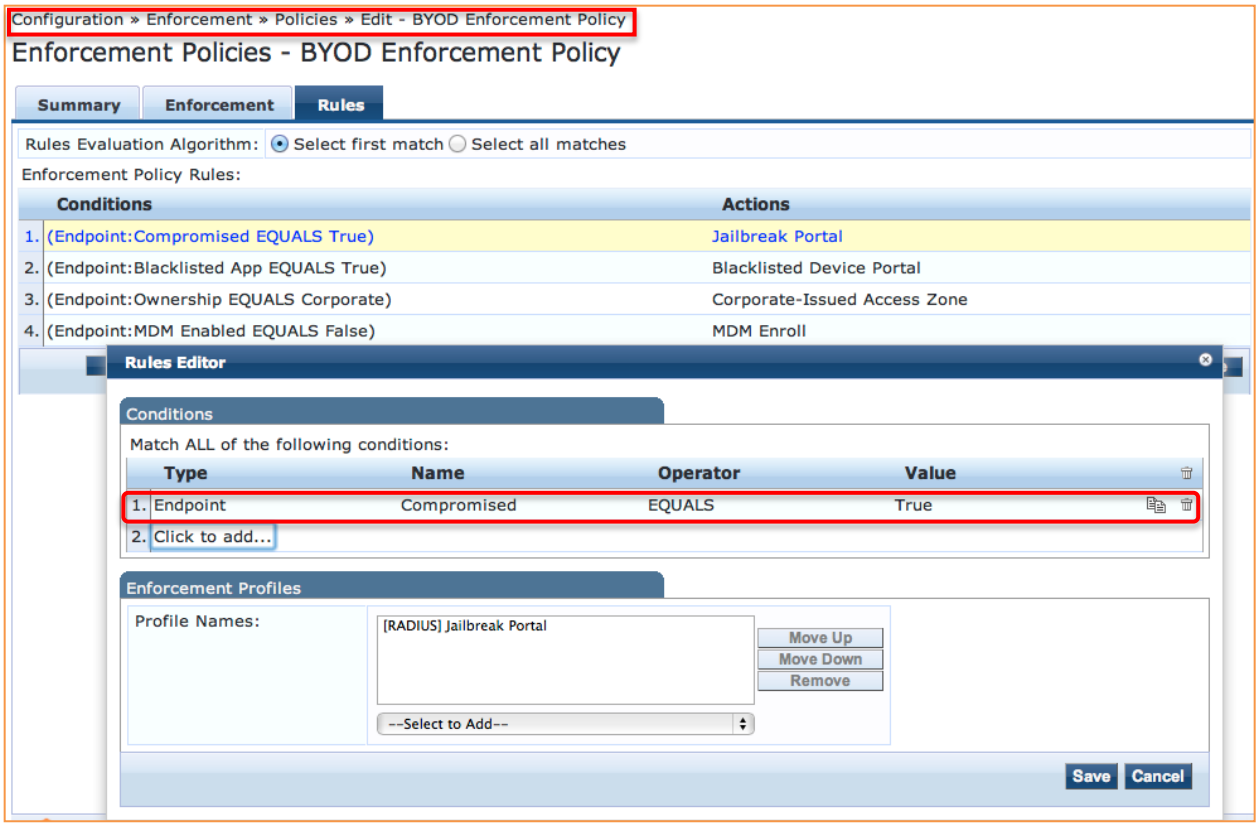


Figure 10 - Enforcement Policy – Endpoint compromised

In the event that this flag is set to True by the configured EMM platform, then the network enforcement profile applied will result in the device being placed in a quarantine state. This is achieved by ClearPass informing the Aruba controller to redirect the access attempt to a captive portal page informing the user of their breach of network access policy.

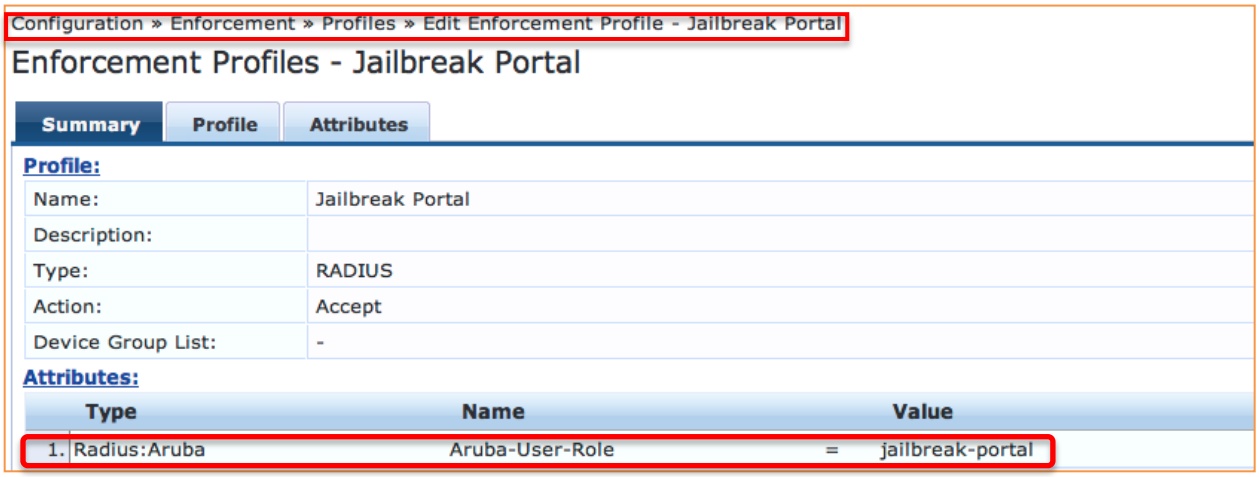


Figure 11 - Enforcement Profile – redirect for Jailbreak/rooted devices

Figure 12 - Captive portal Jailbreak detection warning

Blacklisted App Detected

Several EMM platforms have the ability to build compliance policies around the Apps that have been installed on a smartphone or tablet. This is possible because the EMM platform will harvest the entire list of Apps that have been installed on the device and track them on an ongoing basis. This is a key reason why EMM is more appropriate for corporate issued devices where there are no privacy concerns about personally installed Apps that is often the case in a BYOD environment.

As part of the EMM compliance policy, a list of Blacklisted Apps can be defined and during a device check-in, if one of these Apps is installed on the device, the compliance state can be triggered. The EMM integration with ClearPass does not recover the details of the Apps installed on the device, but instead recognizes that the EMM has detected the presence of a Blacklisted App by the EMM internal compliance policy. This allows

ClearPass to maintain its BYOD friendly approach, which is central to its Onboard provisioning solution, by avoiding any potential violation of the end user privacy through personal App visibility.

The following enforcement policy example shows how the Endpoint *Blacklist App* data tag is being referenced whenever a device attempts to connect to the enterprise network.

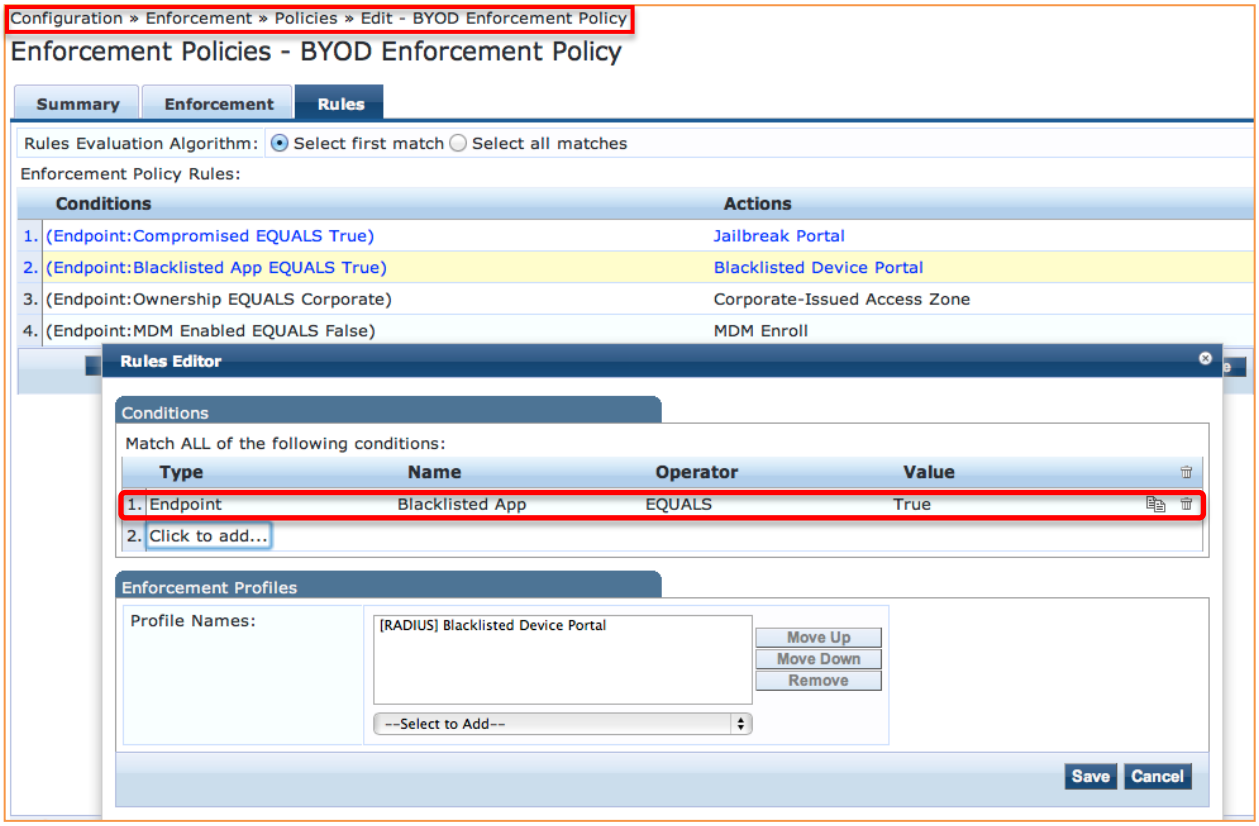


Figure 13 - Enforcement Policy – Blacklisted App

In the event that this flag is set to True by the configured EMM platform, then the network enforcement profile applied will result in the device being redirected to a Blacklisted App portal informing the user of their breach of network access policy. Optionally the device could be restricted network access, such as only to the Internet.

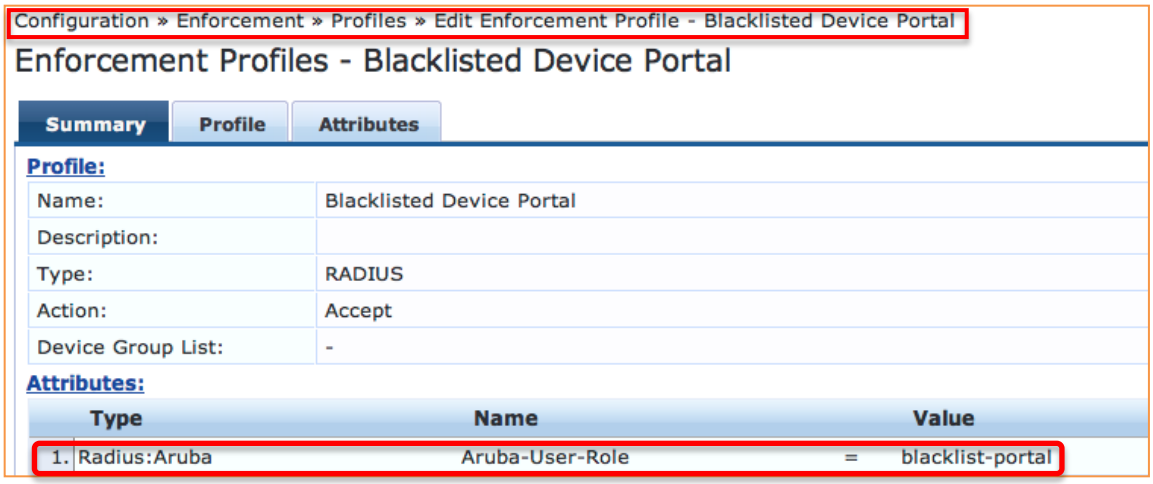


Figure 14 - Enforcement Profile – redirect for Blacklisted App

Corporate Issued vs. Employee Liable Device

Many EMM platforms allow the administrator to define the ownership type of each device taken under management. Corporate-owned or Employee-owned device types are tracked and can be reported to ClearPass via the API integration.

Some customers may wish to leverage this knowledge of corporate issued devices and an associated rollout of a corporate application to change the way that device accesses the network. The following enforcement policy example shows how the Endpoint *Ownernship* data tag is being referenced whenever a device attempts to connect to the enterprise network.

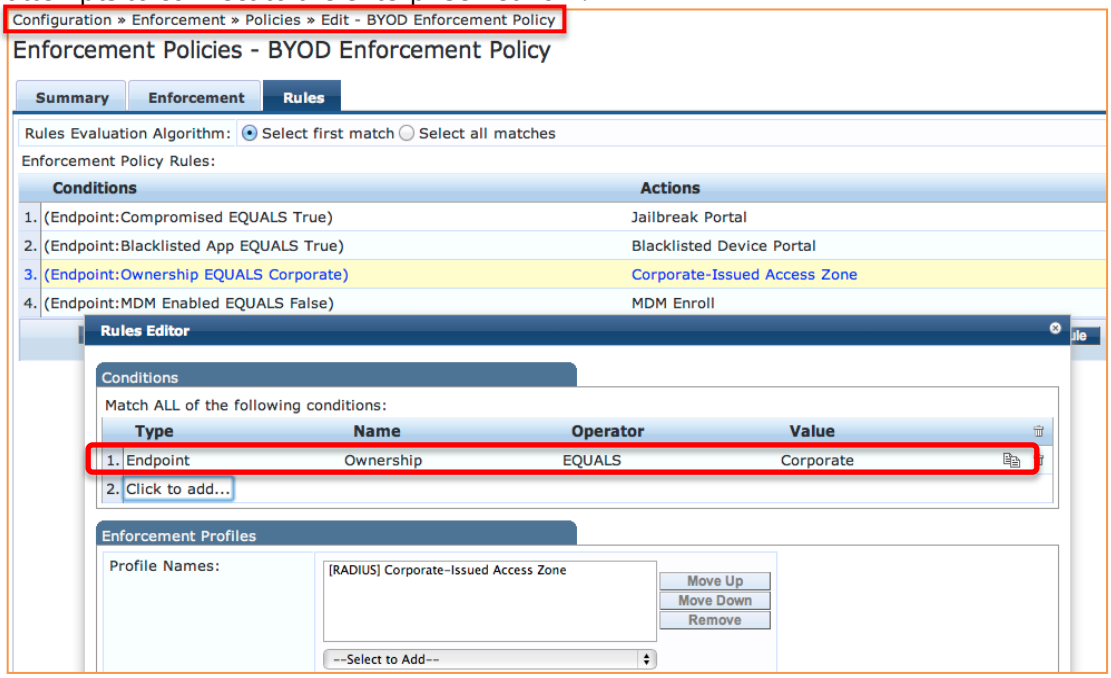


Figure 15: Enforcement Policy – Corporate device

In the event that this flag is set to Corporate by the configured EMM platform, then the network enforcement profile applied will result in the device being placed in the corporate access role which grants access to specific application servers and also enables a high level of Quality of Service (QoS) for these applications. Alternatively, if the flag is set to Employee, the network enforcement profile applied will restrict access to only essential internal resources and apply a best effort QoS profile for the user.

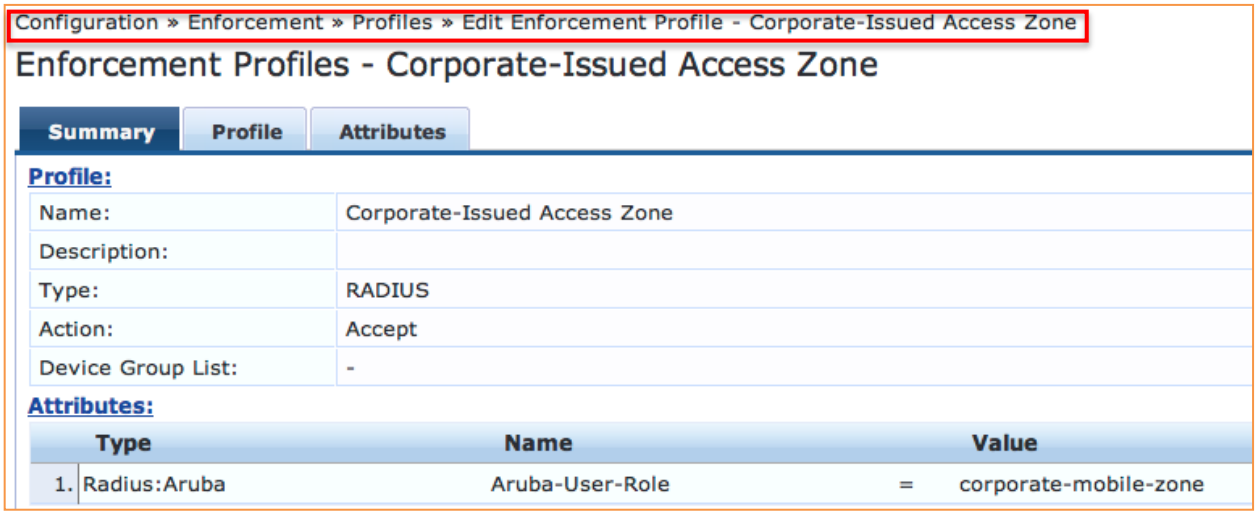


Figure 16 - Enforcement Profile – Corporate device

EMM Agent Removed

A common scenario in many EMM deployments occurs when a user either purposely (to avoid corporate monitoring) or by accident removes the EMM agent or profile from their device. This results in the device management communication channels being severed and the ability for the EMM platform to enforce policy to be become marginalized.

The ability for ClearPass to learn via the API integration that the device is no longer under management allows the administrator to differentiate this device the next time it attempts to access the enterprise network and redirect it back to the device management portal for re-provisioning.

The following enforcement policy example shows how the Endpoint *EMM Enabled* data tag is being referenced whenever a device attempts to connect to the enterprise network.

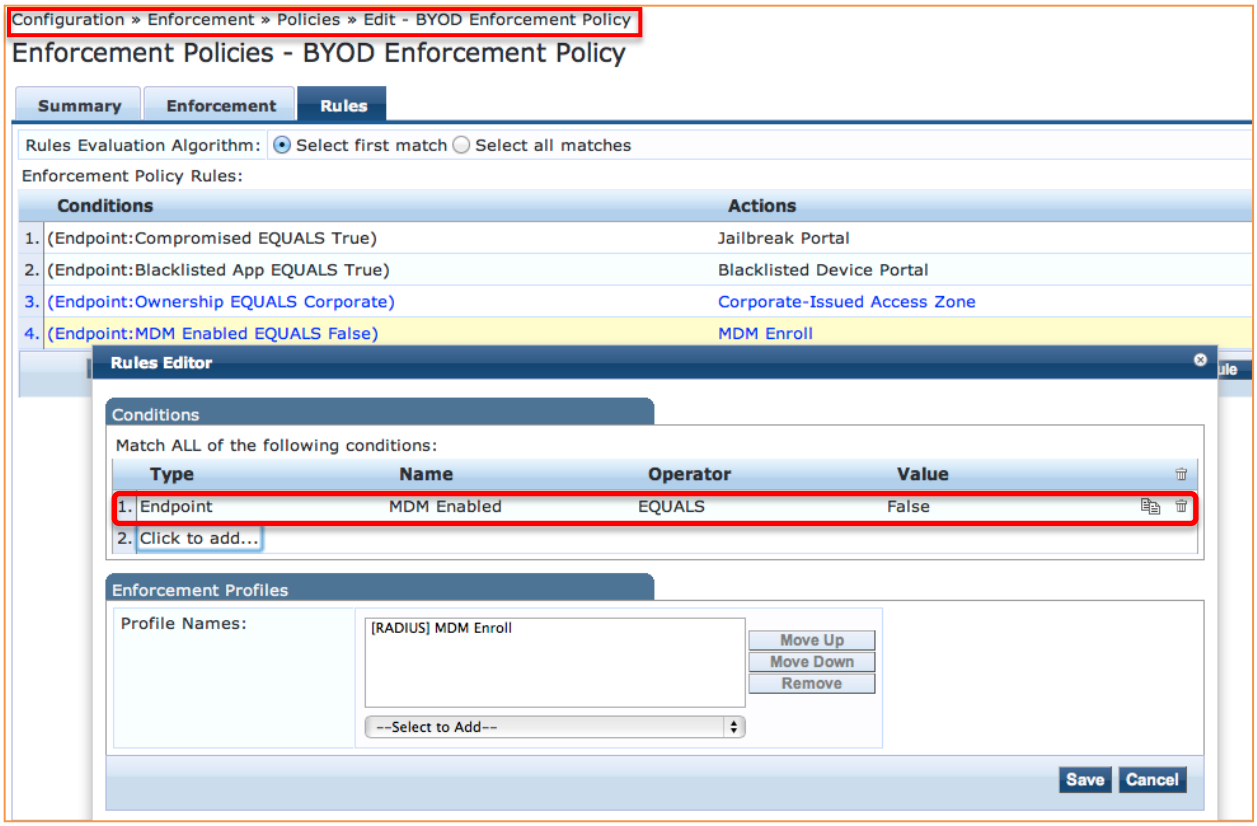


Figure 17 - BYOD enforcement – endpoint EMM managed

In the event that this flag is set to False by the configured EMM platform, then the network enforcement profile applied will result in the device being placed in a quarantine state and redirected to the device management provisioning page. This results in the user being forced to comply with the corporate policy and place the device back under management if they wish to access any corporate resources, without any manual intervention from the IT helpdesk staff.

Profile Data

The data retrieved from the EMM platform and stored in the Profile database table consists of a dataset made up of *Device Category*, *OS Family* and *Device Name* as shown in the screenshot below.

Hostname	AndroidSamsung 00086
MAC Vendor	Samsung Electronics
Category	SmartDevice
OS Family	Android
Device Name	Samsung-SGH-T679
Updated At	Dec 05, 2012 23:54:58 PST

Figure 18 - Profile database info

The inventory data available from the EMM platforms allows for explicit device type knowledge such as the Samsung device listed above. Alternatively, relying solely on passively collected network data would result in the device only being seen as a generic Android device manufactured by Samsung.

The following sample business rules included below illustrate how the EMM data included in the device Profile database can be used to enforce network policy decisions and control the way these devices are admitted onto the network.

iPad vs iPhone/iPod Network Access

Small screen devices are not always appropriate for the roll out of some corporate applications. For example, if a customer had deployed a corporate application that is designed to be accessed via a VDI solution such as Citrix Receiver, the administrator may wish to restrict use to iPad devices to take advantage of the larger screen. Having knowledge of the class of device as it connects to the network and being able to differentiate iPads allows the administrator to open up access to the Citrix server farm and potentially provide differentiated QoS for the Citrix ICA traffic.

The following enforcement policy example shows how the Profiler *Model* attribute is being referenced whenever a device attempts to connect to the enterprise network.

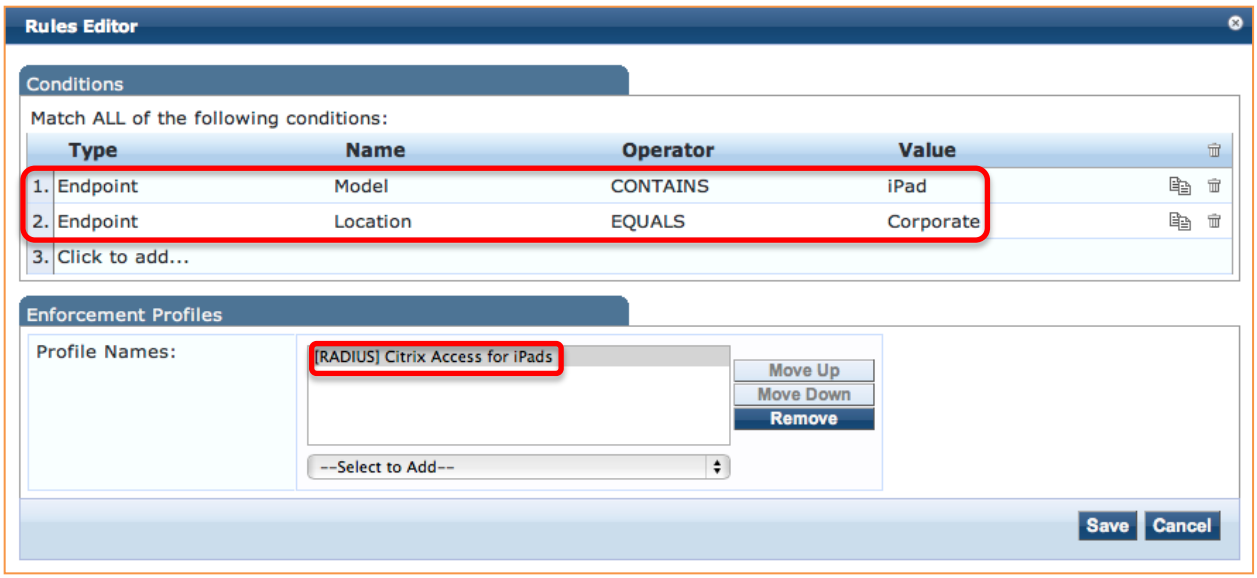


Figure 19 - Network Enforcement – Device Model type

In the event that this attribute contains a reference to iPad as configured by the EMM platform, then the network enforcement profile applied will result in the device being placed in the corporate access role which grants access to the Citrix application servers and also enables a high level of Quality of Service (QoS) for these applications. Alternatively, if this attribute does not include a reference to iPad as the device name, the network enforcement profile applied will restrict access to only essential internal resources and apply a best effort QoS profile.

Quarantine Device Type

It has become a regular occurrence that vulnerabilities are being discovered on smart phones and tablets. The open source nature of the Android operating system has provided a rich environment for potential vulnerabilities to be exposed and being able to classify devices at a granular level allows for administrators to quickly put in place quarantine rules in the event of a targeted exposure being discovered.

For example in early 2012, a vulnerability in a range of HTC smartphones was discovered where enterprise 802.1x credentials could be recovered from the operating system from a rouge application and potentially published remotely via standard Internet access.

Leveraging the EMM inventory data, ClearPass can clearly differentiate between Android devices from different manufacturers such as Samsung, HTC and Motorola and moreover leverage knowledge of individual model types of devices if such a granular policy is needed.

The following enforcement policy example shows how the Profiler *Device Name* attribute is being referenced whenever a device attempts to connect to the enterprise network.

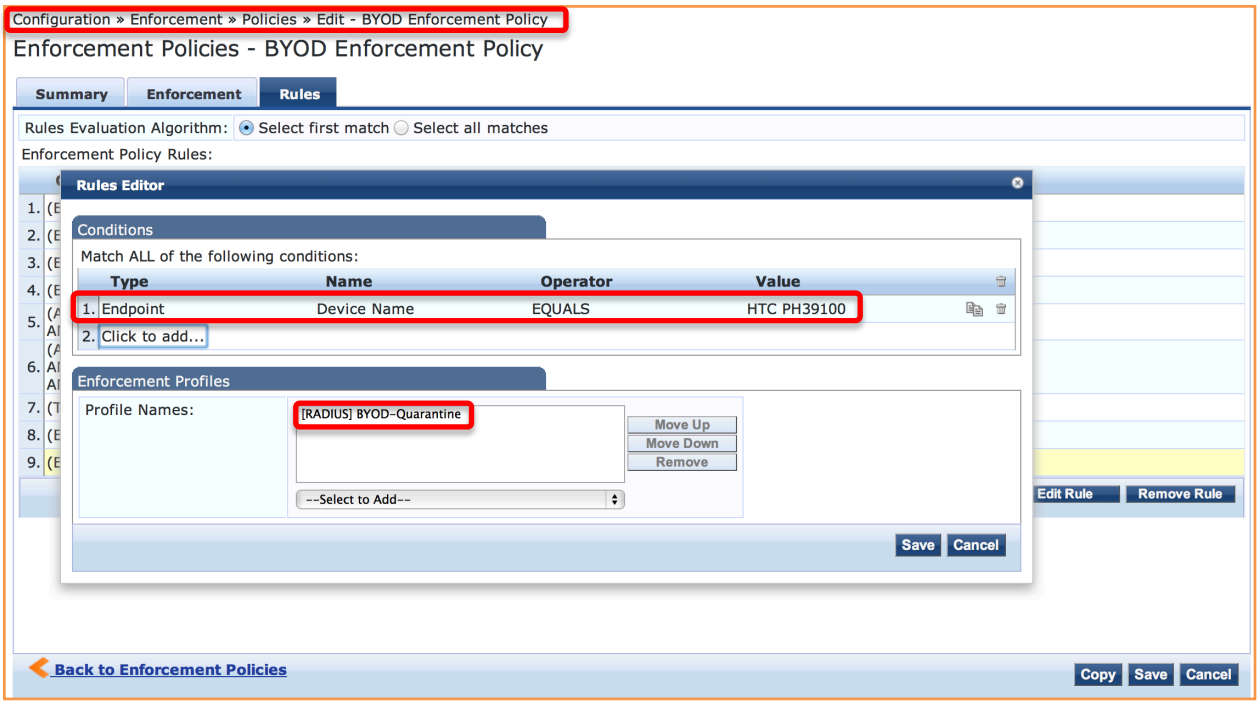


Figure 20 - Network Enforcement – device name

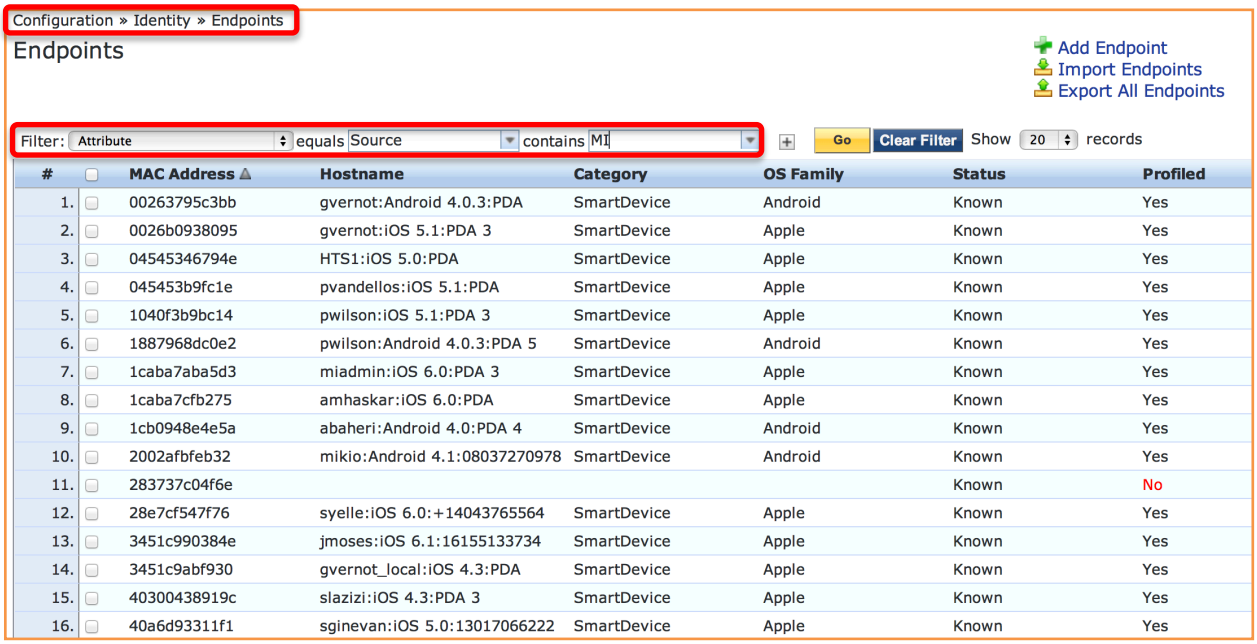
In the event that this attribute contains a reference to HTC as configured by EMM platform, then the network enforcement profile applied will result in the device being placed in a quarantine state and redirected to a captive portal page informing the user of the potential vulnerability on their device and advise on remediation steps via software upgrade. For more information on this vulnerability, please refer to the following article. http://www.kb.cert.org/vuls/id/763355

Managing Endpoint Data

The data received from EMM vendors is normalized and stored into the Endpoint database can be accessed from the **ClearPass Configuration > Identity > Endpoints** menu option.

Using the Endpoint information in the Endpoint Database you can query the ingested endpoint information using the following options.

Note: A filter can be created within the Endpoint database to restrict the view of endpoints to only those populated via the selected/preferred EMM platforms.



#	MAC Address	Hostname	Category	OS Family	Status	Profiled
1.	00263795c3bb	gvernot:Android 4.0.3:PDA	SmartDevice	Android	Known	Yes
2.	0026b0938095	gvernot:iOS 5.1:PDA 3	SmartDevice	Apple	Known	Yes
3.	04545346794e	HTS1:iOS 5.0:PDA	SmartDevice	Apple	Known	Yes
4.	045453b9fc1e	pvandellos:iOS 5.1:PDA	SmartDevice	Apple	Known	Yes
5.	1040f3b9bc14	pwilson:iOS 5.1:PDA 3	SmartDevice	Apple	Known	Yes
6.	1887968dc0e2	pwilson:Android 4.0.3:PDA 5	SmartDevice	Android	Known	Yes
7.	1caba7aba5d3	miadmin:iOS 6.0:PDA 3	SmartDevice	Apple	Known	Yes
8.	1caba7cfb275	amhaskar:iOS 6.0:PDA	SmartDevice	Apple	Known	Yes
9.	1cb0948e4e5a	abaheri:Android 4.0:PDA 4	SmartDevice	Android	Known	Yes
10.	2002afbfeb32	mikio:Android 4.1:08037270978	SmartDevice	Android	Known	Yes
11.	283737c04f6e				Known	No
12.	28e7cf547f76	syelle:iOS 6.0:+14043765564	SmartDevice	Apple	Known	Yes
13.	3451c990384e	jmoses:iOS 6.1:16155133734	SmartDevice	Apple	Known	Yes
14.	3451c9abf930	gvernot_local:iOS 4.3:PDA	SmartDevice	Apple	Known	Yes
15.	40300438919c	slazizi:iOS 4.3:PDA 3	SmartDevice	Apple	Known	Yes
16.	40a6d93311f1	sginevan:iOS 5.0:13017066222	SmartDevice	Apple	Known	Yes

Figure 21 – Example of Endpoint device list

It's important you configure the Filter in the following fashion.

Filter = 'Attribute'

Equals = 'Source'

Contains = 'as shown in the table below'

Vendor	MaaS360
Use this value in the **Contains** field	MaaS360

IBM MaaS360 Configuration

To configure the MaaS360 connector, you will need a considerable amount of information. To start, enter a hostname into the "Server Name" field. This is typically **services.fiberlink.com**. You should not need to alter the "Server Base URL". See the following paragraph for an explanation of the additional values required.

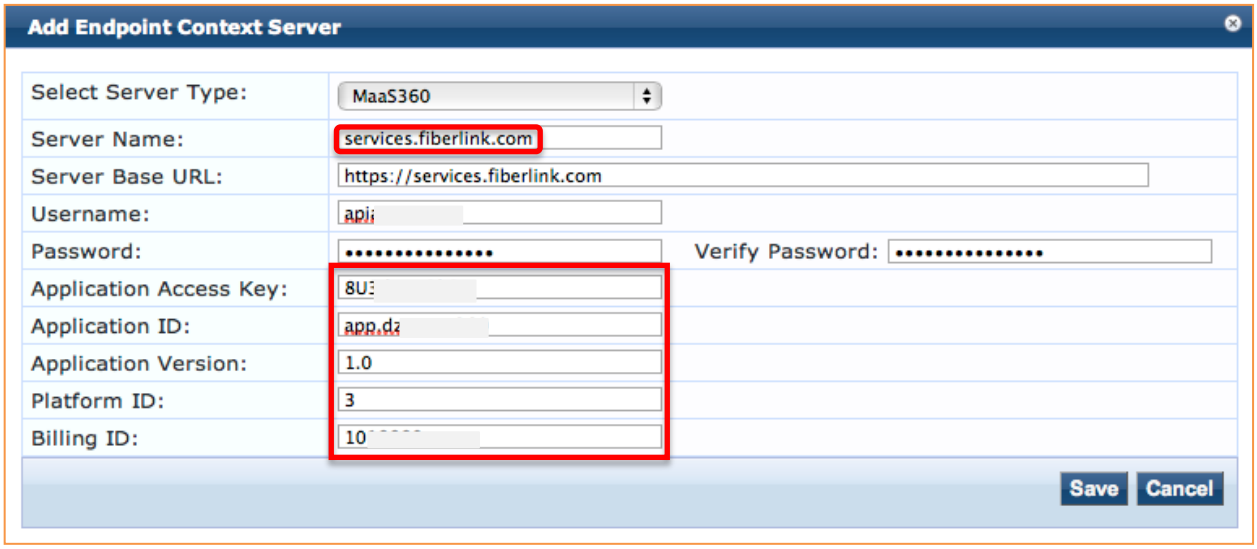


Figure 22 - MaaS360 Context Server configuration screen

MaaS360 utilizes multiple attributes over and above basic HTTP authentication as shown above. The following inputs will need to be configured inside of ClearPass.

Application Access Key: `<Obtained from MaaS360>`

App ID (for App authorized to use MaaS360 services): `<your-network-domain.com>`

App Version: **`1.0`**

Platform ID: **`3`**

Billing ID: **`<Your MaaS360 ID>`**

Most of the above details will be supplied by IBM, however your Billing ID is visible in the footer of your MaaS360 portal page (labeled Account #) as shown below.

MaaS360 Endpoint Attributes

The CPPM EMM service will normalize data received from MaaS360 in the Endpoint identity database. The table below shows the normalized data attributes that are available from MaaS360. If there are specific normalized values, those are also shown in the table.

Endpoint Tag	Tag Type	Specific Values
Manufacturer	Inventory	
Model	Inventory	
OS Version	Inventory	
Phone Number	Inventory	
Source	Inventory	MaaS360
Owner	Inventory	
UDID	Inventory	
IMEI	Inventory	
Display Name	Inventory	
Ownership	Inventory	
EMM Identifier	Inventory	
Last Check In	Policy	
Compromised	Policy	True or False
Blacklisted App	Policy	True or False
Required Apps	Policy	False/Installed/Missing
Encryption Enabled	Policy	True or False

Figure 23 - Maas360 Endpoints Attributes

Note: Not all endpoint attributes are available for all OS types.

CPPM & MDM/EMM SCEP Setup

This feature provides for a 3rd party gateway to send Simple Certificate Enrollment Protocol (SCEP) requests to the ClearPass Onboard CA to automate the enrollment provisioning process and leverage certificates for advanced user authentication. Primarily we have tested with EMM vendors as the SCEP client (Proxy).

CPPM SCEP Configuration

Configuring the SCEP Server functionality on CPPM is very simple. We are assuming you already have configured a Certificate Authority (CA) for Onboard. Initially when we added the proxy-enrollment process we provided for just SCEP based enrollment. We also support for Enrollment over Secure Transport (EST), a new comprehensive and more secure method of obtaining certificates than previous approaches, i.e. SCEP.

Figure 24 - Configuring SCEP & EST

Enable this within the Onboard CA **Guest -> Onboard -> Certificate Authorities**. Take special notice of the SCEP/EST URL that will be used on the SCEP/EST proxy server. Set a strong-shared SCEP/EST password.

EMM SCEP Configuration

Configuration within the EMM portals differs as vendors have differing frameworks and workflows. We will enhance this section as we document the workflows of other vendors.

Troubleshooting

Logging information regarding the Endpoint Context servers is available in the Event Viewer.

Go to **Monitoring > Event Viewer** You should see various messages relating to your configured EMM connectors.

Checking Logs files in CPPM

CPPM collects multiple log files that can assist the user in debugging CPPM's EMM integration problem. The most useful of these logs is the **mdm.log** file.

To collect and access this log file is slightly complicated and lengthy, follow these steps….

Under Administration -> Server Manager -> Server Configuration, select your system then '**Collect Logs'**. Once this process has completed you need to download this tar file and open with an appropriate application. For OS-X, **finder** will allow you to extract the file to a folder for analysis. For MSFT Windows multiple applications exist, but a really good free one is **7-Zip** http://www.7-zip.org.

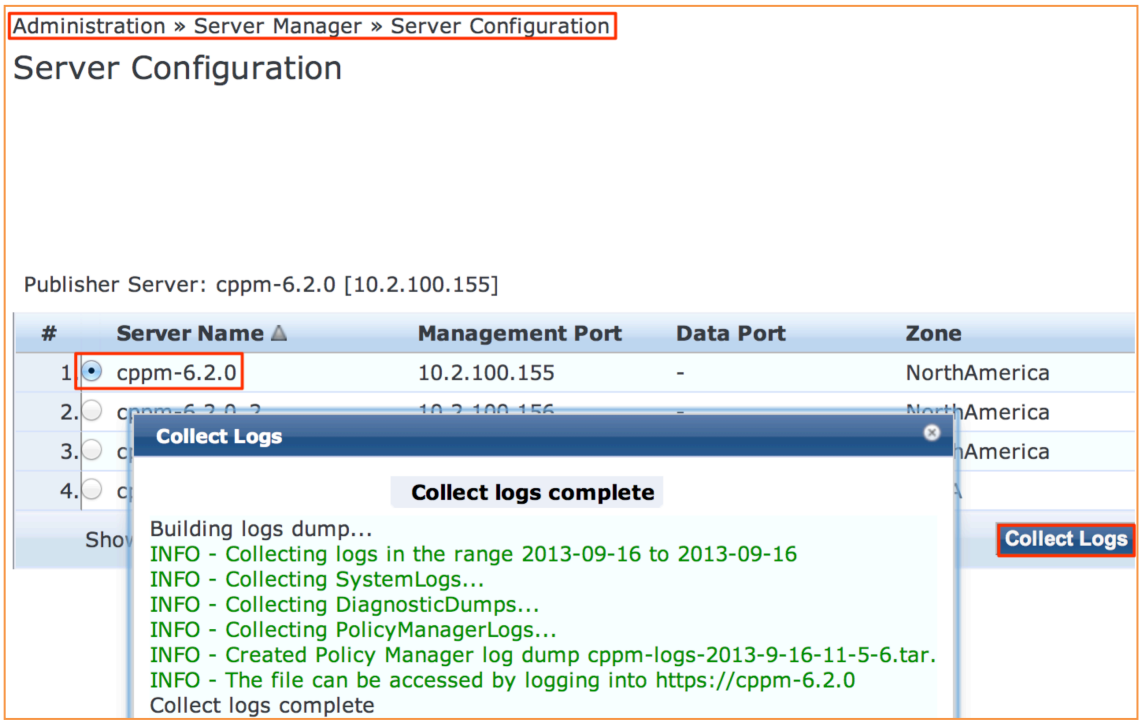


Figure 25 - How to collecting CPPM Logs

After you have opened the archive, the mdm.log file can be found in the following path…

PolicyManagerLogs/async-netd/mdm.log as shown below.

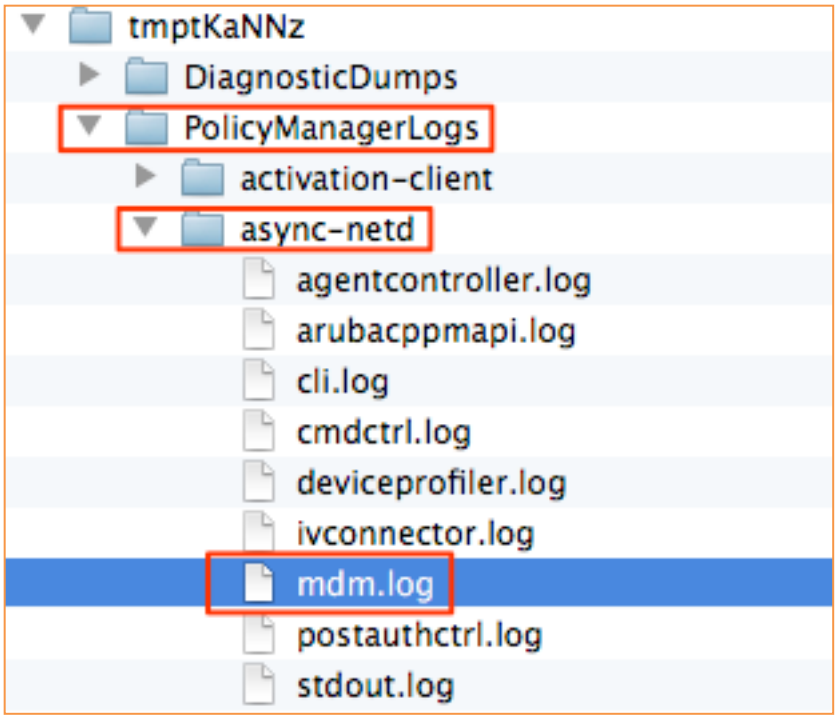


Figure 26 - Where to locate mdm.log file

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, CA 94089
Phone: 1-800-WIFI-LAN (+800-943-4526)

General SCEP/EST – Licensing – Q&A....

Anything you configure within the 'Onboard' menu that interact with a device for provisioning, will consume an 'onboard' license. That includes MSFT Active Directory Certificate Services and SCEP/EST server. Therefore EVERY issued certificate will consume and require a license in Onboard.

Caveats/Queries for CPPM SCEP/EST

SCEP/EST is **only** for TLS client certificates (and device identity certificates used for configuration profiles, an internal detail of iOS/OS X over-the-air provisioning).

Q) Is it programmable via API, i.e. Can we revoke certificates via API calls?

A) No, today we do not provide an API interface into the CPPM CA to revoke/disable certificate.

Q) If Onboard CA is being used only to issue certificates via SCEP/EST then how is Onboard expected to know the "device/user attributes"?

A) SCEP signs the certificate request and sends back the result as a certificate - Whatever is in the CSR should be part of the certificate. Onboard will honor the attributes presented in the CSR of a SCEP / EST request so it is critical to ensure that the EMM configured CSR meets your deployment requirements.