ClearPass
Integration with McAfee ePolicy Orchestrator
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1 &amp; 0.2</td>
<td>June 2016</td>
<td>Danny Jump</td>
<td>Draft Version feedback from R Filer / D Wilson</td>
</tr>
<tr>
<td>1.0</td>
<td>October 2016</td>
<td>Danny Jump</td>
<td>Initial Published version</td>
</tr>
<tr>
<td>2017-01</td>
<td>August 2017</td>
<td>Danny Jump</td>
<td>Updated to reflect security changes</td>
</tr>
</tbody>
</table>

Copyright

© Copyright 2017 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 ........................................................................................................................................... 7
Software Requirements ............................................................................................................................. 7
Installation and Deployment Guide .......................................................................................................... 7
Pictorial view of the Integration ................................................................................................................ 8
McAfee ePO Extension Installation ........................................................................................................ 8
  Create an Extension API Operator Profile ............................................................................................ 9
  Create an API Client ............................................................................................................................... 10
  Generate an Access Token ...................................................................................................................... 11
  Go to the Extension APIs ....................................................................................................................... 11
  Install the Extension .............................................................................................................................. 13
  Query the Extension after Installation ................................................................................................. 15
Managing and Configuring the McAfee ePO Extension ........................................................................... 17
  Starting the Extension ............................................................................................................................ 19
  Verify the Extension is Running ............................................................................................................ 19
  Configuring the Extension Password .................................................................................................... 20
  Troubleshooting the Extension ............................................................................................................. 21
Configuring ClearPass Policy Manager ................................................................................................ 21
  Add HTTP Authorization Source ......................................................................................................... 22
  Options for defining the Query String .................................................................................................. 23
Using results from ePO in an Enforcement Policy .................................................................................. 27
Installing the ClearPass Extension in McAfee’s ePolicy Orchestrator ..................................................... 28
  ePO Extension Installation .................................................................................................................... 28
  Utilizing the ePO Installed Permission set ............................................................................................ 29
  Un-Installing the ClearPass ePO Extension ......................................................................................... 32
  Using ePO Tags to drive Endpoint Enforcement ............................................................................... 32
Appendix A: EPOComputerProperties .................................................................................................. 36
  Field Descriptions ................................................................................................................................. 36
  Field Names ......................................................................................................................................... 37
Appendix B: AM_CustomProps .................................................................................................................. 38
  Field Descriptions ................................................................................................................................. 38
  Field Names ......................................................................................................................................... 39
Appendix C: GS_CustomProps .................................................................................................................. 40
  Field Descriptions ................................................................................................................................. 40
  Field Names ......................................................................................................................................... 41
Appendix D: FW_CustomProps .................................................................................................................. 42
Field Descriptions.................................................................................................................................................. 42
Field Names .......................................................................................................................................................... 43
Appendix E: WP_CustomProps .................................................................................................................................. 44
  Field Descriptions .................................................................................................................................................. 44
  Field Names .......................................................................................................................................................... 45
Appendix F – Authorization Source XML Configuration File .................................................................................. 46
Appendix G – Additional Diagnostics & Support ..................................................................................................... 47
  Extension Service .................................................................................................................................................. 47
  Extension Logs/Debugging .................................................................................................................................... 47
  Accessing Extension logs within ClearPass ‘Collect Logs’ ...................................................................................... 49
Figures

Figure 1: Pictorial view of ClearPass Policy Manager integration with McAfee ePO ............................................................... 8
Figure 2: Duplicate API Guest Operator profile .......................................................................................................................... 9
Figure 3: Modifying Operator Profile permissions for extensions .................................................................................................. 9
Figure 4: Creating your API client ................................................................................................................................................. 10
Figure 5: Generate the Access Token ........................................................................................................................................... 11
Figure 6: API Explorer UI ............................................................................................................................................................... 11
Figure 7: Accessing the Store API ................................................................................................................................................. 12
Figure 8: Checking in the Extension store for a particular Extension ID .......................................................................................... 12
Figure 9: Details of the Extension .................................................................................................................................................... 13
Figure 10: Installing the Extension directly from the Extension store ......................................................................................... 14
Figure 11: Checking the Extension Installation Status .................................................................................................................. 15
Figure 12: Checking Extension Installation Progress .................................................................................................................... 16
Figure 13: Response to check on progress of Extension installation .............................................................................................. 16
Figure 14: Get Extension configuration ......................................................................................................................................... 17
Figure 15: Response to a request for the Extension configuration ................................................................................................ 17
Figure 16: Setting the Extension configuration .............................................................................................................................. 18
Figure 17: HTTP 204 response to the configuration PUT ............................................................................................................... 18
Figure 18: Example of JSON formatted payload .......................................................................................................................... 18
Figure 19: Starting the Extension ..................................................................................................................................................... 19
Figure 20: Detailed information on the running Extension ........................................................................................................... 20
Figure 21: Setting the ePO Extension password ............................................................................................................................ 20
Figure 22: Example of the response from the Extension after setting the password ................................................................. 21
Figure 23: Getting Debug Logs from the Extension .......................................................................................................................... 21
Figure 24: Adding an HTTP authZ source ...................................................................................................................................... 22
Figure 25: Adding HTTP authorization source credentials .......................................................................................................... 22
Figure 26: Adding HTTP authorization source query string and returned field definitions ....................................................... 24
Figure 27: A larger list of multiple queries and fields definitions .................................................................................................. 26
Figure 28: Example of an Enforcement Policy utilizing attributes returned from ePO ................................................................. 27
Figure 29: ePO Extension Installation .............................................................................................................................................. 28
Figure 30: Select the location of the Aruba ClearPass Extension ZIP ............................................................................................ 28
Figure 31: Final installation confirmation ....................................................................................................................................... 29
Figure 32: Checking status of the ePO Extension installation .................................................................................................... 29
Figure 33: Defining the Permission set authorities .......................................................................................................................... 30
Figure 34: Creating a new user in ePO ............................................................................................................................................ 31
Figure 35: Creating a user and assigning the permission set ......................................................................................................... 31
Figure 36: ePO Extension Removal .................................................................................................................................................. 32
Figure 37: ePO Extension Removal – Confirmation .......................................................................................................................... 32
Figure 38: Creating Tags in ePO console ........................................................................................................................................ 33
Figure 39: Endpoints with Infected Tag .......................................................................................................................................... 33
Figure 40: Authorization attributes and ePO TAGS received .......................................................................................................... 34
Figure 41: CPPM assigning epo-infected-role .................................................................................................................................. 34
Figure 42: Enforcement Policy for infected device Tag ................................................................................................................... 35
Figure 43: Enforcement Profile - Sending an Aruba-User-Role via RADIUS to network .................................................................. 35
Figure 44: Checking on Extension service and how to start/stop the service ............................................................ 47
Figure 45: Turning on Debug logging on an Extension ........................................................................................................ 48
Figure 46: Accessing Logs in an extension from API Explorer UI .................................................................................... 48
Figure 47: An example of the logs from the extension in the API Explorer UI ................................................................. 49
Figure 48: Extension logs location in 'Collect Logs' diagnostic GZ file ............................................................................ 49
Introduction

This TechNote covers the setup, configuration, and monitoring of the McAfee ePolicy Orchestrator [ePO] ClearPass Extension within ClearPass Policy Manager [CPPM]. ClearPass Extensions are micro-services running on top of the base CPPM platform. These micro-services enable Aruba to deliver new features outside of the main software release cycle, facilitating a faster time to market for specific features. Configuration and control of ClearPass Extensions is accomplished through the CPPM REST API. Prior to accessing the APIs, you need to complete some pre-configuration, which is covered in the Installation, Configuration and Setup section below.

Installation of the ePO ClearPass Extension is performed via the REST API interface. ClearPass REST APIs were initially introduced in CPPM 6.5 and have continued to be enhanced. Access to the APIs is through the following URL https://<ClearPass_IP>/api-docs. You have to provide Admin credentials as usual to access the API interface. Note: the APIs to support ClearPass Extensions were released in CPPM 6.6.

Software Requirements

The minimum software version required for CPPM is 6.6.0. At the time of writing, version 6.6.7 is available and is the recommended release. CPPM runs on 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 5.0, 5.1, 5.5, 6.0, or higher
- Microsoft Hyper-V Server 2012 R2
- Hyper-V on Microsoft Windows Server 2012 R2

McAfee ePolicy Orchestrator must be version 5.3 or later. The McAfee approved Product ID for the CPPM integration is referred to as S_CPPM6600.

Installation and Deployment Guide

The ClearPass installation and deployment guide is located here: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Default.htm#1%20About%20ClearPass/Intro_ClearPass.htm%3FTocPath%3D1%2520About%2520ClearPass%7C0
**Pictorial view of the Integration**

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

**Figure 1: Pictorial view of ClearPass Policy Manager integration with McAfee ePO**

![Diagram showing integration of ClearPass and McAfee ePO](image)

**McAfee ePO Extension Installation**

Installation of the McAfee ePO ClearPass Extension is performed via the REST API interface. ClearPass REST APIs were initially introduced in CPPM 6.5 and have continued to be enhanced in subsequent releases. Access to the APIs is through the following URL `https://<ClearPass_IP>/api-docs`. Admin credentials are required to access the API interface.

The APIs to support ClearPass Extensions were initially released in ClearPass version 6.6.

Several components, and multiple steps, are required to complete the ClearPass configuration:

- Extension Installation and Configuration
- Policy Manager HTTP authorization source
- Policy Manager Enforcement Policy and Profiles

The ClearPass extension installation is shown below. Follow these steps to enable the extension to communicate with McAfee ePO.
Create an Extension API Operator Profile

Before setting up the API access, you must configure an Operator Profile that will be associated with the configured API client. This new Operator Profile will be used in the next section when creating the API Client. Login to Guest and go to Administration > Operator Logins > Profiles. Next, Click on API Guest Operator and select Duplicate.

Figure 2: Duplicate API Guest Operator profile

ClearPass will copy the profile and name it API Guest Operator (2). Click Edit on the new profile and rename it to be API Extension Profile. For the Platform privilege, change No Access to Custom and then set all the Extension options as shown below (furthest option to the right). Scroll to the bottom of the page and click Save.

Figure 3: Modifying Operator Profile permissions for extensions

In the next step, this profile will be used as the Operator Profile when generating the API Client.
Create an API Client

The next step in installing and enabling the McAfee ePO ClearPass Extension is to create an API Client. An API client provides authentication and authorization for the REST APIs. Authentication is performed using OAuth2, which is an authorization framework that enables applications to obtain limited access to data over a HTTP service without sharing their private credentials. Log into ClearPass Guest at https://<ClearPass_IP>/guest.

Navigate to Guest > Administration > API Services > API Clients and create an API client by entering the following:

1. **Client ID**: Your choice
2. **Operator Profile**: API Extension Profile [just created]
3. **Grant Type**: Client credentials

*Figure 4: Creating your API client*

Click on Create API Client to save and create the API Client.
Generate an Access Token

Click **Generate Access Token** and then launch the **API Explorer**, as highlighted at the bottom of the image.

*Figure 5: Generate the Access Token*

This will pre-populate the Authorization header in the API Explorer and permit commands to be run directly from the ClearPass UI.

**Go to the Extension APIs**

Next check whether ClearPass can communicate with the Extension store. This is an important step to ensure that Proxy-Servers and/or Firewalls are not blocking connectivity to the ClearPass Extension Store. Click on **Extension > Store**.

*Figure 6: API Explorer UI*

Under Store, click on **GET /extension/store/{id}**
Notice that the Authorization header is populated. This is populated from creating the token in the previous step. Next expand the **GET /extension/store/{id}** and paste in the extension's store ID. The store ID for this McAfee ePO extension is a fixed value of: 4aaac613-7f4d-4d11-a807-803ddd657d4c.

Click on **Try it out!**.

Remember that the store ID 4aaac613-7f4d-4d11-a807-803ddd657d4c is unique to this version of the McAfee ePO Extension. The store ID will change if new versions of the Extension are published.
This will return details for the McAfee ePO Extension. This provides assurance that the correct authority is configured to allow access to the Store, and that this is the correct ID for the extension being installed.

**Figure 9: Details of the Extension**

**Install the Extension**

Prior to installing this extension, note that if a previous McAfee ePO extension is running then consider when you will migrate from the previous extension to the new. The new extension can be installed and configured independently of the old extension. When started, depending on if the previous extension is still deployed the new extension might use the same or a new IP address. The recommendation is to migrate to the new extension in a period of scheduled down-time. Stop the old extension, delete it then install the new extension, configure it and finally start it. If appropriate adjust the HTTP Authorization source in Policy Manager to use the IP address of the new extension.

After checking for extension visibility, the next step is to install it. Under **Instance > POST /extension/instance**, paste in the body as shown below:

```
{"state":"stopped", "store_id":"4aaac613-7f4d-4d11-a807-803ddd657d4c"}
```

And then click on **Try it out!**.
**Figure 10: Installing the Extension directly from the Extension store**

This will return an ID (Note: this is different from the store ID. It will be referred to as the run-time ID). Make a copy of this ID as it will be required later.

The below shows the state of the Extension as **preparing**. This indicates the extension is in the process of being downloaded. A typical installation should take just a few seconds to complete.
From the above, you can see the ID is **0922e27a-4494-4ee8-8927-420c29aa4185**. This ID (the run-time ID) will be used to query and configure the extension.

Your run-time ID will be different from the one used here. It is generated per installation and is unique to each installation.

### Query the Extension after Installation

Under **Instance > GET /extension/instance/{id}**, paste in the run-time ID from the previous step: **0922e27a-4494-4ee8-8927-420c29aa4185** and then click on **Try it out!**. Remember your runtime ID will be different.
Within the Body Response from this GET you should observe the following:

**Figure 13: Response to check on progress of Extension installation**

```json
{
  "id": "0922e27a-4494-4ee8-8927-420c29ab4185",
  "state": "stopped",
  "state_details": "Created",
  "store_id": "4aaaac513-7f4d-4d11-a807-803dd657d4c",
  "name": "McAfee-epo-pwd",
  "version": "1.0.0",
  "description": "McAfee ePolicy Orchestrator Integration – Password Update",
  "icon_href": "https://www.mcafee.com/microsites/mcafee-brand/img/logo.png",
  "hostname": "835b415c8d16",
  "network_ports": [],
  "extension_hrefs": [],
  "files": [],
  "_links": {
    "self": {
      "href": "https://10.2.100.160/api/extension/instance/0922e27a-4494-4ee8-8927-420c29ab4185"
    }
  }
}
```

The details of the extension will be displayed (could be **downloading**, etc.). Eventually the state will change to either **stopped** or **failed**. In this example, it is clear that the extension is **Created** and **stopped**.
Managing and Configuring the McAfee ePO Extension

To complete the configuration of the McAfee ePO extension, there are a number of parameters which need to be collected and then set. Below is the default configuration shipped with the extension.

Under **InstanceConfig > GET /extension/instance/{id}/config**, paste in the run-time ID **0922e27a-4494-4ee8-8927-420c29aa4185** and Click on **Try it out**. This returns a copy of the current default configuration.

**Figure 14: Get Extension configuration**

![Example screenshot of the Get Extension configuration](image)

**Figure 15: Response to a request for the Extension configuration**

```
"ePoHost": "Your_ePO_Server_IP_Address",
"ePoPort": 8443,
"ePoAdminUser": "admin.user",
"verifySSLCerts": true,
"logLevel": "INFO"
```

The above default configuration will need to be changed to match your environment. There are several configuration parameters that must be changed from the default shipped configuration.

- **ePoHost**: the McAfee ePolicy Orchestrator destination Server IP address
- **ePoPort**: the TCP port used
- **ePoAdminUser**: the Admin account

These will be used to communicate between the ClearPass Extension and the ePO Server and must be configured. Unless instructed by Aruba TAC, leave the **logLevel** and **verifySSLCerts** as default values.

---

**Note**: There is NO ePO Password configured here for the ePOAdminUser. This is configured later on Page 20. The matching ePoAdminUser account and its credentials must be created within the McAfee ePO console.
To set the configuration under **InstanceConfig > PUT /extension/instance/{id}/config**, copy and paste the run time ID and configuration settings to the PUT method. Adjust settings as required. Click on **Try it out!**.

**Figure 16: Setting the Extension configuration**

![Setting the Extension configuration](Image)

If you change the extension configuration, **InstanceRestart > POST /extension/instance/{id}/restart**

Below is the Response to the **PUT**. A successful result is indicated by a **No Content 204**.

**Figure 17: HTTP 204 response to the configuration PUT**

![HTTP 204 response to the configuration PUT](Image)

It's important to ensure you format the body correctly when configuring the Extension. Below is the example used in the configuration.

**Figure 18: Example of JSON formatted payload**

```json
{
    "ePoHost": "IP_of_my_ePO-Server",
    "ePoPort": "8443",
    "ePoAdminUser": "test_user",
    "verifySSLCerts": true,
    "logLevel": "INFO"
}
```
As previously noted the `ePOAdminUser` needs to match a user account in McAfee ePO. Using the default Admin account is not recommended. We recommend creating a dedicated account that will be used to communicate with ClearPass Policy Manager and is assigned to the permission set where the ‘Aruba ClearPass’ permission control is defined.

From the above configuration, you may have noticed that no password is configured. The password is configured later on Page20 in a secure way such that it can't be exposed or seen. Note that to set the password for the `ePOAdminUser` requires the extension to be running.

**Starting the Extension**

Under **InstanceStart > POST /extension/instance/{id}/start** enter the run-time ID and click on **Try it out!**.

*Figure 19: Starting the Extension*

A successful result is indicated by a **204 No Content** result as shown below.

**Verify the Extension is Running**

Under **Instance > GET /extension/instance/{id}** copy and paste the extension ID and click on **Try it out!**. The extension should be **running**. An example of the HTTP response is shown below:
**Figure 20: Detailed information on the running Extension**

```
"id": "ab8402a9-50b3-4cd3-b578-ad6ace2d2ebf",
"state": "running",
"state_details": "Started 1 day ago",
"store_id": "4aaaac613-7f4d-4111-a807-803dd7657d4c",
"name": "mcafee-ePO-pwd",
"version": "1.0.0",
"description": "McAfee ePolicy Orchestrator Integration - Password Update",
"icon_href": "https://www.mcafee.com/microsites/mcafee-brand/img/logo.png",
"hostname": "b8e9a7b74a1",
"network_ports": [],
"extension_hrefs": [
  {
    "href": "/extension/ab8402a9-50b3-4cd3-b578-ad6ace2d2ebf/password/",
    "description": "Set the hidden password here."
  }
],
"internal_ip_address": "172.17.0.5",
"_links": {
  "self": {
  }
}
```

Note the "internal_ip_address" of the extension. Use this for configuring the authZ source in ClearPass.

**Configuring the Extension Password**

Once the extension is running, the next step is to set the password used by the ClearPass extension to authenticate itself against the McAfee ePO system. Use the following url format to access the password configuration portal `https://<ClearPass_IP>/extension/runtime_ID/password`

From the above figure, use the ID, referred to as the runtime_ID [yours will be different] as in the below example.

E.g. `https://10.1.2.3/extension/ab8402a9-50b3-4cd3-b578-ad6ace2d2ebf/password`

**Figure 21: Setting the ePO Extension password**

![Update ePO Password](image)

Enter the password to match the **ePoAdminUser** account created in McAfee ePO and click on **Save**... the expected response is shown below.
Figure 22: Example of the response from the Extension after setting the password.

```
[Image: Screenshot showing a window with the text 'Saving Settings... The password was set. ']
```

Please note that the password cannot be retrieved, it can only be set.

**Troubleshooting the Extension**

Under **InstanceLog > GET /extension/instance/{id}/log**, paste in the run-time ID. Enter a value for **tail**, e.g. 100 will show the last 100 lines of logs, then click on **Try it out!**. Note that other settings are applicable when getting logs, e.g. timestamps.

Figure 23: Getting Debug Logs from the Extension.

---

**Configuring ClearPass Policy Manager**

Following the deployment and configuration of the ClearPass Extension, the next step is to configure an authorization source within ClearPass. At this stage of the integration, McAfee ePO is treated as an authorization source for authenticating endpoints. Multiple use-cases exist, such as:

- Ensuring that the endpoint is enrolled and managed by ePO
- Using context such as the installed operating system version to make enforcement decisions
- Looking at the compliance state returned from the McAfee Endpoint Security agent to ensure the Threat Detection is compliant & that the scan has perhaps run in the last 24-hours
- Using the ePO LABELS to decide on the access policies that can be applied to this device
These, and other context items of data can be used to evaluate the suitability of an endpoint at the time of network authentication to help drive the access policy for the device and the user behind the device.

**Add HTTP Authorization Source**

The first step is to add the authorization source. Under **Configuration -> Authentication -> Sources**, Click **Add** and choose type **HTTP**.

*Figure 24: Adding an HTTP authZ source*

Provide a **Name** for the Authentication Source and click **Next**. On the **Primary** Tab, provide the **IP Address** in the Base URL using the **internal_ip_address** of the extension you recorded previously.

The **Login Username/Password** below can be set to ANYTHING, they are not used, but must be set.

*Figure 25: Adding HTTP authorization source credentials*
Options for defining the Query String

It's extremely important that the Filter Query be defined correctly. This query string is sent to the McAfee ePO system requesting context about the endpoint, based upon the MAC Address of the authenticating endpoint. The modules installed in ePO and deployed to the endpoints will determine the query string that can be sent to ePO, but more importantly the context that can be returned about the endpoint.

For the basic Computer context and ePO labels the below query is required:

?macAddress=%{Connection:Client-Mac-Address-NoDelim}&joinTable=EPOComputerProperties

The table below lists additional or optional query string that can be used. You can use one or more of the below Attributes depending on the data you want to return and expose within the Enforcement Policy.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPOComputerProperties</td>
<td>Basic query string for endpoint attributes and labels</td>
<td>See Appendix A</td>
</tr>
<tr>
<td>AM_CustomProps</td>
<td>Add this to query for OnDemand Scan Threat &amp; Exploit Prevention.</td>
<td>See Appendix B</td>
</tr>
<tr>
<td>GS_CustomProps</td>
<td>Add this to query data about the General Security context.</td>
<td>See Appendix C</td>
</tr>
<tr>
<td>FW_CustomProps</td>
<td>Add this to query data about the Firewall.</td>
<td>See Appendix D</td>
</tr>
<tr>
<td>WP_CustomProps</td>
<td>Add this to query data about Web Control and browser plugin etc.</td>
<td>See Appendix E</td>
</tr>
</tbody>
</table>

The query string can be any single string [EPOComputerProperties context is ALWAYS returned, even is the query was ?macAddress=%{Connection:Client-Mac-Address-NoDelim}&joinTable=FW_CustomProps] from the above table or other additional query attributes can be added to have the Extension return additional endpoint context. As an example, if context is required about the settings/posture of the Firewall in addition to the basic Computer Properties, then query string would look like this:

?macAddress=%{Connection:Client-Mac-Address-NoDelim}&joinTable=EPOComputerProperties,FW_CustomProps

The data returned from ePO can be extensive, and depending on the query used, varying additional amounts of context will be returned. Not all the data is relevant to making a security policy decision about the endpoint. Carefully choose which attributes are required within your enforcement profile using the information in the Appendices to define the necessary fields. As an example, the filter shown below has the ePO Computer Properties fields. Yours may well differ depending on the use-cases you are trying to meet and the data being queried.

Note that isFound is added by the extension to indicate if the endpoint was or wasn't found in ePO.
Next build the definitions of the attributes that will be returned from the Filter Query. These attributes will subsequently be used within the policy evaluation and ultimately the enforcement policy that will be applied. If additional fields are required to make different authorization checks, then they will need to be defined. Once the filter is defined, click Save. The queries can also be defined separately if required as shown on the next page, but its more efficient to have a single query definition. Note the above is just a small sample of the available fields. Below is a larger sample and shows a number of fields from different queries. As documented above the full list of the fields are documented in the Appendices, but the vast majority will likely not be needed. Here is a list of some important fields found in the Appendices.

These below fields are ‘summary’ fields indicating if the endpoint security feature is enabled or not.

- **bOASEnabled**: Enable On-Access Scan
- **bAPEnabled**: Access Protection Enabled
- **bBOEnabled**: Enable Exploit Prevention
- **bScriptScanEnabled**: Enable ScriptScan

**On-access scan** — The administrator configures on-access scans to run on managed computers. For self-managed computers, configure the on-access scanner in the Settings page. Whenever files, folders, and programs are accessed, the on-access scanner intercepts the operation and scans the item, based on criteria defined in the settings.

- **OASbComplianceStatus**: On-Access Scan Compliance Status
- **OASComplianceStatus**: On-Access Scan Reason
- **OASAdditionalComplianceStatus**: On-Access Scan Additional Reason
**On-demand scan** — The administrator (or user, for self-managed systems) configures predefined or custom on-demand scans that users can run on managed computers.

- **ODSbComplianceStatus**: On-Demand Scan Compliance Status
- **ODSComplianceStatus**: On-Demand Scan Reason
- **ODSAdditionalComplianceStatus**: On-Demand Scan Additional Reasons

**AMCore** — Engine and content contains updates to the Threat Prevention scan engine and signatures based on results of ongoing threat research.

- **AVCMGRbComplianceStatus**: AMCore Content Compliance Status
- **AVCMGRComplianceStatus**: AMCore Content Reason
- **AVCMGRAdditionalComplianceStatus**: AMCore Content Additional Reasons

**Threat Prevention** — Exploit Prevention, enable and configure Exploit Prevention to keep buffer overflow exploits from executing arbitrary code on your computer.

- **BObComplianceStatus**: Exploit Prevention Compliance Status
- **BOComplianceStatus**: Exploit Prevention Reason
- **BOAdditionalComplianceStatus**: Exploit Prevention Additional Reasons

**Enables scanning JavaScript and VBScript scripts** in Internet Explorer to prevent unwanted scripts from executing.

- **SSbComplianceStatus**: ScriptScan Compliance Status
- **SSComplianceStatus**: ScriptScan Reason
- **SSAdditionalComplianceStatus**: ScriptScan Additional Reasons

**Access Protection** prevents unwanted changes to your computer by restricting access to specified ports, files and folders, shares, and registry keys and values. It prevents users from stopping McAfee processes and services, which are critical before and during outbreaks.

- **APbComplianceStatus**: Access Protection Compliance Status
- **APComplianceStatus**: Access Protection Reason
- **APAdditionalComplianceStatus**: Access Protection Additional Reasons

The outcome of the following fields is an integer of either 0=Non-compliant or 1=Compliant.

- **OASbComplianceStatus**
- **ODSbComplianceStatus**
- **AVCMGRbComplianceStatus**
- **BObComplianceStatus**
- **APbComplianceStatus**
- **SSbComplianceStatus**
If you define multiple queries as shown above then correspondingly you will define multiple query strings.

It's a more resource friendly to add all the fields required in a single Filter Name definition with a single query.

Once the HTTP authorization source is defined, the returned attributes can be used in your policy processing. Below are some examples of how to use the results from the authorization query in a simple enforcement policy. As an example you could also define multiple queries strings on a single line, an example is shown below. Notice how we have added the additional query-string parameters simply separated by a comma.

?macAddress=%{Connection:Client-Mac-Address-NoDelim}&joinTable=EPOComputerProperties,AM_CustomProps,FW_CustomProps,GS_CustomProps
Using results from ePO in an Enforcement Policy

Multiple use-cases exist for how the data returned from ePO can be used in your policy-enforcement. The example below shows multiple checks being performed:

Figure 28: Example of an Enforcement Policy utilizing attributes returned from ePO

This is a very short list of example use-cases. In Appendix A thru F is a list of returned attributes from ePO. ClearPass can easily be manipulated to use any of the endpoint context in this list to drive enforcement actions for an endpoint.
Installing the ClearPass Extension in McAfee’s ePolicy Orchestrator

McAfee ePolicy Orchestrator [ePO] supports the concept of installing extensions to add value via 3rd party integration. The integration with ClearPass Policy Manager requires an extension be installed in the ePO console. You can download the ClearPass Extension from the Aruba Support site. Go to the following URL https://support.arubanetworks.com/DownloadSoftware/tabid/75/DMXModule/510/Default.aspx?EntryId=22853 (Download Software/ClearPass/Tools/Extensions)

Support credentials are required to access the McAfee ePO extension from the arubanetworks support site. Download the ePO extension to your local computer, from there upload it into the ePO console.

Note that both McAfee and Aruba use the term ‘extension’ to refer to a similar s/w feature for our own products. However, it’s important to understand the ClearPass extension can only be downloaded and installed from the ClearPass App store via the API’s made available under the 6.6 Extension framework. The ePO extension must be downloaded from the Aruba support site and uploaded into the ePO console.

Note that McAfee does not distribute 3rd party extensions.

ePO Extension Installation

Sign-in to the ePO Console, then from the navigation tab click on Software > Extensions and install the package from ‘Install Extension’ as shown below using an admin level account with the appropriate permission set [authority] to complete the software installation.

Select the ZIP file as shown below and click OK.

*Figure 29: ePO Extension Installation*

Select the software ZIP file from your local directory where you have the file saved.

*Figure 30: Select the location of the Aruba ClearPass Extension ZIP*
One final confirmation that this is the software you want to install is shown, click **OK** and proceed.

**Figure 31: Final installation confirmation**

<table>
<thead>
<tr>
<th>Software</th>
<th>Extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Install Extension</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name:</strong></td>
<td>Aruba</td>
</tr>
<tr>
<td><strong>Version:</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Product:</strong></td>
<td>Aruba ClearPass</td>
</tr>
<tr>
<td><strong>Details:</strong></td>
<td>Copyright (c) 2015 Aruba, a Hewlett Packard Enterprise company.</td>
</tr>
<tr>
<td><strong>Signed by:</strong></td>
<td>Not signed by McAfee</td>
</tr>
<tr>
<td><strong>Requires:</strong></td>
<td></td>
</tr>
</tbody>
</table>

Once the Extension is installed, it will appear under the Software Extensions as **'Running'**, showing the name, version, status etc.

**Figure 32: Checking status of the ePO Extension installation**

---

**Utilizing the ePO Installed Permission set**

During the installation of the Aruba ClearPass extension, a **Permission Set attribute** called **'Aruba ClearPass'** is created. This can be used to restrict the capabilities of the user which communicates/queries ePO. In the context of 'the user', the reference here is to the user defined as **ePOAdminUser** in the ClearPass Extension configuration.

Below is an example of the new Permission Set, called **cppm-api-permission-set**. Name your permission set appropriately, then edit the new permission set to allow **'Run permission'** for **‘Aruba ClearPass’**. This then restricts any users to only being able to run/execute the Aruba ePO extension.

In addition to allowing **Aruba ClearPass**:

you must also allow **Queries and Reports**: as shown below
and you must also allow **System Tree Access**: as shown below.

| System Tree Access: | Can search on the following nodes and portions of the System Tree: My Organization Can access the following nodes and portions of the System Tree: My Organization |

If you intend to use the query-string **FW_CustomProps** to return attributes related to the McAfee Endpoint Threat client specific to the firewall settings then you must also set the following permission. If you are using the other query string options then the existing permission configuration supports the use of those queries.

| Endpoint Security Firewall Client: | View Client Properties |

**Figure 33: Defining the Permission set authorities**

Once the permission set has been defined and the permission set attribute configured, create a dedicated user which will be used to communicate between the ePO extension and the ClearPass extension. Alternately, add the permission set to an existing defined user. Below a new user was created, then assigned the permission set. This is the recommended approach.

Go to the menu and select **Users** as shown below and click on **New User** as highlighted.
**Figure 34:** Creating a new user in ePO

From the **New User** prompt, ensure you select the permission set previously created. In the example this is ‘cppm-api’. If your modifying and existing user, add the permission set to that user profile.

**Figure 35:** Creating a user and assigning the permission set
Un-Installing the ClearPass ePO Extension

To remove the ClearPass ePO Extension from the ePo Console, sign-in to the ePO Console. From the navigation tab click on **Software > Extensions** and on the extension you wish to remove click on **Remove**.

**Figure 36: ePO Extension Removal**

You will be asked to confirm that you do intend to remove the extension.

**Figure 37: ePO Extension Removal – Confirmation**

Using ePO Tags to drive Endpoint Enforcement

Within the ePO Console, the ePO administrator has access to Tags. A Tag can be used for many purposes such as grouping devices within the same authority or identifying an individual device due to an exception (e.g. a device is infected and needs to be Quarantined).

The following is an end-to-end example of using Tags. Create the Tags as required in the ePO Console under **System > Tag Catalog**.
From this page, there is an option to create a **New Tag**. Create the Tags as required or return here to create additional Tags in the future. In the above example, you can see multiple Tags have been created. The ‘Infected’ Tag will be used in this example. Once the Tags have been created, assign them to endpoints as required. Assume there is a requirement to assign the ‘Infected’ Tag to an endpoint such that this device will be Quarantined when it authenticates against ClearPass. Firstly, assign the Tag to an endpoint. From the **System Tree**, select the ‘infected’ endpoint, then from the Actions drop-down at the bottom of the screen, select ‘**Apply Tag**’ and chose the ‘Infected’ Tag and click – OK. The device selected now has the Tag applied.

Now that the endpoint is tagged, when this device authenticates on the network, ClearPass will query ePO and receive as part of the returned authorization attributes the Tags for the endpoint. ClearPass will use these Tags to select the enforcement policy for this device based upon the Tags and any other data that has been defined, to generate a point-in-time role for this device (e.g it may be corporate policy to ensure the endpoint has had a full endpoint-scan completed in the last 24-hours before admitting a device onto the network).

---

**NO*TE**: Remember EPOComputerProperties context is ALWAYS returned, thus TAGS are always returned for any query-string.
Below is an example of a device authentication in ClearPass. In the authorization attributes you can see the highlighted Tags received from ePO.

**Figure 40: Authorization attributes and ePO TAGS received**

```
![Authorization attributes and ePO TAGS received](image)
```

Based on the authorization attributes, specifically the ePO Tags, you can see the multiple enforcement profiles that have been applied based upon the authentication and the authorization policy calculation.

**Figure 41: CPPM assigning epo-infected-role**

```
![CPPM assigning epo-infected-role](image)
```

The ePO Tag attributes can be used to identify the device as being infected.
**Figure 42: Enforcement Policy for infected device Tag**

In the above example, ClearPass sends an Aruba-User-Role via a RADIUS VSA to an Aruba Wireless controller. On the controller, there is a matching ‘epo-infected-device’ role which restricts what the device can and cannot do. Below is the actual RADIUS VSA – ‘Aruba-User-Role’ enforcement-profile.

**Figure 43: Enforcement Profile - Sending an Aruba-User-Role via RADIUS to network**

In a similar way, other roles or dACLs or VLAN IDs could be sent as the outcome of the enforcement policy.
Appendix A: EPOComputerProperties

Field Descriptions

Tags: Infected, Workstation
Excluded Tags:
Last Communication: 7/27/17 4:10:41 PM PDT
Operating System: Windows 7|Workstation|6.1|Service Pack 1
System Name: HPE
Managed State: 1
Agent Version (deprecated): 5.0.5.658
Agent GUID: F2C112A6-6B8F-01E7-3DB1-0050569903F0
System Tree Sorting: true
Server Key: wPYTD1EgoXfJ36eqYNDoM3PAjcbvvoKVwmfNnM5y4=
To be Transferred: false
Sequence Errors: 0
Last Sequence Error: null
Communication Type: 1
System Name: HPE
Description: null
System Description: N/A
Time Zone: Pacific Standard Time
Default Language: 0409
User Name: Administrator
Domain Name: WORKGROUP
DNS Name: HPE
IP Address: 0:0:0:0:0:FFFF:A02:646E
Subnet Address: 0:0:0:0:0:FFFF:A02:6400
Subnet Mask: 0:0:0:0:0:FFFF:FFFF:FF00
IP4 Address (deprecated): -1979554706
IPX Address: N/A
Subnet Address (deprecated):
Subnet Mask (deprecated):
MAC Address: 0050569903F0
OS Type: Windows 7
OS Version: 6.1
OS Service Pack Version: Service Pack 1
OS Build Number: 7601
OS Platform: Workstation
OS OEM Identifier: 00392-918-5000002-85660
CPU Type: Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz
CPU Speed (Mhz): 1997
Management Type: EPOAGENTMETA
Number Of CPUs: 4
CPU Serial Number: N/A
Total Physical Memory: 4294500352
Free Memory: 2482733056
Free Disk Space: 5638
Total Disk Space: 30617
Is Laptop: 0
Is 64 Bit OS: 1
Custom 1: null
Custom 2: null
Custom 3: null
Custom 4: null
Free System Drive Space: 5638
Total System Drive Space: 30617
Vdi: 0
Field Names

"EPOLeafNode.Tags":"Workstation",
"EPOLeafNode.ExcludedTags":"

"EPOLeafNode.LastUpdate":"2016-04-26T15:05:28-07:00",
"EPOLeafNode.os":"Windows 7|workstation|6.1|Service Pack 1",
"EPOLeafNode.NodeName":"CLEARPASS",
"EPOLeafNode.ManagedState":"1",
"EPOLeafNode.AgentVersion":"4.8.0.1500",
"EPOLeafNode.AgentGUID":"21E6B323-8B42-467A-85DF-118703743E30",
"EPOLeafNode.ServerKeyHash":"wPYTD1BEgoXFJ6eqYNDNoMpROAjbvvoKVwmfwNmSy4=",
"EPOLeafNode.TransferSiteListsID":false,
"EPOLeafNode.SequenceErrorCount":"0",
"EPOLeafNode.SequenceErrorCountLastUpdate":null,
"EPOComputerProperties.ComputerName":"CLEARPASS",
"EPOComputerProperties.Description":null,
"EPOComputerProperties.SystemDescription":N/A,
"EPOComputerProperties.TimeZone":"Pacific Standard Time",
"EPOComputerProperties.DefaultLangID":0409,
"EPOComputerProperties.UserName":admin,
"EPOComputerProperties.DomainName":WORKGROUP,
"EPOComputerProperties.IPHostName":clearpass.arubanetworks.com,
"EPOComputerProperties.IPV6":0:0:0:0:0:FFFF:A0B:9A0,
"EPOComputerProperties.IPSubnet":0:0:0:0:0:FFFF:A0B:800,
"EPOComputerProperties.IPSubnetMask":0:0:0:0:0:FFFF:FFFF:F800,
"EPOComputerProperties.IPXAddress":null,
"EPOComputerProperties.NetAddress":5ce0c5eeb579,
"EPOComputerProperties.OSType":Windows 7,
"EPOComputerProperties.OSVersion":6.1,
"EPOComputerProperties.OSServicePackVer":Service Pack 1,
"EPOComputerProperties.OSBuildNum":7601,
"EPOComputerProperties.OSPlatform":Workstation,
"EPOComputerProperties.OSEOMID":00371-OEM-8992671-00008,
"EPOComputerProperties.CPUType":Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz,
"EPOComputerProperties.CPUSpeed":2394,
"EPOComputerProperties.ManagementType":null,
"EPOComputerProperties.NumOfCPU":4,
"EPOComputerProperties.CPUSerialNum":N/A,
"EPOComputerProperties.TotalPhysicalMemory":17048911872,
"EPOComputerProperties.FreeMemory":12788683895,
"EPOComputerProperties.FreeDiskSpace":150053,
"EPOComputerProperties.TotalDiskSpace":243158,
"EPOComputerProperties.IsPortable":1,
"EPOComputerProperties.OSBitMode":1,
"EPOComputerProperties.UserProperty1":null,
"EPOComputerProperties.UserProperty2":null,
"EPOComputerProperties.UserProperty3":null,
"EPOComputerProperties.UserProperty4":null,
"EPOComputerProperties.SysvolFreeSpace":157826,
"EPOComputerProperties.SysvolTotalSpace":225466,
"EPOComputerProperties.Vdi":0,
"isFound":true

ClearPass – McAfee ePolicy Orchestrator - TechNote 37
Appendix B: AM_CustomProps

Field Descriptions

Tags: Infected, Workstation
Excluded Tags:
Last Communication: 7/25/17 5:10:29 AM PDT
Operating System: Windows 7|Workstation|6.1|Service Pack 1
System Name: HPE
Managed State: 1
Agent Version (deprecated): 5.0.5.658
Agent GUID: F2C112A6-68F0-11E7-3DB1-0050569903F0
System Tree Sorting: true
Server Key: wPYTD1BEgoXfJ6eqYNDNoMpROAjqbcvoKVwmfwNmSy4=
To be Transferred: false
Sequence Errors: 0
Last Sequence Error: null
Communication Type: 1
On-Access Scan Enabled: true
Access Protection Enabled: true
Exploit Prevention Enabled: true
ScriptScan Enabled: true
AMCore Content Compliance Days: null
On-Access Scan Compliance Status: 1
On-Access Scan Reason:
On-Access Scan Additional Reason:
On-Access Scan McAfee GTI Sensitivity: 3
On-Demand Scan Compliance Status: 0
On-Demand Scan Reason: IDS_COMPLIANCE_REASON_ODS_DISABLED
On-Demand Scan Additional Reasons:
On-Demand Full Scan Duration (hours): < 1
On-Demand Quick Scan Duration (minutes): 10 - 14
On-Demand Full Scan Date: 7/14/17 6:29:13 PM PDT
On-Demand Quick Scan Date: 7/24/17 9:41:20 PM PDT
On-Demand Full Scan McAfee GTI Sensitivity: 3
On-Demand Quick Scan McAfee GTI Sensitivity: 3
Right-Click Scan McAfee GTI Sensitivity: 3
AMCore Content Compliance Status: 0
AMCore Content Reason: IDS_COMPLIANCE_REASON_DAT_OUT_OF_DATE
AMCore Content Additional Reasons:
Exploit Prevention Compliance Status: 1
Exploit Prevention Reason:
Exploit Prevention Additional Reasons:
Exploit Prevention Content Created: 2017-04-06 21:56:50.0
Exploit Prevention Content Version: 10.5.0.7691
ScriptScan Compliance Status: 1
ScriptScan Reason:
ScriptScan Additional Reasons:
Access Protection Compliance Status: 1
Access Protection Reason:
Access Protection Additional Reasons:
DAT Version (Non-Windows): null
AMCore Content Version: 3027.0
AMCore Engine Version: 5900.7806
Threat Prevention Hotfix:
Threat Prevention Patch Version: 1
License Status: 1
Language: 409
Names of threats that Extra.DAT can detect:
Content Date: 6/29/17 8:43:00 AM PDT
Field Names

"EPOLeafNode.Tags" : "Infected, Workstation",
"EPOLeafNode.ExcludedTags" : "",
"EPOLeafNode.LastUpdate" : "2017-07-31T15:10:34-07:00",
"EPOLeafNode.os" : "Windows 7|Workstation|6.1|Service Pack 1",
"EPOLeafNode.NodeName" : "HPE",
"EPOLeafNode.ManagedState" : 1,
"EPOLeafNode.AgentVersion" : "5.0.5.658",
"EPOLeafNode.ServerKeyHash" : "wPYTD1bEg0xFJ6eqYNNoMphOAjcboxNVwNNmSy4=-",
"AM_CustomProps.OASbComplianceStatus" : 1,
"AM_CustomProps.OASComplianceStatus" : ",",
"AM_CustomProps.OASAdAdditionalComplianceStatus" : "",
"AM_CustomProps.OASGTILevel" : 3,
Appendix C: GS_CustomProps

Field Descriptions

Tags: Infected, Workstation
Excluded Tags: 
Last Communication: 7/25/17 5:10:29 AM PDT
Operating System: Windows 7|Workstation|6.1|Service Pack 1
System Name: HPE
Managed State: 1
Agent Version (deprecated): 5.0.5.658
Agent GUID: F2C112A6-68F0-11E7-3DB1-0050569903F0
System Tree Sorting: true
Server Key: wPYTD1BEgoXf36eqYNDNoMpROAjbvvKvVwmfWm5y4=
To be Transferred: false
Sequence Errors: 0
Last Sequence Error: null
Communication Type: 1
Time-Based Password Enabled: 0
Self Protection Enabled: true
Self Protection Compliance Status: 1
Self Protection Reason: 
Self Protection Additional Reasons: 
User Interface Password Changed: 12/31/99 4:00:00 PM PST
Client User Interface Access Level: 0
McAfee GTI Proxy Type: 0
Windows Application Logging Enabled: true
Send Events to McAfee ePO Enabled: true
Access Protection Events Filter Level: 3
Exploit Prevention Events Filter Level: 3
Firewall Events Filter Level: 3
On Access Scan Events Filter Level: 3
On Demand Scan Events Filter Level: 3
Adaptive Threat Protection Events Filter Level: 3
Web Control Events Filter Level: 3
Client Activity Logging Enabled: true
Access Protection Debug Logging Enabled: false
Exploit Prevention Debug Logging Enabled: false
On Access Scan Debug Logging Enabled: false
On Demand Scan Debug Logging Enabled: false
Firewall Debug Logging Enabled: false
Web Control Debug Logging Enabled: false
Adaptive Threat Protection Debug Logging Enabled: false
Client Activity Log Size in MB: 10
Client Debug Log Size in MB: 50
Client Log Files Location: C:\ProgramData\McAfee\Endpoint Security\Logs
SystemCore Version: 15.6.0.1870
ESP Hotfix: 
ESP Patch Version: 1
License Status: null
Language: 409
Field Names

"EPOLeafNode.Tags" : "Infected, Workstation",
"EPOLeafNode.ExcludedTags" : ",",
"EPOLeafNode.LastUpdate" : "2017-07-31T16:10:33-07:00",
"EPOLeafNode.os" : "Windows 7|Workstation|6.1|Service Pack 1",
"EPOLeafNode.NodeName" : "HPE",
"EPOLeafNode.ManagedState" : 1,
"EPOLeafNode.AgentVersion" : "5.0.5.658",
"EPOLeafNode.AgentGUID" : "F2C112A6-68F0-11E7-3DB1-0050569903F0",
"EPOLeafNode.ResortEnabled" : true,
"EPOLeafNode.ServerKeyHash" : "wPYTDiBEgoXfJ6eqYNDNoMqROAjbvvoKVwnfN5y4=",
"EPOLeafNode.SequenceErrorCount" : 0,
"EPOLeafNode.SequenceErrorCountLastUpdate" : null,
"EPOLeafNode.LastCommSecure" : "1",
"GS_CustomProps.IsTimeBasedPasswordEnabled" : 0,
"GS_CustomProps.SPComplianceStatus" : 1,
"GS_CustomProps.SPComplianceStatus" : ",",
"GS_CustomProps.SPAdditionalComplianceStatus" : "",
"GS_CustomProps.SPbComplianceStatus" : 1,
"GS_CustomProps.SPComplianceStatus" : ",",
"GS_CustomProps.clientUIAccessLevel" : 0,
"GS_CustomProps.gtiProxyType" : 0,
"GS_CustomProps.IsWindowsApplicationLoggingEnabled" : true,
"GS_CustomProps.IsSendEventsToepoEnabled" : true,
"GS_CustomProps.APEEventFilterlevel" : 3,
"GS_CustomProps.BDEventFilterlevel" : 3,
"GS_CustomProps.FWEEventFilterlevel" : 3,
"GS_CustomProps.OASEventFilterlevel" : 3,
"GS_CustomProps.ODSEventFilterlevel" : 3,
"GS_CustomProps.ATPEventFilterlevel" : 3,
"GS_CustomProps.WPEventFilterlevel" : 3,
"GS_CustomProps.IsClientActivityLoggingEnabled" : true,
"GS_CustomProps.IsAPClientDebugLoggingEnabled" : false,
"GS_CustomProps.IsBOClientDebugLoggingEnabled" : false,
"GS_CustomProps.IsOASClientDebugLoggingEnabled" : false,
"GS_CustomProps.IsODSClientDebugLoggingEnabled" : false,
"GS_CustomProps.IsFWClientDebugLoggingEnabled" : false,
"GS_CustomProps.IsWPClientDebugLoggingEnabled" : false,
"GS_CustomProps.IsATPClientDebugLoggingEnabled" : false,
"GS_CustomProps.ClientActivityLogSizeMB" : 10,
"GS_CustomProps.ClientDebugLogSizeMB" : 50,
"GS_CustomProps.ClientLogFilesLocation" : "C:\ProgramData\McAfee\Endpoint Security\Logs",
"GS_CustomProps.AacVersion" : "15.6.0.1870",
"GS_CustomProps.Hotfixes" : ",",
"GS_CustomProps.Patch" : "1",
"GS_CustomProps.LicenseStatus" : null,
"GS_CustomProps.Language" : "409" } ]
Appendix D: **FW_CustomProps**

**Field Descriptions**

Tags: Infected, Workstation

Excluded Tags:

Last Communication: 7/25/17 5:10:29 AM PDT

Operating System: Windows 7|Workstation|6.1|Service Pack 1

System Name: HPE

Managed State: 1

Agent Version (deprecated): 5.0.5.658

Agent GUID: F2C112A6-68F0-11E7-3DB1-0050569903F0

System Tree Sorting: true

Server Key: wPYTDlBEgoXF36eqYNDNoMpROAjcbvvoKVwWmfwNmSy4=

To be Transferred: false

Sequence Errors: 0

Last Sequence Error: null

Communication Type: 1

Endpoint Security Firewall Compliance Status: 1

Compliance Status Reason: 0

Additional Compliance Status Reason: null

Firewall Status: 1

Firewall Adaptive Mode Status: 0

Firewall Fault: 0

Firewall Mode: 0

Firewall Hotfixes:

Language: 409

Firewall Last Policy Enforcement: 2017-07-25T11:11:05

Firewall License Status: 1

Firewall Patch Version: 0

Firewall Name Client UI Policy: null

Firewall Options Policy: My Default

Firewall Rules Policy: My Default

Firewall Trusted Applications Policy: null

Firewall Trusted Networks Policy: null

Endpoint Security Firewall client version: null

Reboot Required: 0

Firewall Service Running: 1

Install Directory (32 bit version): null

Install Directory (64 bit version): null

Product Version: 10.5.0.331
Field Names
"EPOLeafNode.Tags" : "Infected, Workstation", "EPOLeafNode.ExcludedTags" : "",
"EPOLeafNode.LastUpdate" : "2017-07-31T16:10:33-07:00",
"EPOLeafNode.os" : "Windows 7|Workstation|6.1|Service Pack 1",
"EPOLeafNode.NodeName" : "HPE",
"EPOLeafNode.ManagedState" : 1,
"EPOLeafNode.AgentVersion" : "5.0.5.658",
"EPOLeafNode.AgentGUID" : "F2C112A6-68F0-11E7-3DB1-005056903F00",
"EPOLeafNode.ResortEnabled" : true,
"EPOLeafNode.ServerKeyHash" : "wPYTDiBEgoXfJ6eqYNDNoMpoRAjcbvvoKvwmfwNn5y4=",
"EPOLeafNode.SequenceErrorCountLastUpdate" : null,
"FW_CustomProps.SequenceErrorCount" : 0,
"FW_CustomProps.SequenceErrorCountLastUpdate" : null,
"FW_CustomProps.ComplianceStatus" : 1,
"FW_CustomProps.ComplianceReason" : 0,
"FW_CustomProps.AdditionalComplianceReason" : null,
"FW_CustomProps.FWStatus" : 1,
"FW_CustomProps.FWAdaptiveModeStatus" : 0,
"FW_CustomProps.FWFault" : 0,
"FW_CustomProps.FWMode" : 0,
"FW_CustomProps.Hotfix" : "",
"FW_CustomProps.LicenseStatus" : 1,
"FW_CustomProps.ProductVersion" : null,
"FW_CustomProps.RebootRequired" : 0,
"FW_CustomProps.Patch" : "0",
"FW_CustomProps.PolicyNameClientUI" : null,
"FW_CustomProps.PolicyNameFwOptions" : "My Default",
"FW_CustomProps.PolicyNameFwRules" : "My Default",
"FW_CustomProps.PolicyNameTrustedAppList" : null,
"FW_CustomProps.PolicyNameTrustedNetworks" : null,
"FW_CustomProps.ProductVersion" : null,
"FW_CustomProps.RebootRequired" : 0,
Appendix E: WP_CustomProps

Field Descriptions

Tags: Infected, Workstation
Excluded Tags:
Last Communication: 7/25/17 5:10:29 AM PDT
Operating System: Windows 7|Workstation|6.1|Service Pack 1
System Name: HPE
Managed State: 1
Agent Version (deprecated): 5.0.5.658
Agent GUID: F2C112A6-68F8-11E7-3DB1-0050569903F0
System Tree Sorting: true
Server Key: wPYTDl8EgoXF36eqYNDNoMpROAjcbvvoKVwvMfWNm5y4=
To be Transferred: false
Sequence Errors: 0
Last Sequence Error: null
Compliance Type: 1
Compliance Status: 1
Compliance Status Reason:
Compliance Status Additional Reasons:
Web Control Enabled: true
Web Control Hotfixes:
Web Control Patch Version: 1
Language: 0409
License Status: 1
Functional in Internet Explorer: 2
Functional in Firefox: 1
Functional in Chrome: 1
Functional in Safari: null
Web Control functional status: 1
Field Names

"EPOLeafNode.Tags" : "Infected, Workstation",
"EPOLeafNode.ExcludedTags" : "",
"EPOLeafNode.LastUpdate" : "2017-07-31T16:10:33-07:00",
"EPOLeafNode.os" : "Windows 7|Workstation|6.1|Service Pack 1",
"EPOLeafNode.NodeName" : "HPE",
"EPOLeafNode.ManagedState" : 1,
"EPOLeafNode.AgentVersion" : "5.0.5.658",
"EPOLeafNode.AgentGUID" : "F2C112A6-68F0-11E7-3DB8-0050569903F0",
"EPOLeafNode.ResortEnabled" : true,
"EPOLeafNode.ServerKeyHash" : "wPYTDiBEgoXfJ6eqYNDNoMpROAjcbvvoKVwmfwNm5y4=",
"EPOLeafNode.TransferSiteListsID" : false,
"EPOLeafNode.SequenceErrorCount" : 0,
"EPOLeafNode.SequenceErrorCountLastUpdate" : null,
"WP_CustomProps.WPbComplianceStatus" : 1,
"WP_CustomProps.WPComplianceStatus" : "",
"WP_CustomProps.WPAdditionalComplianceStatus" : "",
"WP_CustomProps.bWPEnabled" : true,
"WP_CustomProps.Hotfixes" : "",
"WP_CustomProps.Patch" : "1",
"WP_CustomProps.Language" : "0409",
"WP_CustomProps.LicenseStatus" : 1,
"WP_CustomProps.LoadableIE" : "2",
"WP_CustomProps.LoadableFF" : "1",
"WP_CustomProps.LoadableCH" : "1",
"WP_CustomProps.LoadableSafari" : null,
"WP_CustomProps.WCStatus" : "1" }
Appendix F – Authorization Source XML Configuration File

Below is an example of a HTTP XML configuration file you can copy into a file and Import into your CPPM node. Before you import the file, you need to amend a couple of the attributes below in your preferred editor.

- **your_IP_ADDRESS** goes here
- **USERNAME** can be anything
- **PASSWORD** can be anything

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
  <TipsHeader exportTime="Mon Jun 13 15:20:33 PDT 2016" version="6.6"/>
  <AuthSources>
    <AuthSource description="" name="epo-authz" isAuthorizationSource="false" type="HTTP">
      <NVPair value="http://your_IP_ADDRESS_goes_here" name="base_url"/>
      <NVPair value="USERNAME_can_be_anything" name="username"/>
      <NVPair value="PASSWORD_can_be_anything" name="password"/>
    </AuthSource>
  </AuthSources>
</TipsContents>
```
Appendix G – Additional Diagnostics & Support

Extension Service

The ClearPass Extension is supported by a new system service 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 your cppm node] > Service Control. You can also start/stop the extension service from here. By default this service is automatically started.

Figure 44: Checking on Extension service and how to start/stop the service

Extension Logs/Debugging

If you have a need to access the logs from inside the Extension, you can turn on log collection from the API Explorer. Referencing the configuration previously used, adjust the "logLevel" to "DEBUG". Post this using the API Explorer as shown below.

```json
{
"ePoHost": "10.11.12.13",
"ePoPort": "8443",
"ePoAdminUser": "cppm-api-user",
"verifySSLCerts": true,
"logLevel": "DEBUG"
}
```
Once you have configured the extension to capture logs, there are two methods to access them. The first is directly through the API Explorer and the second using the Collect Logs function.

You can also enable timestamps and optionally limit the number of logs returned to the last ‘N’, e.g. 100 rather than ‘all’ logs by specifying a number in the tail field. By default, all logs are returned and with no timestamps.
**Accessing Extension logs within ClearPass ‘Collect Logs’**

In addition to the logging of messages so they can 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.

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. 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, so if INFO is selected it will show messages for INFO, WARN, ERROR, FATAL.

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

**Figure 48: Extension logs location in ‘Collect Logs’ diagnostic GZ file**