Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01</td>
<td>March 2020</td>
<td>Arpit Bhatt</td>
<td>DRAFT - Initial Release</td>
</tr>
<tr>
<td>2020-01</td>
<td>March 2020</td>
<td>Danny Jump</td>
<td>Initial Published Release</td>
</tr>
</tbody>
</table>

Copyright

©Copyright 2020 Hewlett Packard Enterprise Development LP.

Open Source Code

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

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

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.
Contents
Introduction and Overview .................................................................................................................. 5
Pictorial View of the Integration ......................................................................................................... 5
Software Requirements ........................................................................................................................... 5
Installation and Deployment Guide ...................................................................................................... 6
Access to the Extension Store ............................................................................................................... 6
New Extension Support in ClearPass 6.7+ .............................................................................................. 6
  Extensions and IP address configuration support .............................................................................. 6
  Extensions and web proxy support .................................................................................................... 7
Configuration Steps in CrowdStrike to enable API communication .................................................. 8
  Configuring CrowdStrike for ClearPass Integration ............................................................................ 8
  Getting API Credentials ...................................................................................................................... 8
  Check for Managed Hosts ................................................................................................................ 9
CrowdStrike Extension Installation and Configuration on ClearPass .................................................... 10
Use Cases ............................................................................................................................................ 15
  Periodic Poll ....................................................................................................................................... 15
  CrowdStrike as an Authorization Source ........................................................................................... 17
  Contain an endpoint using CrowdStrike APIs .................................................................................. 21
    Endpoint Context Server .................................................................................................................. 21
    Context Server Action ...................................................................................................................... 22
  Enforcement Profile ............................................................................................................................ 23
Appendix A – Additional Diagnostics and Support ............................................................................. 24
  The Extensions Service ...................................................................................................................... 24
  Extension logs and debugging ............................................................................................................. 24
  Accessing extension logs within ClearPass ‘Collect Logs’ ................................................................. 25
Appendix B – XMLs .............................................................................................................................. 26
Appendix C – Attributes Fetched from CrowdStrike ........................................................................... 27
Figures

Figure 1: Pictorial view of ClearPass Policy Manager integration with CrowdStrike Falcon ................................................. 5
Figure 2: Entering HP Passport credentials .................................................................................................................. 6
Figure 3: Extension framework GUI ............................................................................................................................ 7
Figure 4: Defining the base IP SUBNET and LOCALHOST for the Extensions framework ............................................ 7
Figure 5: Create an API Client and Key ........................................................................................................................ 8
Figure 6: Managed Hosts .................................................................................................................................................. 9
Figure 7: Extensions framework GUI .......................................................................................................................... 10
Figure 8: GUI Extension search ...................................................................................................................................... 10
Figure 9: GUI Extension install ...................................................................................................................................... 11
Figure 10: GUI Extension configuration at install time ................................................................................................ 11
Figure 11: Extension configuration parameters ........................................................................................................... 12
Figure 12: Creating an Admin user on ClearPass ......................................................................................................... 13
Figure 13: GUI review and setting the Extension configuration .................................................................................... 14
Figure 14: Log validation ................................................................................................................................................ 14
Figure 15: Endpoint Repository ..................................................................................................................................... 15
Figure 16: Fetched attributes - I ...................................................................................................................................... 16
Figure 17: Fetched attributes - II .................................................................................................................................... 16
Figure 18: Sample Enforcement Policy ........................................................................................................................ 17
Figure 19: Adding an HTTP Authorization Source – General Tab ............................................................................. 18
Figure 20: Adding an HTTP Authorization Source – Primary Tab ............................................................................ 18
Figure 21: Adding an HTTP Authorization Source – Attributes Tab (Add Filter) ........................................................ 19
Figure 22: Enforcement Policy ....................................................................................................................................... 19
Figure 23: Access Tracker .............................................................................................................................................. 20
Figure 24: Adding an Endpoint Context Server ........................................................................................................... 21
Figure 25: Adding a Context Server Action - Contain ................................................................................................. 22
Figure 26: Adding a Context Server Action – Lift Containment .................................................................................. 22
Figure 27: Enforcement Profile ...................................................................................................................................... 23
Figure 28: Access Tracker .............................................................................................................................................. 23
Figure 29: Checking on the extensions service and how to start/stop the service ......................................................... 24
Figure 30: Using the GUI to change the DEBUG level ................................................................................................ 24
Figure 31: Extension logs location in 'Collect Logs' diagnostic GZ file ........................................................................ 25
Introduction and Overview

CrowdStrike Falcon Endpoint Protection is a cloud-based security platform that combines the capabilities of a next-gen Antivirus (NGAV) and Endpoint Detection and Response (EDR) using a single cloud-delivered agent.

ClearPass Policy Manager integrates with CrowdStrike Falcon in multiple ways:

- Perform a real-time lookup of the device attributes which can be leveraged for Authorization.
- Bulk import of all the endpoints leveraging flexible polling definition based on crontab
- Trigger containment or lift the containment for the quarantined devices using the CrowdStrike Falcon agent.

The above use-cases are covered in Phase 1 of this integration and documented in this Integration Guide.

Pictorial View of the Integration

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

**Figure 1: Pictorial view of ClearPass Policy Manager integration with CrowdStrike Falcon**

Software Requirements

The minimum software version required for ClearPass is 6.7.2. At the time of writing, ClearPass 6.8.4 is the latest available and recommended release. Any subsequent ClearPass software release will support this integration. ClearPass runs on either hardware appliances with pre-installed software, or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 6.0, 6.5, 6.6, 6.7 update 1-3
- Microsoft Hyper-V Server 2012, 2016, 2019
- Hyper-V on Microsoft Windows Server 2012 or 2016 R2
- KVM on CentOS 7.5+, Ubuntu 18.04
Installation and Deployment Guide

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


Access to the Extension Store

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

Figure 2: Entering HP Passport credentials

New Extension Support in ClearPass 6.7+

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

Extensions and IP address configuration support

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

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

The Policy Manger web proxy configuration is ONLY read by the extension at installation time. If the web proxy configuration is changed in Policy Manager, then the extension must be re-installed so the new settings are re-read.

Figure 3: Extension framework GUI

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

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

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

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

**Configuration Steps in CrowdStrike to enable API communication**

There are primarily 2 steps involved in getting this integration configured.

1. Configuration of CrowdStrike for Integration
2. Installation and Configuration of CrowdStrike extension using the ClearPass Policy Manager GUI

**Configuring CrowdStrike for ClearPass Integration**

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

**Getting API Credentials**

Login to the CrowdStrike tenant, using your administrator credentials.

Create a new API Client. Navigate to Support > API Clients and Keys. Click on “Add new API client”.

*Figure 5: Create an API Client and Key*
Save the **API Client ID** and **Client Key** on a notepad. **Client Key** is not displayed again. This will be used while configuring the Extension in ClearPass Policy Manager.

Enter a **Client Name**. Under API Scopes, add the following permissions

1. Read/Write permissions for **Hosts**
2. Read for **Event streams**

### Check for Managed Hosts

This configuration step is optional and is only required if there are no Endpoints managed by CrowdStrike.

Go to **Hosts > Host Management**. Ensure there are hosts being managed by CrowdStrike. These are the hosts that will be pulled by ClearPass Policy Manager, if the sync function is enabled in the Extension configuration.

**Figure 6: Managed Hosts**

If no hosts are managed by CrowdStrike, one needs to install the Falcon Sensor on the endpoints to be managed. These steps vary based on the endpoint Operating System. The installers are available under **Hosts > Sensor Downloads**.

Steps for sensor installation are available under the section “**Sensor Deployment and Maintenance**” here [https://falcon.crowdstrike.com/support/documentation](https://falcon.crowdstrike.com/support/documentation)
CrowdStrike Extension Installation and Configuration on ClearPass

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

Figure 7: Extensions framework GUI

From here, click on 'Install Extension', and the search box below appears. Enter the keyword “CrowdStrike” and click on Search.

Figure 8: GUI Extension search

Starting 6.7, in a cluster environment an extension can be installed on the subscriber nodes directly.

Click on the Extension and then the Install option
Set a specific IP address for the extension if required. It will automatically pick an IP address if not assigned.

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

```json
{
  "logLevel": "INFO",
  "verifySSLCerts": true,
  "crowdStrikeApiHost": "api.crowdstrike.com",
  "clientId": "[Client ID]",
  "clientSecret": "********",
  "enableEndpointLookupCache": false,
  "endpointCacheTimeSeconds": 300,
  "syncAllOnStart": false,
  "enableSyncAll": false,
  "syncAllSchedule": "0 2 * * 6",
  "syncUpdatedOnly": false,
  "pageSize": 500,
  "cppmUserName": "[CPPM User Name]",
  "cppmPassword": "********"
}
```

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

**Figure 11: Extension configuration parameters**

<table>
<thead>
<tr>
<th>Configuration attribute</th>
<th>Description</th>
<th>Example/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>logLevel</td>
<td>Logging level for troubleshooting</td>
<td>&quot;DEBUG&quot;, &quot;INFO&quot;, &quot;WARN&quot;, &quot;ERROR&quot;</td>
</tr>
<tr>
<td>verifySSLCerts</td>
<td>Should SSL Certificates be validated</td>
<td>true/false</td>
</tr>
<tr>
<td>crowdStrikeApiHost</td>
<td>The hostname or IP address of the CrowdStrike API</td>
<td>Default: api.crowdstrike.com</td>
</tr>
<tr>
<td>clientId</td>
<td>The Client ID used to access the CrowdStrike OAuth API</td>
<td>huzBI-xxx-xxxxx-xxxxx</td>
</tr>
<tr>
<td>clientSecret</td>
<td>The Client Secret for the provided Client ID</td>
<td>abcdefg-xxx-qwerty-xxxxx-xxxxx</td>
</tr>
<tr>
<td>enableEndpointLookupCache</td>
<td>The number of seconds that an endpoint lookup should be cached. The value of attributes is not updated for the time they are cached. The timer is used for better performance.</td>
<td>true/false</td>
</tr>
<tr>
<td>endpointCacheTimeSeconds</td>
<td>The number of seconds an endpoint needs to be cached if enableEndpointLookupCache is set to true</td>
<td>Default: 300 seconds</td>
</tr>
<tr>
<td>syncAllOnStart</td>
<td>Syncs all endpoints when the extension starts</td>
<td>true/false</td>
</tr>
<tr>
<td>enableSyncAll</td>
<td>Syncs all endpoints at a frequent interval. Similar to Polling.</td>
<td>true/false</td>
</tr>
<tr>
<td>syncAllSchedule</td>
<td>The schedule to be used when enableSyncAll is set to true</td>
<td>Cron Format (0 2 * * 6)</td>
</tr>
<tr>
<td>syncUpdatedOnly</td>
<td>If enabled, this will limit the updates to machines that have been updated since the last run.</td>
<td>true/false</td>
</tr>
</tbody>
</table>
The `cppmUserName` and `cppmPassword` should be for an Network Administrator account. The device profiling attributes obtained from CrowdStrike need to be written into the endpoint repository leveraging the REST APIs which requires an Network Administrator account.

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

Figure 12: Creating an Admin user on ClearPass

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

A copy of the CrowdStrike Falcon extension with the desired configuration is shown below, this has to be modified for your deployment. Modify the `clientId`, `clientSecret`, `cppmUserName`, `cppmPassword` and other options that will be specific to your environment. Change or include any other values based on the description of each in the above table.
Select **Restart** and click on **Save Changes** to restart the extension.

**Figure 13: GUI review and setting the Extension configuration**

After completing the configuration, click on ‘Save Changes’ and restart of the extension, click on **Show Logs**.

**Figure 14: Log validation**

The above log shows that the extension has been configured and has ingested endpoints from CrowdStrike leveraging sync on start. These logs can be seen in detail if the loglevel setting is changed to **DEBUG**.
**Use Cases**

The extension can serve multiple use cases as described in the Introduction section as well as the Pictorial. Each use case would require some further configuration based on the requirement. Some example configurations are shown below for each use case.

**Periodic Poll**

This is a commonly used method where the extension is configured to sync all the endpoints to begin with. Once finished, the extension is configured to periodically gather updated data at fixed intervals leveraging the configuration parameters as discussed in the table in previous section. Following is the sample configuration used.

```json
{
    "logLevel": "DEBUG",
    "verifySSLCerts": true,
    "crowdStrikeApiHost": "api.crowdstrike.com",
    "clientId": "15ea252aaf744a324345qwerty",
    "clientSecret": "********",
    "enableEndpointLookupCache": false,
    "endpointCacheTimeSeconds": 300,
    "syncAllOnStart": true,
    "enableSyncAll": true,
    "syncAllSchedule": "0 */2 * * *",
    "syncUpdatedOnly": false,
    "pageSize": 500,
    "cppmUserName": "admin",
    "cppmPassword": "********"
}
```

The above configuration enables periodic sync and triggers it every 2 hours. This could be aggressive and should be changed based on the requirement in a particular scenario to ensure that CrowdStrike is not inundated with requests and also to manage the resource utilization on ClearPass Policy Manager.

A parameter that further helps with optimization is `syncUpdatedOnly`. Set this value to true to get updates only if there is a change associated with the endpoint. The value of `pageSize` should not be changed unless recommended by customer support.

Validation of the endpoint context being updated after the initial sync can be done by navigating to **Configuration > Identity > Endpoints**. Filter using the attribute **Source = CrowdStrike** as shown below.

*Figure 15: Endpoint Repository*
Shown below is a sample of security contextual parameters obtained from CrowdStrike for an endpoint, these attributes can be evaluated by the enforcement policy within ClearPass Policy Manager. These attributes are obtained leveraging the default policy on CrowdStrike. The Falcon agent should be capable of capturing further attributes which could be leveraged as well. The full list of endpoint attributes is documented in Appendix C on Page 27.

**Figure 16: Fetched attributes - I**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Agent Load Flags</td>
<td>1</td>
</tr>
<tr>
<td>CrowdStrike Agent Local Time</td>
<td>2019-11-22T16:50:43.649Z</td>
</tr>
<tr>
<td>CrowdStrike Agent Version</td>
<td>5.21.10306.0</td>
</tr>
<tr>
<td>CrowdStrike BIOS Manufacturer</td>
<td>American Megatrends Inc.</td>
</tr>
<tr>
<td>CrowdStrike BIOS Version</td>
<td>090007</td>
</tr>
<tr>
<td>CrowdStrike Build Number</td>
<td>14393</td>
</tr>
<tr>
<td>CrowdStrike Cid</td>
<td>643b2392ec494d948e9c879c4fe11f3a</td>
</tr>
</tbody>
</table>

**Figure 17: Fetched attributes - II**

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Attributes</th>
<th>Device Fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Modified Timestamp</td>
<td>2019-11-23T03:52:10Z</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike OS Version</td>
<td>Windows 10</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Platform ID</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Platform Name</td>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Pointer Size</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Policies</td>
<td>prevention-cae3ac3b9f64f2f1b11ea6b6650e243e</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Product Type</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Product Type Desc</td>
<td>Workstation</td>
<td></td>
</tr>
<tr>
<td>CrowdStrike Provision Status</td>
<td>Provisioned</td>
<td></td>
</tr>
</tbody>
</table>
A sample enforcement policy leveraging the endpoint attributes which can be used in a service is shown below.

**Figure 18: Sample Enforcement Policy**

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Tips.Role  = [User Authenticated]) AND (Endpoint:Source = CrowdStrike) AND (Endpoint:Provision Status = Provisioned)</td>
<td>Full access</td>
</tr>
</tbody>
</table>

**CrowdStrike as an Authorization Source**

With CrowdStrike as an Authorization Source, ClearPass Policy Manager can query CrowdStrike Real-Time to determine if the endpoint is managed by CrowdStrike at the time of Authorization and grant access accordingly. It can leverage other security attributes returned by CrowdStrike within the enforcement policy. For example, a contained device can be denied access, a device with Last Update higher than the expected value can be quarantined etc.

This use case requires further configuration which includes an addition of Authentication Source which will be used for Authorization. It also necessitates modification of a service to use this new source for Authorization and a modification of Enforcement Policy to use this Authorization source which will be covered below.

The addition of Authentication source can be easily configured by importing the XML available on Aruba GitHub. Kindly refer **Appendix B** for details.

Adding CrowdStrike as an Authorization source can be done under **Configuration > Authentication > Sources**, click “Add”.
Click on **Next**. This will advance to the Primary Tab which requires connection details. Here an internally POST is made to the extension. The extension then calls CrowdStrike APIs to retrieve the security attributes associated with the endpoint.

The Base URL is http://<Extension IP>. The extension IP is highlighted in **Figure 14**. The **Login Username** and **Login Password** are mandatory fields but never used here since the contents are posted internally to an extension. This value has to be defined and could be anything.

Click on **“Next”**. This will advance you to the Attributes Tab where you need to provide the authorization attributes. Click on **“Add More Filters”**. Provide a Name for the filter and then a Filter Query. It’s extremely important that the Filter Query is defined correctly. This is the query string that is sent to the CrowdStrike extension asking for context about the endpoint. The query is indexed off the mac-address of the authenticating endpoint. For completeness, the filter query is provided here, copy it carefully.

```
%(Connection:Client-Mac-Address-NoDelim)
```

Next build out the definitions of the attributes that will be returned from the **Filter Query**. These attributes will subsequently be used within our policy-evaluation and ultimately the enforcement policy applied.
Further attributes can be added here if necessary for the policy. Appendix C has a list of attributes captured by the extension.

Once the HTTP authorization source is defined, the returned attributes can be leveraged in a service using an enforcement policy or role mapping. A sample enforcement policy is shown below. Remember to add the newly added Authorization Source under the Authorization tab of the service.

The above policy grants full access to an endpoint if it is provisioned with a CrowdStrike Falcon agent and the agent has not contained the endpoint.

A point to note is that ClearPass Policy Manager would query the Authorization Source every time it authenticates. The problem with this approach is that if there is a latency in the response from CrowdStrike which is hosted in cloud, it would result in a delay for an endpoint to get onto the network. If the delay is beyond an acceptable limit it would result in timeouts. Also, for best performance it is always recommended to leverage the ability of ClearPass to cache the attributes for a configurable time period.
Let’s revisit the configuration parameters of the extension. The parameters of interest are `enableEndpointLookupCache` and `enableCacheTimeSeconds`. The values are explained in the table under the section “Configuration Steps”.

```json
{
    "logLevel": "DEBUG",
    "verifySSLCerts": true,
    "crowdStrikeApiHost": "api.crowdstrike.com",
    "clientId": "15ea252aafe744a12345qwerty",
    "clientSecret": "*******",
    "enableEndpointLookupCache": true,
    "enableCacheTimeSeconds": 3600,
    "syncAllOnStart": true,
    "enableSyncAll": true,
    "syncAllSchedule": " 0 */2 * * *",
    "syncUpdatedOnly": false,
    "pageSize": 500,
    "cppmUserName": "admin",
    "cppmPassword": "*******"
}
```

The access tracker results with the Authorization attributes is shown below

**Figure 23: Access Tracker**

Leverage the benefits of caching the attributes for faster authentication results. This is particularly useful in scenarios where clients roam frequently triggering frequent authentication requests. Use these parameters best suited in a customer environment based on their requirements.
Contain an endpoint using CrowdStrike APIs

ClearPass Policy Manager extension can call the Crowdstrike APIs to trigger containment on the endpoint leveraging the Falcon agent. APIs can also be leveraged to lift the containment.

Configuration for containment includes 3 steps on ClearPass Policy Manager. These steps can be ignored if the Enforcement Policies are exported directly as an XML. The steps are available in Appendix B.

1. Define Endpoint Context Server
2. Add Context Server Action
3. Create an Enforcement Profile to trigger the action

Endpoint Context Server

The first step is to define an Endpoint Context Server. This can be added under Administration > External Servers > Endpoint Context Servers click on Add and use the extension IP address highlighted in Figure 14.

Figure 24: Adding an Endpoint Context Server

Select the **Server Type** as “Generic HTTP”. The **Server Name** is the IP address of the Extension. Once you enter that, the **Server Base URL** gets automatically populated and adds https to begin with.

**WARNING**

Ensure you change this to http else the internal POST fails. Please note that this is an internal post within ClearPass from the Policy Manager to the Extension.
**Context Server Action**

The next step is to define a Context Server Action within ClearPass Policy Manager which will internally POST to the extension. The extension will trigger an API call to CrowdStrike and fetch the information associated with it which can be used for Authorization. The context server action allows us to define the HTTP Method, the URL and the JSON contents that will be used to post the mac address to the extension.

This can be added under **Administration > Dictionaries > Context Server Actions.** Click on **Add** and use the details shown below. All the other tabs are blank.

The URL used below has to match for the API calls to be successful. Kindly copy paste the URL from below

**Contain:** /contain/%{Connection:Client-Mac-Address-NoDelim}

**Lift Containment:** /lift-containment/%{Connection:Client-Mac-Address-NoDelim}

**Figure 25: Adding a Context Server Action - Contain**

Similarly, a Context Server Action for lifting the containment is shown below.

**Figure 26: Adding a Context Server Action - Lift Containment**
**Enforcement Profile**

The next step involves using the Context Server Action in an Enforcement Profile as below. The Enforcement Profile for containing an endpoint leveraging CrowdStrike APIs action is shown below.

**Figure 27: Enforcement Profile**

Containment would only work if the attribute CrowdStrike Device ID exists in the Endpoint repository in CPPM. The attribute is not stored if CrowdStrike is only used as an Authorization source without poll/sync and enableEndpointLookupCache is set to false.

The Access Tracker result is shown below. CPPM triggers an internal API call to the extension configured.

**Figure 28: Access Tracker**

Similarly, containment can be lifted from the hosts using the Lift Containment action or Enforcement Policy within CPPM.
Appendix A – Additional Diagnostics and Support

The Extensions Service

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

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

**Figure 29: Checking on the extensions service and how to start/stop the service**

![Service Control Table]

Extension logs and debugging

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

**Figure 30: Using the GUI to change the DEBUG level**

![GUI Configuration]

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

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

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

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

**Figure 31: Extension logs location in ‘Collect Logs’ diagnostic GZ file**

---

ClearPass and CrowdStrike Falcon - Integration Guide 25
Appendix B – XMLs

The following steps are required to add CrowdStrike as an Authentication Source by importing it into ClearPass Policy Manager using the XML file available in our GitHub repository

https://github.com/aruba/clearpass-exchange-snippets/tree/master/extensions/crowdstrike

- Download the XML profile > “clearpass-extension_crowdstrike_auth-source.xml”.
- Open the XML file using a simple editor and replace X.X.X.X with your EXTENSION IP ADDRESS (Refer Figure 14).
- You can also import the XML without making any edits and then change the “Base URL:” from “http://X.X.X.X” to your extension IP address using the ClearPass Policy Manager UI. This can be changed under the Primary tab of the imported Authentication Source (Refer Figure 20).
- The XML file can be imported into ClearPass by navigating to Configuration > Authentication > Sources. Click on Import and use the file downloaded.

The Enforcement Profile, Context Server Action and the Endpoint Context Server configured in the section “Contain an endpoint using CrowdStrike APIs” can easily be imported using the XML available on Aruba GitHub

https://github.com/aruba/clearpass-exchange-snippets/tree/master/extensions/crowdstrike

- Download the XML profile > “clearpass-extension_crowdstrike_enf-profile.xml”.
- Open this file in your favorite editor. Use the Find and Replace feature of the editor to replace “<<Extension IP>>>” with the actual IP address of the extension configured. Refer Figure 14.
- The XML file can be imported into ClearPass by navigating to Configuration > Authentication > Sources. Click on Import and use the file downloaded.
Appendix C – Attributes Fetched from CrowdStrike

Following is the sample list of the default attributes fetched from CrowdStrike using the default policy.

```
{
    "CrowdStrike MAC Address": "00-15-5d-0d-64-07",
    "CrowdStrike Device ID": "975ce8fa4e4f3d791e399f8151e1da",
    "CrowdStrike Cid": "643b2392ec49d948e9c879c4fe11f3a",
    "CrowdStrike Agent Load Flags": "1",
    "CrowdStrike Agent Local Time": "2019-11-26T22:35:57.134Z",
    "CrowdStrike Agent Version": "5.21.10306.0",
    "CrowdStrike BIOS Manufacturer": "American Megatrends Inc.",
    "CrowdStrike BIOS Version": "000000",
    "CrowdStrike Build Number": "7601",
    "CrowdStrike Config ID Base": "65994753",
    "CrowdStrike Config ID Build": "10306",
    "CrowdStrike Config ID Platform": "3",
    "CrowdStrike External IP": "76.108.39.211",
    "CrowdStrike Hostname": "CS-SA-LI-08NP1",
    "CrowdStrike First Seen": "2019-11-22T15:13:06Z",
    "CrowdStrike Last Seen": "2019-11-28T00:26:18Z",
    "CrowdStrike Local IP": "169.254.200.159",
    "CrowdStrike Major Version": "6",
    "CrowdStrike Minor Version": "1",
    "CrowdStrike OS Version": "Windows Server 2008 R2",
    "CrowdStrike Platform ID": "0",
    "CrowdStrike Platform Name": "Windows",
    "CrowdStrike Policies": "prevention-6dfa63d7790446c4babf32db50e0810e",
    "CrowdStrike Device Policies": "Prevention-6dfa63d7790446c4babf32db50e0810e, Sensor Update-b7178b018dcb4a88d3ec39401acfb5c, Device Control-5d3813ac29c44e54b48987b25c361bda, Global Config-67643d17e357489c8d6a88d38c07f1b4, Remote Response-22b66442b69433db2f8112d1f7dea",
    "CrowdStrike Product Type": "3",
    "CrowdStrike Product Type Desc": "Server",
    "CrowdStrike Provision Status": "Provisioned",
    "CrowdStrike Service Pack Major": "1",
    "CrowdStrike Service Pack Minor": "0",
    "CrowdStrike Pointer Size": "8",
    "CrowdStrike Status": "contained",
    "CrowdStrike System Manufacturer": "Microsoft Corporation",
    "CrowdStrike System Product Name": "Virtual Machine",
    "CrowdStrike Modified Timestamp": "2019-11-28T00:29:06Z",
    "CrowdStrike Last Update": "2019-11-27 16:41:59",
    "CrowdStrike System Found": true
}
```