Trend Micro Apex One
Apex Central

ClearPass

a Hewlett Packard Enterprise company

Integration Guide
ClearPass and Trend Micro Apex Central Integration

Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>v2020-01</td>
<td>March 2020</td>
<td>Danny Jump</td>
<td>First Published Version</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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Log</td>
<td>2</td>
</tr>
<tr>
<td>Contents</td>
<td>3</td>
</tr>
<tr>
<td>Figures</td>
<td>4</td>
</tr>
<tr>
<td>Introduction and Overview</td>
<td>5</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>5</td>
</tr>
<tr>
<td>ClearPass Installation and Deployment Guide</td>
<td>5</td>
</tr>
<tr>
<td>ClearPass Extensions</td>
<td>5</td>
</tr>
<tr>
<td>Access to the Extension Store</td>
<td>6</td>
</tr>
<tr>
<td>Pictorial View of the Integration</td>
<td>7</td>
</tr>
<tr>
<td>Use Cases</td>
<td>7</td>
</tr>
<tr>
<td>New recent extension capabilities</td>
<td>8</td>
</tr>
<tr>
<td>Extensions and IP address configuration support</td>
<td>8</td>
</tr>
<tr>
<td>Configuration Values can be obfuscated in 6.7.2 or later</td>
<td>8</td>
</tr>
<tr>
<td>Extensions and web proxy support</td>
<td>8</td>
</tr>
<tr>
<td>Direct Installation of Extension on Subscribers</td>
<td>9</td>
</tr>
<tr>
<td>Trend Micro Apex Central Extension Installation</td>
<td>10</td>
</tr>
<tr>
<td>Checking API Access Application Control restrictions</td>
<td>12</td>
</tr>
<tr>
<td>Trend Micro Apex Central and ClearPass Extension Configuration</td>
<td>14</td>
</tr>
<tr>
<td>ClearPass Apex Central Extension Configuration options</td>
<td>14</td>
</tr>
<tr>
<td>Apex Central “Application” Configuration</td>
<td>15</td>
</tr>
<tr>
<td>ClearPass Extension Configuration</td>
<td>16</td>
</tr>
<tr>
<td>Using ClearPass Policy Manager with Apex Central</td>
<td>18</td>
</tr>
<tr>
<td>Using endpoint data that has been synchronized and cached</td>
<td>18</td>
</tr>
<tr>
<td>Using a Real-Time authorization check via HTTP authorization source</td>
<td>19</td>
</tr>
<tr>
<td>Triggering an isolation/restore action via Apex-Central</td>
<td>21</td>
</tr>
<tr>
<td>Configuring ClearPass to trigger isolation actions</td>
<td>21</td>
</tr>
<tr>
<td>Configuring ClearPass to trigger restore actions</td>
<td>22</td>
</tr>
<tr>
<td>Enforcement Profile</td>
<td>22</td>
</tr>
<tr>
<td>Appendix A - Copy of the HTTP authentication source in XML</td>
<td>23</td>
</tr>
<tr>
<td>Appendix B – Additional Diagnostics and Support</td>
<td>24</td>
</tr>
<tr>
<td>Checking on the Extension Service</td>
<td>24</td>
</tr>
<tr>
<td>Extension Logs/Debugging</td>
<td>24</td>
</tr>
<tr>
<td>Accessing the extension logs using ‘Collect Logs' system function</td>
<td>25</td>
</tr>
</tbody>
</table>
Figures

Figure 1: Entering HP Passport credentials .............................................................. 6
Figure 2: Pictorial view of the integration .............................................................. 7
Figure 3: Apex Central isolation message .............................................................. 7
Figure 4: Extension Framework GUI ...................................................................... 8
Figure 5: Defining the base IP SUBNET and LOCALHOST for the Extensions Framework .... 9
Figure 6: Extensions Framework GUI .................................................................. 10
Figure 7: GUI Extension Installation ................................................................... 10
Figure 8: Click on the Extension to reveal the 'Install' option ................................. 11
Figure 9: GUI Extension Configuration at Install time ........................................ 11
Figure 10: Reviewing and Setting the Extension configuration, below is the default configuration 12
Figure 11: Example of Extension authorization failure due to Policy Manager Application Control 12
Figure 12: Locking down access to the Policy Manager API for extensions ............. 13
Figure 13: List of Extension configuration options ................................................. 14
Figure 14: Adding an API-Application - part1 ....................................................... 15
Figure 15: Adding an API-Application - part2 ....................................................... 15
Figure 16: reviewing the application configuration ............................................... 16
Figure 17: Setting the Extension configuration ...................................................... 17
Figure 18: Enforcement policy leveraging the EndpointDb .................................... 18
Figure 19: Authorization Source for real-time check ............................................ 19
Figure 20: Authorization Source attribute and query definition ............................ 20
Figure 21: Enforcement policy leveraging the HTTP Authorization-source ............. 20
Figure 22: Context-Server definition isolate/restore function ............................... 21
Figure 23: Context-Server-Action isolate ............................................................ 21
Figure 24: Context-Server-Action restore ........................................................... 22
Figure 25: Enforcement Profile calling isolation CSA ........................................ 22
Figure 26: Services Control ............................................................................... 24
Figure 27: Locating the extension instance ID ..................................................... 25
Figure 28: Locating the Extension logs from 'Collect Logs' diagnostic GZ file .............. 25
Introduction and Overview
This Integration TechNote covers how to deploy and configure the ClearPass Extension to interface with Trend Micro Apex One, previously known as Trend Micro OfficeScan. The actual integration also mandates that a customer has Trend Micro Apex Central deployed, as there is no direct API integration into Apex One. In this TechNote we will cover the complete installation, configuration and integration between the Extension and ClearPass Policy Manager.

Software Requirements
The minimum software version required for ClearPass is 6.7.2. At the time of writing, ClearPass 6.8.5 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 or higher
- Microsoft Hyper-V Server 2012, 2016 R2 or 2019
- Hyper-V on Microsoft Windows Server 2012, 2016 R2 or 2019
- KVM on CentOS 7.5 or later
- Amazon EC2
- Certified with Apex One Version 2019 Build 2012 or later
- Certified with Apex Central Version 2019 Hotfix 2943 or later

ClearPass 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: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Default.htm

ClearPass Extensions
The integration between ClearPass Policy Manager and Trend Micro Apex Central is driven through a ClearPass capability known as Extensions, a sub-component of the ClearPass Exchange Integration framework. ClearPass Extensions are micro-services running on top of the base ClearPass platform. These micro-services enable Aruba to deliver new features outside of the main software release cycle and facilitate a faster time to market for specific features and integrations. Configuration and control of ClearPass Extensions is covered later in this document.
Access to the Extension Store

Access to the Extension Store to download extensions is simplified starting in 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 1: Entering HP Passport credentials**

Failure to define Passport Credentials manifests itself as an error at installation time, you will still be allowed to search for Extension but upon trying to install one the below message will be displayed.
Pictorial View of the Integration

**Figure 2: Pictorial view of the integration**

Use Cases

Unfortunately, unlike other EDR/EPP security endpoint vendors where content rich context is exposed Trend Micro provided a very limited amount of data. That said, there are still a number of very useful use-cases relevant to the integration and multiple ways you can leverage the integration.

The first use-case everyone should enable is ‘Does the authenticating endpoint have Apex One installed?’

After that we can check if the endpoint has been tagged by Apex One as in ‘isolation’ mode, this being an example where we might want to quarantine this device if it ever connects to the network because Trend has identified it for whatever reason as being malicious, stolen or behaving erroneously.

We also have the ability to directly trigger an ‘isolation’ request into TrendMicro, as an example we could receive a IEE syslog from a firewall identifying an infected or badly behaving endpoint and trigger a context-server-action to make an API call to the Extension to ‘isolate’ the endpoint, this is in effect like changing the ROLE or sending a new dACL for the endpoint, but application access can still be controlled from Apex.

**Figure 3: Apex Central isolation message**

Notice the ‘control’ option above, Apex can be used to directly alter the application level data flow.
New recent extension capabilities

With the release of 6.7, several new features were added to enhance the functionality of the extension framework. Previously, all extension installation and operation tasks required use of the API Explorer. This functionality has been moved into the GUI. To manage extensions, use the Guest UI as shown below, access it from Guest > Administration > Extensions.

Extensions and IP address configuration support

The other major additions in the 6.7 release is the ability to define a static IP address for an extension. This being especially useful when deploying extensions across nodes within a cluster where there is the requirement for a consistent IP address for the extension, e.g. in the situation where a HTTP authorization source is configured, its mandatory the local Extension has the same IP address on all nodes in the cluster.

Configuration Values can be obfuscated in 6.7.2 or later.

Starting in 6.7.2 password and security sensitive configuration items are now obfuscated when presented in both the Extension GUI or in the Explorer configuration.

Extensions and web proxy support

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

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

Figure 4: 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 fall within the following subnet range 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 as defined by RFC1918.**

*Figure 5: Defining the base IP SUBNET and LOCALHOST for the Extensions Framework*

![ClearPass Policy Manager](image)

**Note that 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 using an IP address in the extension default range of 172.17.x.x/12. Set the new network address range as needed and restart the extension service for this change to take effect.

**Never set the DATA or MGMT IP address to use an address that matches the Extension Network**

**Direct Installation of Extension on Subscribers**

In 6.7.2 support was added to allow a ClearPass subscriber to directly access the Extension store and install an Extension thus simplifying the deployment process.
Trend Micro Apex Central Extension Installation

Starting in ClearPass 6.7, a Graphical User Interface (GUI) was introduced to make the process of interacting with the extension framework easier. To manage extensions, go to Guest > Administration > Extension.

*Figure 6: Extensions Framework GUI*

From here, click on ‘Install Extension’, in the top RHS of the screen and the search box below appears.

*Figure 7: GUI Extension Installation*

Enter the name of the Extension required, in this case **Trend** and click on ‘Search’.
Click on the extension and then the ‘Install’ option will appear.

**Figure 8: Click on the Extension to reveal the 'Install' option**

If necessary, be sure to set the IP address now.

**Figure 9: GUI Extension Configuration at Install time**

Do not choose to Start the extension as the configuration will need to be modified before it’s started, after the extension has been installed, review the extension configuration as necessary and adjust as needed.

Notice the options to Start, Delete, Reinstall or Show Logs and the option to review and set the extension configuration.
A copy of the default Trend Micro Apex Central Extension is shown above, this will need to be modified. In the next section we discuss the configuration values and how to use them and where to collect the configuration items that are required, i.e. applicationId.

**Checking API Access Application Control restrictions**

Within ClearPass additional controls can be leveraged to harden a ClearPass Policy Manager deployment, it's possible that at the time of the Extension deployment, these guidelines might have already been followed and the result is that the Extension does not work. Reviewing Extension Log might show something like the following after immediately starting the Extension, this likely indicates the ClearPass Application API's are in place.

**Figure 11: Example of Extension authorization failure due to Policy Manager Application Control**

```
<head>
  <title>
    Error 403 (Forbidden)
  </title>
  <script language="javascript">
    function reloadPage() {
      var locHref = window.location.protocol + "/" + window.location.hostname;
      window.location.href = locHref;
    }
  </script>
</head>
```
To resolve this, add the IP address of the Extension to the list of nodes permitted, for this reason its good practice to fix the IP address of the extension at installation time such that it doesn't change over time and break the application controls. Access to the Policy Manager API can be controlled from **Administration > Server Manager > Server Configuration (choose your node) > Network**

*Figure 12: Locking down access to the Policy Manager API for extensions*
Trend Micro Apex Central and ClearPass Extension Configuration

The ClearPass Trend Micro Apex Central extension configuration necessitates that you set and/or collect a number of items, some will have to be configured and collected based upon the configuration of your Apex Central. Deployment and Configuration of Apex One and Apex Central are beyond the scope of this document, we only cover the necessary components required to enable the integration.

ClearPass Apex Central Extension Configuration options

After installing the Extension, the configuration will need to be updated. Below is an explanation of the configuration value pairs. The **logLevel**, **verifySSLCerts** should be left as their default settings unless advised by ClearPass TAC or your Aruba SE/Partner, adjust the configuration to meet your goals.

**Figure 13: List of Extension configuration options**

<table>
<thead>
<tr>
<th>Configuration attribute</th>
<th>Description</th>
<th>Example/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>logLevel</td>
<td>Used to define the level of logging with in the Extension Log file.</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>apexCentralHost</td>
<td>The host name or IP address of the Trend Micro Apex Central System. Note: This should <strong>not</strong> be a URL</td>
<td>[Host Name or IP]</td>
</tr>
<tr>
<td>applicationId</td>
<td>The Application ID generated when creating a new application in Apex Central.</td>
<td>[Application ID]</td>
</tr>
<tr>
<td>apikey</td>
<td>The API Key generated when creating a new application in Apex Central</td>
<td>[API Key]</td>
</tr>
<tr>
<td>enableEndpointCache</td>
<td>When using the auth source, should endpoints be cached</td>
<td>true/false</td>
</tr>
<tr>
<td>cacheTimeSeconds</td>
<td>If enableEndpointCache is true then this is the timeout value for when a device will be refreshed</td>
<td>1800</td>
</tr>
<tr>
<td>syncAllOnStart</td>
<td>Sync all endpoints when the extension starts</td>
<td>true/false</td>
</tr>
<tr>
<td>enableSyncAll</td>
<td>Enable a timed sync all process controlled by syncAllSchedule</td>
<td>true/false</td>
</tr>
<tr>
<td>syncAllSchedule</td>
<td>The schedule for when the Sync All Endpoints process should run. Note: This uses CRON type scheduling.</td>
<td>0 2 * * 6</td>
</tr>
</tbody>
</table>

Several of these configuration items needs to be created/collected from within Apex Central, these items are

- apexCentralHost
- applicationId
- apikey

**Pay special attention to the values in the extension configuration.** Where a configuration attribute is a Boolean value {true/false}, it must not be enclosed with literals.
**Apex Central “Application” Configuration**

To permit ClearPass to make API calls into Apex Central, you must configure an ‘application’, this become the conduit to allow the ClearPass Policy Manager Trend Micro Apex Central extension the ability to access data with in Apex Central, ingest this data with the scheduler, make real-time calls via the HTTP authorization source or trigger ‘Apex Central isolation’ actions.

Sign in to Apex Central and follow the below, **Administration > Settings > Automation API Access Settings** to create the necessary configuration.

*Figure 14: Adding an API-Application - part1*

Click on “+ Add”, define an ‘Application name’ and identity its relevancy, e.g, ‘CPPM-Integration’, the other settings, **Application ID** and **API key** are auto configured, makes copies of the Application ID and key.

*Figure 15: Adding an API-Application - part2*

Click ‘Save’ to continue.
You should see the Application defined and active, **Application ID** and **API key** can be copied from here and the ‘application’ can also be enabled/disabled if necessary, as shown below.

When copying the Application ID or API Key **ENSURE** there are no trailing or leading space if copying/pasting this directly from the below into the Extension configuration.

**Figure 16: reviewing the application configuration**

ClearPass Extension Configuration

Enter these two parameters from above into the Trend Micro ClearPass extension configuration, notice the API key is obfuscated in the configuration after being saved and re-viewed. Adjust the other configuration switches as necessary, pay attention to **enableEndpointCache, cacheTimeSeconds, syncAllOnStart, enableSyncAll** and **syncAllSchedule**.

Specific to the **syncAllSchedule** we use our standardized process of scheduling within the Extension, it's based on a slightly modified version of the CRON job scheduler found in Unix-like operating systems. It can be used to schedule jobs to run periodically at fixed times, dates or intervals.

Let's break it down. A ‘cron’ is a job scheduler. Any task that is scheduled is called a ‘cron job’, this is useful for any action that need scheduling. The syntax for a cron job schedule is as follows:

```
minute (0-59)
hour (0-23)
day of month (1-31)
month (1-12)
day of week (0-6) (Sunday is 0)
* * * * * <command to execute>
```

In our use of the cron scheduler, we've dropped the use of the last instruction `<command to execute>` and use only the time/date functions, see below for a number of examples of scheduling a sync process.

- Schedule a sync to run at 2am daily:- 0 2 * * *
- Schedule a sync to run twice a day at 5am and 5pm:- 0 5,17 * * *
- Schedule a sync to run on every Sunday at 5pm:- 0 17 * * sun
- Schedule a sync to run every 30 minutes:- */30 * * *
- Schedule a sync to run at 5pm on selected days:- 0 17 * * sun,fri

You can see from the above that the scheduling process is extremely flexible.
**Figure 17**: Setting the *Extension configuration*

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>State</th>
<th>Hostname</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro Apex Central Integration</td>
<td>1.0.0</td>
<td>Running</td>
<td>d38cca16f5b</td>
<td>172.17.0.21</td>
</tr>
</tbody>
</table>

**Extension Configuration**

```json
{
    "logLevel": "DEBUG",
    "verifySSLCert": false,
    "apexCentralHost": "10.2.100.125",
    "applicationId": "3B1D685F-5A03-49AC-8D0A-9214136ABC01",
    "apiKey": "*******",
    "enableEndpointCache": false,
    "cacheTimeSeconds": 1800,
    "syncAllOnStart": true,
    "enableSyncAll": false,
    "syncAllSchedule": "0 2 * * 6"
}
```

Provide JSON configuration parameters for the extension.

Restart: ☐ Restart extension after updating configuration

[Save Changes]
Using ClearPass Policy Manager with Apex Central

Following the deployment and configuration of the ClearPass Extension, there are several options in how to integrate with Trend Micro and use its endpoint security context.

Using endpoint data that has been synchronized and cached

The first is the simplest, use the Extension to sync data from Apex Central on a regular process, write this data into the ClearPass EndpointDb, then use the EndpointDb as the authorization source. Be aware that this data will not be completely ‘real-time’, making real-time API calls to Apex Central every time a device authenticates may not be scalable (endpoint caching will help), it will be very dependable on the customer environment.

For this use-case set the Extension config as required, in our example below we've set the schedule to run every 2-hours, sync all endpoint when the extension starts/restarts and cache the results for 30 minutes adjust as necessary for your environment.

```
"enableEndpointCache": true,
"cacheTimeSeconds": 1800,
"syncAllOnStart": true,
"enableSyncAll": true,
"syncAllSchedule": "0 */2 * * *"
```

As an example of a simple enforcement policy leveraging the EndpointDb as an authorization source the below is a simple example, first check if the end point is actually managed inside of Apex Central, if it's unknown we direct the device to an enrollment captive portal page, then make a similar check to ensure its known AND it not been set to isolate, if it's not normal, then we will quarantine the devices. The third policy item ensures the device is known, managed and is not set to be isolated so full-access is provided. Finally as an example we could utilize other context to trigger an action, you'd actually have this fourth policy in an EVENT policy, its only shown here for ease of reading but we'd trigger a context-server-action to isolate the endpoint if we perhaps received a threat alert for the endpoint, more on how to setup this up later.

**Figure 18: Enforcement policy leveraging the EndpointDb**
Using a Real-Time authorization check via HTTP authorization source

This option details how to configure and use a HTTP authorization source to provide near real-time checks on endpoints, then process the returned data from Apex-Central. Note that with an HTTP authorization source configured, ClearPass will make a call to Apex-Central (via the Extension) every time a device authenticates that matches the Service Policy which has this authorization source defined, unless the data is still fresh as determined by the cache policy then if returns cached data.

The HTTP Authorization source is the conduit between the Extension and ClearPass Policy Manager. It's through the authorization source that we expose the Apex-Central endpoint attributes to Policy Manager so they can be used to perform role-mapping or enforcement policy action. Multiple use-cases exist for how Policy Manager can utilize the returned data in Policy, such as those describe in the previous section.

For this feature, set the Extension config, in our example below we've disabled the scheduled sync but we have maintained the ability to cache the results for 30 minutes adjust as necessary for your environment.

```
{"enableEndpointCache": true,
"cacheTimeSeconds": 1800,
"syncAllOnStart": false,
"enableSyncAll": false,
"syncAllSchedule": "0 */2 * * *"
```

Following on from setting the configuration in the extension, below is a copy of the HTTP authorization source you can use to trigger a query into the Extension {client mac-address}. The first step is to add the authorization source. Under Configuration > Authentication > Sources, click Add and choose type HTTP.

**Type**  
HTTP

**Base URL**  
http://IP_of_my_Trend_Extension

**Login Username**  
notused_but_must_be_set

**Login Password**  
notused_but_must_be_set

*Figure 19: Authorization Source for real-time check*

<table>
<thead>
<tr>
<th>Authentication Sources - trendmicro-authZ-src</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td><strong>General:</strong></td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>Type:</td>
</tr>
<tr>
<td>Use for Authorization:</td>
</tr>
<tr>
<td>Authorization Sources:</td>
</tr>
<tr>
<td><strong>Primary:</strong></td>
</tr>
<tr>
<td>Base URL:</td>
</tr>
<tr>
<td>Login Username:</td>
</tr>
<tr>
<td>Login Password:</td>
</tr>
<tr>
<td>Timeout:</td>
</tr>
<tr>
<td><strong>Attributes:</strong></td>
</tr>
<tr>
<td>Filters:</td>
</tr>
</tbody>
</table>
Under attributes define the Attributes and the query string, pay special attention to the filter-query

?macAddress=%{Connection:Client-Mac-Address-Upper-Hyphen}

In Appendix A is an XML copy of this HTTP authentication source, you need to adjust your base-url to match your Trend Micro extension.

**Figure 20:** Authorization Source attribute and query definition

Below is an example of an Enforcement Policy that leverages a real-time authorization check.

**Figure 21:** Enforcement policy leveraging the HTTP Authorization-source
Triggering an isolation/restore action via Apex-Central

The concept behind the isolation action is that ClearPass has received an update/message to indicate an infected endpoint, the desired action might be to typically change the Aruba-Role or drop the endpoint into a new VLAN via a Dynamic Authorization request, the option detailed below is an additional option to leverage the capabilities of an Apex Central/Apex One framework.

Configuring ClearPass to trigger isolation actions

Create a Context-Server as below point at the IP address of the extension, ensure you configure this as http.

*Figure 22: Context-Server definition isolate/restore function*

![Context-Server definition isolate/restore function](image)

Next configure a Content-Server-Action, ensure you set the method as GET and the base URL is correct, `/isolate/%{Connection:Client-Mac-Address-NoDelim}`

*Figure 23: Context-Server-Action isolate*

![Context-Server-Action isolate](image)
This is the basic configuration, how this is triggered depends on how you want to utilize this in policy, you could tie this this an IEE syslog event, perhaps a UEM endpoint check at authentication time that determines a macOS endpoint is running non-approved software and as such you trigger the profile shown below.

**Configuring ClearPass to trigger restore actions**

The process to restore an isolate endpoint is to use the same Context-Server but use a different Content-Server-Action with a restore base-URL, see below.

**Figure 24: Context-Server-Action restore**

<table>
<thead>
<tr>
<th>Action</th>
<th>Header</th>
<th>Content</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type:</td>
<td>Generic HTTP Context Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Name:</td>
<td>172.17.0.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action Name:</td>
<td>trendmicro-trigger-restore-csa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Method:</td>
<td>GET</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Method:</td>
<td>Basic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL:</td>
<td>/restore/%(Connection.CLIENT-MAC-Address-NoDelim)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Enforcement Profile**

**Figure 25: Enforcement Profile calling isolation CSA**

<table>
<thead>
<tr>
<th>Profile:</th>
<th>Profile</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>trendmicro-trigger-isolation-profile (not post_auth)</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type:</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>Action:</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>Device Group List:</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attributes:</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Target Server</td>
<td>172.17.0.21</td>
</tr>
<tr>
<td>2. Action</td>
<td>trendmicro-trigger-isolate-csa</td>
</tr>
</tbody>
</table>
Appendix A – Copy of the HTTP authentication source in XML

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
  <TipsHeader exportTime="Fri Mar 13 11:49:29 PDT 2020" version="6.8"/>
  <AuthSources>
    <AuthSource description="" name="trendmicro-authZ-src" isAuthorizationSource="true" type="HTTP">
      <NVPair value="http://extension_ip_address_change_me" name="base_url"/>
      <NVPair value="notused" name="username"/>
      <NVPair value="notused" name="password"/>
      <NVPair value="60" name="timeout"/>
      <Filters>
        <Filter paramValues="" filterQuery="?macAddress=%{Connection:Client-Mac-Address-Upper-Hyphen}" filterName="trend">
          <Attributes>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Product" attrName="Trend Micro Product"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Entity ID" attrName="Trend Micro Entity ID"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Managing Server ID" attrName="Trend Micro Managing Server ID"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Folder Path" attrName="Trend Micro Folder Path"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro IP Address List" attrName="Trend Micro IP Address List"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro MAC Address List" attrName="Trend Micro MAC Address List"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Host Name" attrName="Trend Micro Host Name"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Isolation Status" attrName="Trend Micro Isolation Status"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro Last Update" attrName="Trend Micro Last Update"/>
            <Attribute isUserAttr="false" isRole="false" attrDataType="String" aliasName="Trend Micro System Found" attrName="Trend Micro System Found"/>
          </Attributes>
        </Filter>
      </Filters>
    </AuthSource>
  </AuthSources>
</TipsContents>
Appendix B – Additional Diagnostics and Support

Checking on the Extension Service

The ClearPass Extensions are supported by a new system service added in 6.6. This service must be running.

**Note:** Restarting this service will affect all deployed and running extensions.

To check on the state of the Extension Service, or to restart the service, go to Administration > Server Manager > Server Configuration > [SERVER] > Service Control. By default this service is automatically started.

*Figure 26: Services Control*

Extension Logs/Debugging

If you have a requirement to access and view the logs from the Extension, you can view or amend different logging levels direct inside the extension configuration. It's just a matter of updating the configuration and restarting it. For example, the configuration below sets the `logLevel` to DEBUG.

```
{
    "logLevel": "DEBUG",
    "verifySSLCerts": false,
    "apexCentralHost": "10.2.100.125",
    "applicationId": "3B1D885F-5A03-49AC-8D0A-9214136ABC01",
    "apiKey": "********",
    "enableEndpointCache": false,
    "cacheTimeSeconds": 1800,
    "syncAllOnStart": true,
    "enableSyncAll": false,
    "syncAllSchedule": "0 2 * * 6",
}
```
Accessing the extension logs using ‘Collect Logs’ system function

In addition to viewing the logs as shown above, logs can also be collected and examined via the Policy Manager Collect Logs system function (Administration > Server Manager > Server Configuration > [Select SERVER] > Collect Logs). This is useful should you have a need to call for technical assistance.

If the support team needs to investigate a system issue, one of the items they regularly ask for is the system logs to aid with their diagnostic investigation. By default the “logLevel” is set to INFO, but TRACE, DEBUG, INFO, WARN, ERROR, FATAL can also be set as required. Locate the running extension-Id as in the below graphic.

**Figure 27: Locating the extension instance ID**

![Extension Details]

After the logs have been collected, downloaded and expanded, you can locate the extension logs in the following location in the folder structure PolicyManagerLogs > extension > <your_Instance_ID>

**Figure 28: Locating the Extension logs from ‘Collect Logs’ diagnostic GZ file**