Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-01</td>
<td>Feb 2019</td>
<td>Arpit Bhatt</td>
<td>Initial Release</td>
</tr>
<tr>
<td>2019-02</td>
<td>July 2019</td>
<td>Arpit Bhatt</td>
<td>Changed content for v2 of the Extension</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Update Screenshots for BigFix branding. Restricted BigFix account permissions required for integration.</td>
</tr>
</tbody>
</table>

Copyright

©Copyright 2019 Hewlett Packard Enterprise Development LP.

Open Source Code

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

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

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.
Contents
Introduction and Overview ........................................................................................................ 5
Pictorial View of the Integration ................................................................................................ 5
Software Requirements .................................................................................................................. 6
Installation and Deployment Guide ............................................................................................ 6
Access to the Extension Store ..................................................................................................... 7
New Extension Support in ClearPass 6.7+ .................................................................................. 7
  Extensions and IP address configuration support .................................................................... 7
  Extensions and web proxy support ......................................................................................... 7
BigFix Extension Installation and Configuration ........................................................................ 9
BigFix as an Authorization Source ............................................................................................ 16
Appendix A – Additional Diagnostics and Support ................................................................. 20
  The Extensions Service ........................................................................................................... 20
  Extension logs and debugging ............................................................................................... 20
  Accessing extension logs within ClearPass ’Collect Logs’ .................................................... 21
Appendix B – BigFix configuration ........................................................................................... 22
Appendix C – XMLs ...................................................................................................................... 24
Figures
Figure 1: Pictorial view of ClearPass Policy Manager integration with BigFix ................................................................. 5
Figure 2: Entering HP Passport credentials .................................................................................................................. 7
Figure 3: Extension framework GUI ............................................................................................................................. 8
Figure 4: Defining the base IP SUBNET and LOCALHOST for the Extensions framework ................................................. 8
Figure 5: Extensions framework GUI ............................................................................................................................. 9
Figure 6: GUI Extension search ....................................................................................................................................... 9
Figure 7: GUI Extension install ....................................................................................................................................... 10
Figure 8: GUI Extension configuration at install time .................................................................................................. 10
Figure 9: Extension configuration parameters ........................................................................................................... 11
Figure 10: Creating an Admin user on ClearPass........................................................................................................ 12
Figure 11: GUI review and setting the Extension configuration ...................................................................................... 13
Figure 12: Show Details for the Extension .................................................................................................................... 13
Figure 13: Extension URLs ............................................................................................................................................. 14
Figure 14: Log validation ............................................................................................................................................... 15
Figure 15: Attributes fetched ......................................................................................................................................... 15
Figure 16: Authentication Source – General tab ........................................................................................................ 16
Figure 17: Authentication Source – Primary tab .......................................................................................................... 16
Figure 18: Authentication Source – Attribute Filters ................................................................................................. 17
Figure 19: Authentication Source – Attribute Filters modified .................................................................................... 18
Figure 20: Service Configuration – Enable Authorization .......................................................................................... 18
Figure 21: Service Configuration – Authorization tab ................................................................................................ 19
Figure 22: Service Configuration – Enforcement tab .................................................................................................. 19
Figure 23: Checking on the extensions service and how to stop the service .............................................................. 20
Figure 24: Using the GUI to change the DEBUG level ................................................................................................ 20
Figure 25: Extension logs location in 'Collect Logs' diagnostic GZ file ........................................................................ 21
Figure 26: Create a BigFix Operator ............................................................................................................................. 22
Figure 27: BigFix Operator Permission – Details 1 ....................................................................................................... 22
Figure 28: BigFix Operator Permission – Details 2 ....................................................................................................... 23
Figure 29: BigFix Operator Permission – Details 3 ....................................................................................................... 23
Figure 30: BigFix Operator Permission – Computer Assignments ................................................................................ 23
Figure 30: BigFix Operator Permission – Sites .............................................................................................................. 23
Figure 30: Import Authentication Source ...................................................................................................................... 24
Introduction and Overview

BigFix is one of the leading endpoint management and security platforms. It quickly identifies and discovers information about endpoints, patches operating systems and monitors the inventory continuously to ensure compliance of endpoints in the infrastructure. BigFix aims at keeping the endpoints secure by ensuring they are patched on the network. Unpatched systems are a big threat to organizations as hackers frequently look for ways to leverage known vulnerabilities for malicious activities.

It has a rich set of device attributes gathered from the agents running on an endpoint. These attributes can be used by ClearPass Policy Manager to get more context for the endpoint trying to connect onto the network. Unpatched or non-compliant systems can be sent to a Quarantine zone to ensure they do not have access to valuable assets on the network.

This integration guide covers the deployment and configuration of a ClearPass Extension to interface with BigFix. The Extension leverages BigFix APIs to obtain attributes associated with an endpoint. This allows the Extension to provide the following integration capabilities.

1. Periodic Poll: enable periodic polling of endpoints in BigFix with a valid mac address. This allows Policy Manager to access a number of endpoint attributes which can be leveraged for creating policies. For example
   a. Check if the endpoint is known to BigFix
   b. Check if the Last Update was less than 7 days
   c. Check if the endpoint has been locked by BigFix

2. Authorization source: trigger the Extension to get the attributes for the authenticated endpoint.

Pictorial View of the Integration

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

**Figure 1:** Pictoral view of ClearPass Policy Manager integration with BigFix
Software Requirements

The minimum software version required for ClearPass is 6.7.2. At the time of writing, ClearPass 6.7.9 is the latest available and recommended release. Any subsequent ClearPass software release will support this integration. ClearPass runs on either hardware appliances with pre-installed software, or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

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

The BigFix console version used to verify interoperability for this guide was 9.5.9.62.

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 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 2: Entering HP Passport credentials**

![ClearPass Policy Manager](image)

New Extension Support in ClearPass 6.7+

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

**Extensions and IP address configuration support**

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

**Extensions and web proxy support**

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

---

**NOTE**

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

Configuring the base Extension IP subnet, this is defined within Policy Manager as shown below under Administration -> Server Manager -> Server Configuration [choose 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.
BigFix Extension Installation and Configuration

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

Figure 5: Extensions framework GUI

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

Figure 6: GUI Extension search

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

**Figure 7: GUI Extension install**

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

**Figure 8: GUI Extension configuration at install time**
After the Extension has been installed, review the configuration and adjust as needed. Notice the options to Start, Delete, Reinstall or Show Logs and the option to edit and set the Extension configuration.

The default configuration used for v2 of the extension is below:

```
{
    "bigFixHost": "{{BigFix IP or Domain}}",
    "bigFixPort": 52311,
    "bigFixUserName": "{{BigFix User Name}}",
    "bigFixPassword": "********",
    "bigFixAdditionalProperties": [],
    "bigFixIncludePatchSummary": false,
    "enableEndpointCache": false,
    "cacheSync": false,
    "cacheSyncSchedule": "0 5 * * 1",
    "syncOnStart": false,
    "cppmUserName": "{{Admin User Name}}",
    "cppmPassword": "********",
    "verifySSLCerts": true,
    "logLevel": "INFO"
}
```

BigFix v2 of the extension provides the ability to fetch the patch summary for an endpoint. This is an important attribute for policy decisions. This was not possible using v1 of the extension. The configuration option used to enable this is "bigFixIncludePatchSummary".

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

**Figure 9: Extension configuration parameters**

<table>
<thead>
<tr>
<th>Configuration attribute</th>
<th>Description</th>
<th>Example/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>bigFixHost</td>
<td>The host name or IP address of your BigFix system.</td>
<td>Example: 192.168.1.10 or bigfix.arubasecurity.net</td>
</tr>
<tr>
<td>bigFixPort</td>
<td>The port number for the BigFix API</td>
<td>Default is 52311</td>
</tr>
<tr>
<td>bigFixUserName</td>
<td>The user name of an account in BigFix with access to Computer Properties and the Query API</td>
<td>Username for account created in Figure 6</td>
</tr>
<tr>
<td>bigFixPassword</td>
<td>The password for the user entered in the bigFixUserName setting.</td>
<td>Password for account created in Figure 6</td>
</tr>
<tr>
<td>bigFixAdditionalProperties</td>
<td>A JSON array of additional properties to pull from BigFix. We pull a set of default properties that cannot be removed, but additional values can be added as desired.</td>
<td>The format is: [&quot;Property Name&quot;, &quot;Property Name&quot;]</td>
</tr>
<tr>
<td>bigFixIncludePatchSummary</td>
<td>Enables the extension to add patch summary information to device attributes. The patch summary is the numeric integer for missing patches classified as Critical, Important, Moderate and Low.</td>
<td>true/false</td>
</tr>
<tr>
<td>enableEndpointCache</td>
<td>Enables the endpoint cache process when performing a single MAC Address or IP Address based device lookup.</td>
<td>true/false</td>
</tr>
</tbody>
</table>
When leveraging the sync capabilities of the Extension to get the device attributes from BigFix, use the attribute enableCacheSync and specify cacheSyncSchedule. These 2 attributes are leveraged for periodic poll of endpoints from BigFix. The syncOnStart attribute can be leveraged as well to sync everything upon the start of the extension.

The bigFixUserName and bigFixPassword are credentials of the operator on BigFix which will give access to endpoints discovered by BigFix via REST APIs. A default administrator account can be used for this setup or a separate local operator can be created. For steps on creating this operator on BigFix, refer Appendix B.

The cppmUserName and cppmPassword should be for an Administrator account. The device profiling attributes obtained from BigFix need to be written into the endpoint repository leveraging the REST APIs which requires an Administrator account.

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

**Figure 10: 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 BigFix Extension with the desired configuration is shown below, this has to be modified for your deployment. Include the `bigfixHost`, `bigfixPort`, `bigfixUserName`, `bigfixPassword`, `cppmUserName` and `cppmPassword` 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 11: GUI review and setting the Extension configuration**

An interesting optional parameter to note here is `bigfixAdditionalProperties`. By default, the parameter has the value of `[]` which basically indicates that the sync would only get the default attributes. However, BigFix does fetch a huge list of attributes from an endpoint. All of these attributes might not be very useful for ClearPass and would increase the payload to be captured from BigFix. Customization options are available with this parameter so that an administrator can pull values apart from the default which are important in their environment. Navigate to the BigFix Extension and click on **Show Details** as shown below.

**Figure 12: Show Details for the Extension**
Click on the Extension URL under the details. This gives a list of all the attributes that can be fetched from BigFix. If the information is available for the endpoint on BigFix, ClearPass can pull it.

**Figure 13: Extension URLs**

The URL above gives a long list of available attributes. The ones marked in bold are mandatory and fetched by default. If any of the other properties are useful in a particular environment it can be fetched using the `bigFixAdditionalProperties` parameter. This can be then be leveraged in the Policy.

For example, here we have added BIOS and Client Settings to the list of additional attributes that need to be fetched from BigFix.

Following is the change in the Extension configuration. Remember this change is only required if additional attributes need to be fetched from BigFix. This can be totally skipped for the basic setup of this integration.

```json
{
    "bigFixHost": "10.2.98.40",
    "bigFixPort": 52311,
    "bigFixUserName": "admin",
    "bigFixPassword": "********",
    "bigFixAdditionalProperties": [
        "Client Settings",
        "BIOS"
    ],
    "bigFixIncludePatchSummary": true,
    "enableEndpointCache": true,
    "enableCacheSync": true,
    "cacheSyncSchedule": "0 5 * * 1",
    "syncOnStart": true,
    "cppmUserName": "admin",
    "cppmPassword": "********",
    "verifySSLCerts": false,
    "logLevel": "INFO"
}
```
Ensure the Extension is restarted upon a configuration change. After the restart of the extension, click on Show Logs.

**Figure 14: Log validation**

```plaintext
bigFixIncludePatchSummary": true,
"enableEndpointCache": false,
"enableCacheSync": false,
"cacheSyncSchedule": "0 * * 1",
"syncOnStart": true,
"cppnUserName": "admin",
"cppnPassword": "*********",
"verifySSLcert": true,
"logLevel": "INFO"
}
```

The above log states that the Extension has sync’d the endpoint data from BigFix. The above steps sync endpoint details at the time of starting the Extension and then regular updates are fetched at the interval specified by `cacheSyncSchedule`.

Please note the IP address of the Extension. This will be used in the next section where we leverage BigFix Extension as an Authorization source. A sample of attributes fetched for an endpoint is shown below.

**Figure 15: Attributes fetched**

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Attributes</th>
<th>Device Fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. BigFix Agent Version</td>
<td>9.5.9.62</td>
<td></td>
</tr>
<tr>
<td>3. BigFix BES Root Server</td>
<td>av-bigfix (0)</td>
<td></td>
</tr>
<tr>
<td>4. BigFix Computer Name</td>
<td>WIN10-2</td>
<td></td>
</tr>
<tr>
<td>5. BigFix Computer Type</td>
<td>Virtual</td>
<td></td>
</tr>
<tr>
<td>6. BigFix Device Type</td>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>7. BigFix ID</td>
<td>7209:15</td>
<td></td>
</tr>
<tr>
<td>8. BigFix IP Address</td>
<td>10.2.100.217</td>
<td></td>
</tr>
<tr>
<td>9. BigFix IPv6 Address</td>
<td>fe80:0:0:0::e805:dc0:6f0:66</td>
<td></td>
</tr>
<tr>
<td>10. BigFix Is Found</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>11. BigFix Last Report Time</td>
<td>Tue, 02 Jul 2019 20:31:34 +0000</td>
<td></td>
</tr>
<tr>
<td>13. BigFix Locked</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>14. BigFix MAC Address</td>
<td>00:50-56-99-2b-7d</td>
<td></td>
</tr>
<tr>
<td>15. BigFix Missing Patches - Critical</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>16. BigFix Missing Patches - Important</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>17. BigFix Missing Patches - Low</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>18. BigFix Missing Patches - Moderate</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

*Added in v2*
BigFix as an Authorization Source

The integration can also be used leveraging BigFix as an Authorization source. In this scenario, the Extension makes an API call for an endpoint at the time of authentication of the client to get it’s attributes from BigFix. These attributes can then be leveraged for Authorization. The benefit of this method is that it allows for real-time fetching of attributes and hence the authorization policies applied are based on real-time data available on BigFix. In order to use this, it is mandatory to install the Extension first. The steps for this installation are covered in the previous section. The options to sync the endpoint attributes can be skipped if leveraging BigFix as an Authorization source.

In order to use BigFix Extension as an Authorization source, add an HTTP Authentication source in ClearPass. The following steps of adding the Authentication Source can be skipped and can be directly imported using the XML available on Aruba GitHub. Refer Appendix C for details.

Navigate to Configuration > Authentication > Sources. Click on Add

Figure 16: Authentication Source – General tab

![Figure 16: Authentication Source – General tab](image)

Figure 17: Authentication Source – Primary tab

![Figure 17: Authentication Source – Primary tab](image)
Notice that the Base URL here leverages the Extension IP captured in the previous section while installing the BigFix Extension. Hence ClearPass Policy Manager makes an internal API call to the Extension which leverages the BigFix APIs to fetch the endpoint attributes. The credentials are not required as this is an internal API call but has to be defined to a random value since it’s a mandatory setting for adding an Authentication source.

The next tab is the Attributes tab which basically specifies the attributes that can be leveraged as Authorization attributes under the service created. Click on Attributes tab and then on “Add More Filters”. Configure the filters that are required for Authorization as shown below.

As mentioned before, to avoid going through the hassle of manually configuring these filters, please download the XML from Aruba GitHub and import the Authentication source.

**Figure 18: Authentication Source – Attribute Filters**

In the previous section, we discussed about an optional parameter called `bigFixAdditionalProperties`. It is used to fetch more attributes than the ones available above. In order to use that attribute with Authorization source it is necessary to add the same using the option “Add More Filters”. Without doing this, it will not be available for use with Authorization.
Let’s look at the example below where the BigFix Missing Patches – Critical attribute fetched in v2 of the extension is mapped within the Authorization source as shown below.

**Figure 19: Authentication Source – Attribute Filters modified**

Let’s look at the service configuration within ClearPass to see how this HTTP source can be leveraged as an Authorization source within a service. Ensure we check the option for enabling Authorization as shown below.

**Figure 20: Service Configuration – Enable Authorization**
The next step is to add this source under Authorization. The Authorization tab for the service is shown below.

**Figure 21: Service Configuration – Authorization tab**

![Service Configuration - Authorization tab](image)

Finally, the authorization source is leveraged under Enforcement for the policies to be defined. A sample Enforcement Policy for this service is shown below.

**Figure 22: Service Configuration – Enforcement tab**

![Service Configuration - Enforcement tab](image)

In the above policy if BigFix marks an endpoint as **Locked**, the endpoint is assigned a **Quarantine role** with restricted Access. A full access role is granted only if the Endpoint "**Is Found**" by BigFix. If not, a default of **[Deny Access Profile]** is assigned.
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 23: Checking on the extensions service and how to start/stop the service

Extension logs and debugging

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

Figure 24: Using the GUI to change the DEBUG level
Remember after changing the logging level, the extension will need to be restarted for this change to take effect.

**Accessing extension logs within ClearPass ‘Collect Logs’**

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

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

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

*Figure 25: Extension logs location in ‘Collect Logs’ diagnostic GZ file*
Appendix B – BigFix configuration

It is assumed that a working BigFix environment is leveraged for this extension. The configuration of BigFix is beyond the scope of this guide.

The Extension configuration requires a valid BigFix administrator account to leverage BigFix APIs. This account can be created on BigFix as shown below.

Go to Tools Menu on top of your screen and click on “Create Operator”. Add a user with credentials as shown below.

*Figure 26: Create a BigFix Operator*

The next step involves assigning permissions for this account. It is important that the account has the permissions for “Can use REST API”. Also, the account should have a list of “Administered Computers”. In our lab, a user with restricted permissions was used and should be preferred. For details on this, please contact your local BigFix representative.

Under the “Details” tab for this account, provide restricted access as shown below.

*Figure 27: BigFix Operator Permission – Details 1*

If there are permission issues when trying to fetch computers, one can check or troubleshoot by giving this account the Master Operator permission as shown below or use an administrator account for testing only.
Navigate to the “Computer Assignments” tab. Add the computers in scope for this Extension or select all computers. It is important that after the settings are saved, the “Administered Computers” tab gets updated. An empty list of Administered Computers would always result in extension fetching no computers.

Further restrictions can be assigned by to this account by granting a Reader permission only to the sites within the scope.
Appendix C – XMLs

The Authentication Source can be easily imported into ClearPass so that it can be leveraged to use the BigFix Extension as an Authorization source in a service. The XML file can be downloaded from

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

- Download the XML profile > “clearpass-extension_tenable-securitycenter_enf-profile.xml”.
- Open this file in your favorite editor.
- Use the Find and Replace feature of the editor to replace "<BigFix Extension IP>" with the actual IP address of the BigFix Extension configured. Refer Figure 24.
- Save the file and Import.

The file can be imported from Configuration > Enforcement > Profiles.

Figure 32: Import Authentication Source

The above action will import an HTTP Authentication Source in ClearPass which can be leveraged as an Authorization source for a service.