Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>May 2019</td>
<td>Danny Jump</td>
<td>First Published Version – Phase1</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 .................................................................................................................................................. 5
Software Requirements ............................................................................................................................. 5
Installation and Deployment Guide ........................................................................................................ 5
Pictorial view of the Integration .............................................................................................................. 6
Configuration ................................................................................................................................................ 7
  Configuration of ClearPass ....................................................................................................................... 7
  Create a ClearPass ‘API’ User ................................................................................................................. 7
  Create a ClearPass Operator Profile ....................................................................................................... 8
  Create a ClearPass OAuth API Client ..................................................................................................... 10
  Configuration of CyberX ......................................................................................................................... 11
Monitoring/Reviewing ClearPass and CyberX communications .............................................................. 16
Figures

Figure 1: Pictorial view of ClearPass Policy Manager integration with CyberX.......................................................... 6
Figure 2: Create an API level account in ClearPass.................................................................................................... 7
Figure 3: Creating a restricted access Operator Profile – Part1 .................................................................................. 8
Figure 4: Creating a restricted access Operator Profile – Part2 .................................................................................. 9
Figure 5: Create an API Client .................................................................................................................................. 10
Figure 6: CyberX Main Dashboard.............................................................................................................................. 11
Figure 7: Configuring communication with ClearPass............................................................................................... 12
Figure 8: Definition of ClearPass communication options........................................................................................... 12
Figure 9: Endpoint Dictionary Attributes created by CyberX ....................................................................................... 13
Figure 10: Example of Endpoints created by CyberX................................................................................................. 13
Figure 11: Normalized Endpoint data created by CyberX............................................................................................ 14
Figure 12: Custom Endpoint data created by CyberX................................................................................................. 14
Figure 13: Reviewing 'Last Sync' time to ClearPass................................................................................................... 16
Figure 14: Example of API logs between CyberX and ClearPass.................................................................................. 16
Introduction

This Integration Guide covers the configuration and use of the integration between CyberX and ClearPass Policy Manager. The CyberX platform delivers continuous ICS threat monitoring and asset discovery, combining a deep embedded understanding of industrial protocols, devices, and applications with ICS-specific behavioral anomaly detection, threat intelligence, risk analytics, and automated threat modeling. This initial integration between CyberX and ClearPass focuses on the ability for CyberX to detect, discover and classify OT/ICS endpoints and share this classification directly with ClearPass via the ClearPass Security Exchange framework and the open API we expose. CyberX will automatically update the ClearPass Policy Manager Endpoint Database with endpoint classification data and a number of custom security attributes.

This is Phase1 of our planned integration with CyberX, centralized visibility of network assets and endpoints across IT and OT infrastructure. From here a centralized endpoint and edge security policy can be defined and administered. Check back for updates to our CyberX integration framework.

Software Requirements

At the time of writing, ClearPass version 6.8.0 is available and the recommended release. CPPM runs on hardware appliances with pre-installed software or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.5, 6.0, 6.5, 6.6 or higher
- Microsoft Hyper-V Server 2012 R2 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 R2 or 2016 R2
- KVM on CentOS 7.5 or later.

The minimum version of CyberX required is, 2.5.1 that supports the integration features.

Installation and Deployment Guide

The generic ClearPass installation and deployment guide is located here:

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 CyberX*

CyberX synchronizes its asset inventory list into the ClearPass Endpoint Database. The device context can be used for Dynamic Segmentation leveraging policy.

Discovered OT/ICS devices are pushed into the ClearPass Policy Manager Endpoint Database leveraging the endpoint REST API’s. The sync schedule can be configured.
Configuration

Configuration of ClearPass

Prior to creating and enabling the integration in CyberX a number of configuration elements need to be pre-created in ClearPass. Follow the below configuration steps carefully, collecting data as highlighted as you will need this in the following section when configuring CyberX to communicate with ClearPass.

Create a ClearPass ‘API’ User

As part of the communications channel between the two products, CyberX will use a number of API’s (both TIPS and REST), access to the TIPS API’s is validated via Username/Password combination credentials. This user Id needs to have minimum levels of access, do not use a Super Administrator profile, use API Administrator as shown below.

Create a user from Administration -> Users and Privileges -> +ADD -> {Create a user, ensure that you set a privilege level of API Administrator}

Make a note of the User Id and the password that was configured, ensure Privilege level is API Administrator

Figure 2: Create an API level account in ClearPass
Create a ClearPass Operator Profile

CyberX also uses the REST API’s as part of the integration, REST API’s are authenticated under an OAuth framework. Create as shown below an API Client. To secure access to only the REST API for the API Client create a restricted access Operator Profile as shown below. In summary all options are set as ‘No Access’ except for API Services and Policy Manager, which is custom and then specific as shown below.

Under API Services

- **Allow API Access** = Allow Access

Under Policy Manager

- **Dictionaries – Attributes** = Read, Write, Delete
- **Dictionaries – Fingerprints** = Read, Write, Delete
- **Identity – Endpoints** = Read, Write, Delete

*Figure 3: Creating a restricted access Operator Profile – Part1*
Figure 4: Creating a restricted access Operator Profile – Part 2

Policy Manager

Select operator permissions for Policy Manager

- Application Licenses
  - Operators with this privilege can manage Application Licenses
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Authentication - Methods
  - Operators with this privilege can manage authentication methods
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Certificate - Revocation List
  - Operators with this privilege can manage Revocation Lists
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Certificate - Trust List
  - Operators with this privilege can manage certificate trust lists
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Certificates
  - Operators with this privilege can manage certificates
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Clearpass Portal
  - Operators with this privilege can manage Clearpass Portal
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Configuration - Network Scan
  - Operators with this privilege can manage Network Scan under Configuration
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Configuration - Services
  - Operators with this privilege can manage Services under Configuration
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Dictionaries - Attributes
  - Operators with this privilege can manage attributes
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Dictionaries - Context Server Actions
  - Operators with this privilege can manage context server actions
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Dictionaries - Fingerprints
  - Operators with this privilege can manage fingerprints
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Events - Login Audit
  - Operators with this privilege can manage login audits
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Events - System Events
  - Operators with this privilege can manage system events
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- External Servers - Endpoint Context Servers
  - Operators with this privilege can manage endpoint context servers
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- External Servers - File Backup Server
  - Operators with this privilege can manage file backup servers
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- External Servers - SNMP trap receivers
  - Operators with this privilege can manage SNMP trap receivers
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- External Servers - Syslog Export Filters
  - Operators with this privilege can manage syslog export filters
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- External Servers - Syslog Targets
  - Operators with this privilege can manage syslog targets
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete

- Identity - Endpoints
  - Operators with this privilege can manage endpoints
    - No Access
    - Read
    - Read, Write
    - Read, Write, Delete
Create a ClearPass OAuth API Client

Next create an API Client Guest -> Administration -> API Services -> API Clients -> {Create API Client}

Ensure you use the Operator Profile previously created to restrict the capabilities of the API Client.

Notice the highlighted configuration options needed, and set as appropriate

- **Operating Mode** = ClearPass REST API – Client will be used for API calls to ClearPass
- **Operator Profile** = Use the Profile you created previously
- **Grant Type** = Client credentials (grant_type = client_credentials)

Ensure you record the Client Secret and the ACTUAL API-Client name i.e. cyberx-rest as below

**Figure 5: Create an API Client**

At this time all of the necessary config has been created in Policy Manager, ensure you collected the below list of information before proceeding to the next section.

- CPPM UserID
- CPPM UserId Password
- CPPM OAuth2 API Client NAME
- CPPM OAuth2 API Client Secret
Configuration of CyberX

For this initial integration between the two products, there is limited configuration required on CyberX. After the configuration is complete the CyberX platform will continue to update the ClearPass Policy Manager EndpointDb as it discovers new endpoints. Follow the below to configure and enable the integration.

From the CyberX main console follow the **System Settings -> Integrations -> ClearPass**

*Figure 6: CyberX Main Dashboard*

After clicking on ‘ClearPass’ the following screen is shown, configure as required the integration, all fields are required. Below is an explanation of these fields. Notice that the Last Sync is Unknown, ensure you Enable Sync at this time, if you forget or have a need to disable it you can go back to this screen to enable/disable at a later date.
As part of enabling the above integration, CyberX will create a number of custom Endpoint Dictionary attributes using the ClearPass REST API, /attribute. This is a record of the Dictionary Attributes created by CyberX, these custom attributes can then be used for role-mapping/enforcement actions in a Service Policy.
Figure 9: Endpoint Dictionary Attributes created by CyberX

The Endpoint data is sent by CyberX, it creates the Endpoints, sets the endpoint classification and also configures custom endpoint attributes. An example of the data sent is below.

Figure 10: Example of Endpoints created by CyberX

Looking closer at the endpoint data we can see several important things, the mac-address, mac-vendor, and some endpoint classification as determined by CyberX, other valuable data such as the date the endpoint was added and profiled, said another way the time CyberX updated ClearPass with the devices data.
In addition to the standard data, CyberX supplies other customer attributes, clicking on the Attribute tab provides the below attributes, any of this data could be used in Policy.

**Figure 11: Normalized Endpoint data created by CyberX**

![Normalized Endpoint data created by CyberX](image)

In addition to the standard data, CyberX supplies other customer attributes, clicking on the Attribute tab provides the below attributes, any of this data could be used in Policy.

**Figure 12: Custom Endpoint data created by CyberX**

![Custom Endpoint data created by CyberX](image)

One special attribute the "cyberx Authorized" flag is a way to distinguish known, recognized devices operating on the network from new, unexpected and potentially rogue devices that are detected. Devices that are imported into the system from the customer's inventory list, or discovered during the learning phase, would have authorized=true, and new devices that are seen on the network after the learning phase ended would be added with authorized=false, until an administrator reviewed the device, decided it's a valid device operating on the network, at which point he could set it to authorized=true. So the unauthorized devices are either unrecognized and potentially untrusted/malicious, or just haven't yet been "handled" by the administrator to authorize their presence on the network.
Another special attribute is the “cyberx_engineeringStation”, used to signify the function of an node in an OT/ICS system that is monitoring and being used to query/control OT devices. EngineeringStations should be protected and access to these devices specifically controlled and monitored. Knowing which devices on the network are signified for this role is important.
Monitoring/Reviewing ClearPass and CyberX communications

Once the sync has started endpoint data will be populated directly into the Policy Manager Endpo, you can view the last update time from the integration configuration screen, see below for an example.

*Figure 13: Reviewing 'Last Sync' time to ClearPass*

![Last Sync: May 24, 2019 4:49:16 PM](image)

If the Sync is not working or shows an error then it’s likely you’ve missed capturing some of the information, recheck the data recorded, additionally you can view the API calls between CyberX and ClearPass from Guest-> Administration-> Support-> Application Log below an example of API’s from CyberX to ClearPass.

*Figure 14: Example of API logs between CyberX and ClearPass*