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>Arpit Bhatt</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
  ClearPass Configuration ....................................................................................................................... 7
    Create a ClearPass User ....................................................................................................................... 7
  Create an Operator Profile .................................................................................................................. 7
  Create an API Client .............................................................................................................................. 9
  Indegy Configuration ........................................................................................................................... 10
Integration Results .................................................................................................................................. 12
Monitoring/Reviewing ClearPass and Indegy communications ......................................................... 14
Figures

Figure 1: Pictorial view of ClearPass Policy Manager integration with Indegy ................................................................. 6
Figure 2: Create an API level account in ClearPass ........................................................................................................ 7
Figure 3: Operator Profile - Access restrictions 1 ........................................................................................................... 8
Figure 4: Operator Profile - Access restrictions 2 ........................................................................................................... 8
Figure 5: Operator Profile - Access restrictions 3 ........................................................................................................... 9
Figure 6: Create an API Client ........................................................................................................................................ 9
Figure 7: Indegy Configuration Console ........................................................................................................................ 10
Figure 8: Endpoint Dictionary Attributes created by Indegy ............................................................................................. 12
Figure 9: Example of Endpoints created by Indegy ........................................................................................................ 12
Figure 10: Normalized Endpoint data created by Indegy ................................................................................................. 13
Figure 11: Custom Endpoint data created by Indegy ....................................................................................................... 13
Figure 12: Reviewing Status of connection on Indegy .................................................................................................... 14
Figure 13: Example of API logs between Indegy and ClearPass ...................................................................................... 14
Introduction

This Integration Guide covers the configuration and use of the integration between Indegy and ClearPass Policy Manager (CPPM). Indegy protects Industrial Control Systems (ICS) networks by providing full visibility, security and control of OT networks. This initial integration between Indegy and ClearPass Policy Manager focuses on the ability of Indegy to detect, discover and classify OT/ICS endpoints and share this classification directly with ClearPass via the ClearPass Security Exchange framework and the open APIs we expose. Indegy will automatically update the ClearPass Policy Manager endpoint database with endpoint classification data and a variety of custom security attributes.

This guide is written based on Phase1 of our planned integration with Indegy, which provides 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 this integration framework.

Software Requirements

At the time of writing, ClearPass Policy Manager 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 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 version of Indegy that was used for writing this integration guide is 2.7 SP3.

Installation and Deployment Guide

The generic ClearPass Policy Manager 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 Indegy

The ClearPass Policy Manager syncs the asset list from Indegy into its endpoint database. The device context can be used for Dynamic Segmentation leveraging policies.

Discovered devices are pushed into ClearPass Policy Manager endpoint database leveraging the endpoints REST APIs. Periodic sync occurs to push data into CPPM.
Configuration

ClearPass Configuration

Prior to creating and enabling the integration in Indegy a number of configuration elements need to be pre-created in ClearPass Policy Manager. Follow the below configuration steps carefully, collecting data as highlighted which will be needed in the following section when configuring Indegy to establish an integration with CPPM.

Create a ClearPass User

As part of the communications channel between the two products, Indegy will use a number of APIs. Access to the TIPS API is validated via Username/Password combination credentials. This user needs to have minimum levels of access, do not use a Super Administrator profile.

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

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

Figure 2: Create an API level account in ClearPass

Create an Operator Profile

To securely access the REST APIs for the API Client, create a restricted access Operator Profile. Navigate to ClearPass Guest > Administration > Operator Logins > Profiles.

Click on “Create a new operator profile” on the top right corner of the page and define an operator profile as shown below.

Pick and choose the necessary access for Indegy to update CPPM endpoint database with the device context. In summary all options are set as ‘No Access’ except for the following.

For API Services, select custom and then grant the following access

- Allow API Access = Allow Access
For Policy Manager, select custom and then grant the following access:

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

**Figure 3: Operator Profile - Access restrictions 1**

**Figure 4: Operator Profile - Access restrictions 2**
Create an API Client

Indegy uses the REST APIs for this integration, REST APIs are authenticated under an OAuth2 framework. Create an API Client under **Guest > Administration > API Services > API Clients** > {Create API Client}

**Ensure the Operator Profile previously created is used here 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 Operator Profile created previously
- **Grant Type** = Client credentials (grant_type=client_credentials)

**Record the Client Secret and the ACTUAL API Client ID i.e. Indegy as below**

**Figure 5: Operator Profile - Access restrictions**

<table>
<thead>
<tr>
<th>External Servers - Syslog Targets</th>
<th>No Access</th>
<th>Read</th>
<th>Read, Write</th>
<th>Read, Write, Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators with this privilege can manage syslog targets</td>
<td>Read, Write, Delete</td>
<td>No Access</td>
<td>Read</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

**Figure 6: Create an API Client**

Use this form to create a new API client.

<table>
<thead>
<tr>
<th>Create API Client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client ID:</strong> Indegy</td>
</tr>
<tr>
<td><strong>Description:</strong> The unique string identifying this API client. Use this value in the OAuth2 &quot;client_id&quot; parameter.</td>
</tr>
<tr>
<td><strong>Enabled:</strong> Check to enable API client</td>
</tr>
<tr>
<td><strong>Operating Mode:</strong> ClearPass REST API - Client will be used for API calls to ClearPass</td>
</tr>
<tr>
<td><strong>Operator Profile:</strong> The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.</td>
</tr>
<tr>
<td><strong>Grant Type:</strong> Client credentials (grant_type=client_credentials)</td>
</tr>
<tr>
<td><strong>Client Secret:</strong> N0dp10fuRK2m5Q062eILir+hGGJgh00zhPCWqJ0Cs8Y</td>
</tr>
<tr>
<td><strong>Access Token Lifetime:</strong> 8 hours</td>
</tr>
</tbody>
</table>

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

- CPPM API Administrator User ID
- CPPM API Administrator User Password
- CPPM OAuth2 API Client NAME
- CPPM OAuth2 API Client Secret

**Indegy Configuration**

For this initial integration between the two products, there is limited configuration necessary on Indegy. After the configuration is complete the Indegy platform will continue to update the ClearPass Policy Manager endpoint database as it discovers new endpoints at a periodic schedule. Follow the steps below to configure and enable this integration.

Login as an administrator into Indegy UI. From the Indegy main console, navigate to **Administraotor dropdown (top right corner) > Settings > Integrations > Aruba**.

After clicking on ‘Aruba’ the following screen is shown, all fields are required for the configuration. Use the values collected during ClearPass Policy Manager configuration. Once configured, click on **Save**.

*Figure 7: Indegy Configuration Console*

Once saved, the UI would show the **Status** as **Connected**.
Below table explains the fields used for configuration in detail.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP</td>
<td>This should be the ClearPass Publisher’s IP address or FQDN</td>
</tr>
<tr>
<td>User Name</td>
<td>API Administrator User ID created in the previous section</td>
</tr>
<tr>
<td>Password</td>
<td>API Administrator Password created in the previous section</td>
</tr>
<tr>
<td>Client ID</td>
<td>OAuth2 client ID created in the previous section</td>
</tr>
<tr>
<td>API Client Secret</td>
<td>OAuth2 Client Secret copied in the previous section</td>
</tr>
</tbody>
</table>
**Integration Results**

As part of enabling the above integration, Indegy will create a number of custom Endpoint Dictionary attributes using the ClearPass REST APIs. This is a record of the Dictionary Attributes created by Indegy.

Check under **Administration > Dictionaries > Dictionary Attributes**.

**Figure 8: Endpoint Dictionary Attributes created by Indegy**

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Entity</th>
<th>Data Type</th>
<th>Is Mandatory</th>
<th>Allow Multiple</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Indegy_PrimName</td>
<td>Endpoint</td>
<td>String</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2.</td>
<td>Indegy_XKey</td>
<td>endpoint</td>
<td>String</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3.</td>
<td>Indegy_Serial</td>
<td>endpoint</td>
<td>String</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The Endpoint data is sent by Indegy, it creates the endpoints, sets the endpoint classification and also configures some custom endpoint attributes. An example of the endpoints created are shown below.

**Figure 9: Example of Endpoints created by Indegy**

Looking closer at the endpoint data we can see several important things, the mac-address, mac-vendor, and some device classification as determined by Indegy, other valuable data such as the date the endpoint was added and profiled, said another way the time Indegy updated ClearPass with the devices data.
Figure 10: Normalized Endpoint data created by Indegy

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

In addition to the standard data, Indegy also supplies other custom attributes. Click on the Attributes tab to see them. Any of these attributes could be used in a Policy.

Figure 11: Custom Endpoint data created by Indegy

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

**Indegy_Role** and **Indegy_Firmware** are useful attributes that can be used within the enforcement policy. For example, a known vulnerable Firmware for a device category can be blocked. Indegy_Role can be leveraged for downloading an appropriate user role for the endpoint to be connected.
Monitoring/Reviewing ClearPass and Indegy communications

Once the sync has started endpoint data will be populated directedly into the Policy Manager endpoint database, view the Status of the connection, see below for an example.

**Figure 12: Reviewing Status of connection on Indegy**

If the sync is not working or shows an error then it’s likely you’ve missed capturing the information correctly, recheck the data recorded, additionally you can view the API calls between Indegy and ClearPass from ClearPass Guest > Administration > Support > Application Log. Below is an example of logs from Indegy to ClearPass. Filter using the IP address of Indegy.

**Figure 13: Example of API logs between Indegy and ClearPass**

Notice there may be a few error logs. These errors indicate that the mac address did not exist hence a new one was created by Indegy. If the mac address exists, it will be updated if necessary and the errors will not be seen.