IntroSpect
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-01</td>
<td>Aug 2018</td>
<td>Arpit Bhatt</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

Copyright

©Copyright 2018 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** .......................................................................................................................... 6
- **Installation and Deployment Guide** ......................................................................................................... 6
- **Preparing ClearPass for Integration** ........................................................................................................ 7
  - ClearPass Post-Auth v2 and Insight .............................................................................................................. 7
- **Configuration steps for posting context from ClearPass to IntroSpect** ............................................... 9
  - ClearPass as a Log Source .......................................................................................................................... 9
  - User Account on IntroSpect ....................................................................................................................... 11
  - Endpoint Context Server ........................................................................................................................... 12
  - Context Server Actions ............................................................................................................................ 13
  - Enforcement Profiles ............................................................................................................................... 17
  - Sample Service Configurations ................................................................................................................ 18
- **Configuration steps for invoking action from IntroSpect** ....................................................................... 20
  - IntroSpect Operator Profile ...................................................................................................................... 20
  - API Client on ClearPass ............................................................................................................................ 22
  - Add ClearPass Server ................................................................................................................................ 23
- **Testing/Demo** .......................................................................................................................................... 24
- **Appendix A – Troubleshooting and Support** .............................................................................................. 33
  - Accessing Post-Auth v2 logs within ClearPass ‘Collect Logs’ ................................................................... 33
- **Appendix B – AMON Integration** ............................................................................................................ 36
- **Appendix C – Integrating with Packet Processor** ..................................................................................... 38
- **Appendix D – XMLs** .................................................................................................................................. 39
Figures

Figure 1: Pictorial view of ClearPass integration with Aruba IntroSpect .......................................................... 5
Figure 2: Enable Post-Auth v2 .................................................................................................................................. 7
Figure 3: Restart Async Network services ........................................................................................................ 8
Figure 4: Enable Insight .......................................................................................................................................... 8
Figure 5: ClearPass as a Log Source – part I ......................................................................................................... 9
Figure 6: ClearPass as a Log Source – part II ..................................................................................................... 10
Figure 7: ClearPass as a Log Source – part III .................................................................................................. 10
Figure 8: Create a User on IntroSpect ................................................................................................................ 11
Figure 9: Add an Endpoint Context Server ........................................................................................................ 12
Figure 10: Add a Context Server Action ........................................................................................................... 13
Figure 11: Add Content to the Content Server .................................................................................................. 13
Figure 12: Enforcement Profile for Generic User Authentication ...................................................................... 17
Figure 13: Summary of ClearPass Service used for Authentication ................................................................. 18
Figure 14: Enforcement Policy used in the Service ........................................................................................... 18
Figure 15: Time Source in Enforcement Policy .................................................................................................. 19
Figure 16: Time Source in Role Mapping ........................................................................................................... 19
Figure 17: Operator Profile – Part I .................................................................................................................... 20
Figure 18: Operator Profile – Part II ................................................................................................................... 21
Figure 19: Create an API Client on ClearPass .................................................................................................... 22
Figure 20: Add ClearPass server in IntroSpect .................................................................................................. 23
Figure 21: Access Tracker 1 ............................................................................................................................... 24
Figure 22: Access Tracker 2 ............................................................................................................................... 25
Figure 23: NAC Timeline ..................................................................................................................................... 26
Figure 24: Quarantine an endpoint from IntroSpect .......................................................................................... 26
Figure 25: Select the device to be Quarantined ................................................................................................. 27
Figure 26: Endpoint IntroSpectPosture token ................................................................................................. 27
Figure 27: Quarantine Role on Access Tracker ............................................................................................... 28
Figure 28: Access Tracker 1 ............................................................................................................................... 29
Figure 29: Access Tracker 2 ............................................................................................................................... 30
Figure 30: Access Tracker 3 ............................................................................................................................... 30
Figure 31: Endpoint details on ClearPass .......................................................................................................... 31
Figure 32: Entity360 Summary ............................................................................................................................ 31
Figure 33: Entity360 NAC Timeline ................................................................................................................... 32
Figure 34: Async network services in DEBUG .................................................................................................. 33
Figure 35: Policy Manager Logs ....................................................................................................................... 33
Figure 36: Log Source on Packet Processor ..................................................................................................... 38
Figure 37: Log Source Stats on Analyzer .......................................................................................................... 38
Figure 38: Import Enforcement Profiles ............................................................................................................ 39
**Introduction**

Aruba IntroSpect is a User and Entity Behavior Analytics (UEBA) platform that uses AI-based machine learning to detect changes in user behavior that often indicate inside attacks that have evaded perimeter defenses. It arms the security teams with insights into malicious, compromised or negligent users, systems and devices.

As a UEBA platform, it builds analytics with user identity. IntroSpect primarily requires Network data and identity information. IntroSpect would capture network traffic data leveraging raw SPAN ports, AMON, Netflow etc whereas the identity information is captured using LDAP and Active Directory logs. To build the user profile and associate a risk score with every user on the network, it is very important to capture the user identity and correlate it with the traffic captured.

**Figure 1: Pictorial view of ClearPass integration with Aruba IntroSpect**

Integration of ClearPass with IntroSpect is two-fold as shown in the picture above.

1. **ClearPass shares the user and device context with IntroSpect.**

   ClearPass can authenticate users and devices on the network. While doing so, it can also profile the devices connecting to the network. It becomes a context aggregator for users and devices connecting onto the network. It can share this rich context with IntroSpect. ClearPass can act as a very useful log source for IntroSpect in scenarios where user authentication is not against an Active Directory (AD). For instance, there are no AD events triggered during guest-user access. Therefore, the only way IntroSpect can gather the user context in such scenarios is via ClearPass. Similarly, for IoT-based scenarios, device context gathered by profiling is shared by ClearPass with IntroSpect which helps enhance IoT-based analytics within IntroSpect.

2. **IntroSpect can flag an endpoint as Quarantine, triggering ClearPass to take an action on the endpoint.**

   In an event, when the risk score reaches a value which is unacceptable on a network, a security analyst can trigger an action from the IntroSpect UI which optionally flags the endpoint as Quarantine within ClearPass and issues a terminate session for the endpoint using the REST APIs. ClearPass would then take appropriate action upon re-authentication changing the role for the endpoint so that it gets restricted or limited access on the network.
This guide covers the setup, configuration, and troubleshooting of ClearPass and IntroSpect to ensure the integration works as explained. It covers multiple user/device authentication scenarios

1. Active Directory user authentication
2. Local user authentication
3. Guest user authentication
4. Guest user authentication with MAC caching
5. MAC authentication for IoT devices

**Software Requirements**

- The minimum software version required for ClearPass is 6.7.3.
  - At the time of writing, version 6.7.5 is available and is the recommended release
- The versions of IntroSpect used for this integration is 2.3.0.X.
  - At the time of writing, version 2.3.0.3 is available and is the recommended release

The integration is available across the Standard as well as the Advanced edition of IntroSpect.

It is highly recommended to use ClearPass version 6.7.3 or above and the IntroSpect version 2.3.X for this integration. For other versions, please contact Aruba support.

**Installation and Deployment Guide**

This document is intended to help field engineering, customers, and channel partners integrate ClearPass Policy Manager with Aruba IntroSpect. Configuration of ClearPass Policy Manager and Profiler is beyond the scope of this document.

The generic **ClearPass Installation and Deployment** guide is located [here](#).

The **Profiling Configuration** guide can be accessed [here](#).

For assistance with IntroSpect installation and deployment, please contact your local Systems Engineer (SE) or Aruba support.
Preparing ClearPass for Integration

ClearPass Post-Auth v2 and Insight

The data that ClearPass collates and writes to the Insight database is extracted and written to the IntroSpect endpoint by the post_authentication daemon. Several seconds can elapse between when the client has authenticated and obtains its IP address and when the NAS sends RADIUS Accounting packets to ClearPass (it needs this for the client IP address). Assuming that Profiling is enabled, ClearPass then will profile the endpoint. Following these steps ClearPass has the attributes it needs to update IntroSpect endpoint. Once the data is gathered there is a process which POSTs this data to IntroSpect.

Starting 6.7.3, ClearPass has enhanced the Post-authentication daemon for higher scalability. This is available for the customers once they enable it. In current versions, this is disabled by default.

This can be enabled from “Cluster-Wide Parameters” under Administration > Server Manager > Server Configuration.

![Cluster-Wide Parameters](image)

It is strongly recommended to enable Post-Auth v2 for this Integration.

Figure 2: Enable Post-Auth v2
The **Async Network services** have to be restarted after enabling Post-Auth v2. This can be done under **Administration > Server Manager > Server Configuration**. Click on the server and navigate to **Services Control** tab as shown below.

**Figure 3: Restart Async Network services**

The Insight database is disabled by default on ClearPass. This must be enabled on at least one node in the cluster for the IntroSpect integration to function.

For Post-Auth session enforcement, Insight must be enabled. This is done under **Administration > Server Manager > Server Configuration**. Click on the server and **Enable Insight** as shown below.

**Figure 4: Enable Insight**

**Why INSIGHT must be enabled** - It is used to collate the records that feed the API used to send information to IntroSpect. The RADIUS Authentication triggers a NetEvent, from which data is written into the Insight DB. When Insight receives the RADIUS Accounting data (again from a NetEvent) it’s matched with the endpoint MAC address to update the source IP address in Insight.

**Why PROFILING must be enabled** - Additionally, it’s extremely important that you enable Profiling. Profiling allows ClearPass to identify the device-types, device-categories, etc. of the authenticating devices on the network. Profiling uses several techniques to identify the device, be that a SPAN port, DHCP-fingerprinting, TCP-fingerprinting, HTTP User-Agent, NMAP passive scanning, Netflow/IPFIX, etc.

In addition to enabling the profiling on ClearPass, it’s important to know that other configuration is required on the network to make the ClearPass Profiling/Fingerprinting work.
Configuration steps for posting context from ClearPass to IntroSpect

As explained in the Introduction section there are 2 phases to this integration. This section talks about the necessary configuration steps to ensure ClearPass can POST valid context data to IntroSpect successfully.

A lot of these steps can be easily achieved on ClearPass by leveraging the XML files available on Aruba GitHub. We will specify the steps that can be skipped upon successful import of XML files. Kindly refer Appendix D for details.

ClearPass as a Log Source

For IntroSpect, the first step is to add ClearPass as a log source so that it can successfully receive and parse data from ClearPass. From the IntroSpect Analyzer, navigate to Menu > Configuration > Log Sources. Click on “Add Log Source”.

Select the entries as shown below for the Vendor, Category and Format. Click on “New Source”.

Figure 5: ClearPass as a Log Source – part I
Enter a "Label" for this Log Source and do not change the default values. In this example, I have used the label as **Events** as highlighted below. Click "Ok" and "Add Log Source" to save.

**Figure 6: ClearPass as a Log Source – part II**

The Network Access Control logs will be used in correlating the username, mac address, location and other attributes to the network conversations. It can also be used to send the posture data associated with the endpoint. After adding a log source on IntroSpect, the UI will display the events received and parsed by this log source. Any errors or dropped events will be highlighted. IntroSpect does not start using this data immediately and the log source by default is added in profiling mode where the data is parsed but not used.

Once the ClearPass server is setup and posts data to IntroSpect, the counter shown below for **THROUGHPUT** goes up. Once the counters increment and you see a SUCCESS rate of 100%, ensure you change the mode to **PRODUCTION** by toggling the highlighted button below. If not, IntroSpect will continue to keep this log source in profiling mode and discard all the data.

**Figure 7: ClearPass as a Log Source – part III**

User Account on IntroSpect

The next step is to create a user account on IntroSpect which will be used by ClearPass to successfully authenticate before posting the JSON attributes. The role

Navigate to Menu > Configuration > User Accounts. Click on “Add User”. Assign the Role as superuser. The E-mail field highlighted below will be used as the “Username” field in ClearPass while adding the Endpoint Context Server for authentication. Note the account details as this will be used during ClearPass configuration.

Figure 8: Create a User on IntroSpect

Please note that the E-mail field of the IntroSpect user will be used as the username in the Endpoint Context Server configured on ClearPass.
Endpoint Context Server

This step can be skipped, if the XML file posted on Aruba GitHub is successfully imported into the ClearPass. Refer Appendix D for more details.

ClearPass server needs to post the user/device context to IntroSpect. Currently, an administrator needs to add a Generic HTTP Endpoint Context Server to post this information to IntroSpect.

This can be configured under Administration > External Servers > Endpoint Context Servers. Click on “Add” and select the Server Type as “Generic HTTP”. Enter the IP/FQDN of the Analyzer instance as shown below.

Notice the Username being used. It should match with the “E-mail” field of the user account created on IntroSpect.

Figure 9: Add an Endpoint Context Server

Please note that Server Base URL will need port 8443 to be added manually if a Hardware instance of the IntroSpect Analyzer is being used. For AWS instance, the URL will be the same as “https://Server Name” and the port number is not required for a successful post.
**Context Server Actions**

This step can be skipped, if the XML file posted on Aruba GitHub is successfully imported into the ClearPass. Refer Appendix D for more details.

The JSON attributes to be posted from ClearPass to IntroSpect are defined using the Context Server Actions. These Context Server Actions are then tied to the Enforcement Profiles, which in-turn are a part of the Services configured on ClearPass.

These attributes vary based on the type of authentication hence we have a different Context Server Action for Guest and MAC caching based authentications.

There are 3 mandatory attributes which if absent will result in attributes not getting posted on IntroSpect.

1. **User_name**: User details of the device posted from ClearPass.
2. **Src_ip**: This is the IP address of the endpoint. Enable Radius Accounting on the Network Access Device (NAD) for this value to get populated.
3. **Timestamp**: For this to work, add Time Source as an Authorization source in the Service Configuration which will be covered later in the Service Configuration.

The context server actions can be added under Administration > Dictionaries > Context Server Actions. Click on “Add”, select the Endpoint Context Server defined in the previous step as the Server Name. This is the IntroSpect analyzer to which we are posting the contents.

**Figure 10: Add a Context Server Action**
The next step is to add the **Content**. This varies based on the type of authentication and the Login/Logout action. The contents for respective actions are mentioned below. You can copy and paste them as is in the **Content** section as shown below.

**Figure 11: Add Content to the Content Server**

The following 6 context servers can be easily imported into your ClearPass server instead of manually configuring them. Please refer **Appendix-D** for details.

1. **IntroSpect Login Action**

   This is a generic Login post which will be used for users authenticating against Active Directory, Local Repository and for devices authenticating with MAC Authentication like IoT devices. It should be used for most of the scenarios except Guest and Mac-Caching based user authentications.

   Following is the Content-Type posted from ClearPass to IntroSpect.

   **Content-Type: JSON**

   ```json
   {"user_name": "%{Authentication:Username}", "source": "%{Connection:Dest-IP-Address}"},
   "host_name": "%{Authorization:[Endpoints Repository]:Hostname}", "device_family": "%{Authorization:Endpoints Repository]:OS Family}"}, "event_type": "login", "user_type": "normal",
2. IntroSpect Logout Action

This is a generic Login post which will be used for users authenticating against Active Directory, Local Repository and for devices authenticating with MAC Authentication like IoT devices. It should be used for most of the scenarios except Guest and Mac-Caching based user authentications.

Following is the Content-Type posted from ClearPass to IntroSpect.

**Content-Type: JSON**

```json
{
    "user_name": "%{Authentication:Username}",
    "source": "%{Connection:Dest-IP-Address}",
    "timestamp": "%{Authorization:[Time Source]:Now}",
    "event_type": "logout"
}
```

3. IntroSpect Guest Login Activity

This is a Login Action used for Guest users. It also posts other details associated with the Guest user like visitor_company, visitor_phone, visitor_email, sponsor_email, sponsor_name etc.

Following is the Content-Type posted from ClearPass to IntroSpect.

**Content-Type: JSON**

```json
{
    "user_name": "%{Authentication:Username}",
    "source": "%{Connection:Dest-IP-Address}",
    "timestamp": "%{Authorization:[Time Source]:Now}",
    "event_type": "login"
}
```

4. IntroSpect Guest Logout Activity

This is a Logout Action used for Guest users. It also posts other details associated with the Guest user like visitor_company, visitor_phone, visitor_email, sponsor_email, sponsor_name etc.

Following is the Content-Type posted from ClearPass to IntroSpect.

**Content-Type: JSON**

```json
{
    "user_name": "%{Authentication:Username}",
    "source": "%{Connection:Dest-IP-Address}",
    "timestamp": "%{Authorization:[Time Source]:Now}",
    "event_type": "logout"
}
```
5. IntroSpect Guest MAC Caching Login Activity

This is a Login Action used for cached Guest users. These users will login with MAC authentication for the cached duration. The value of %\{Authentication:Username\} for such cases is the MAC address. To use the correct value of user_name for the post we must use "%\{name\}". This is the only change from the previous IntroSpect-Guest Login Activity.

Following is the Content-Type posted from ClearPass to IntroSpect.

**Content-Type: JSON**

```
{"user_name": "%\{name\}\", "source": "%\{Connection:Dest-IP-Address\}\", "host_name": "%\{Authorization:[Endpoints Repository]:Hostname\}\", "device_family": "%\{Authorization:[Endpoints Repository]:OS Family\}\", "event_type": "login", "user_type": "guest", "timestamp": "%\{Authorization:[Time Source]:Now\}\", "device_category": "%\{Authorization:[Endpoints Repository]:Category\}\", "device_name": "%\{Authorization:[Endpoints Repository]:Device Name\}\", "src_ip": "%\{ip\}\", "device_posture": "%\{Authentication:Posture\}\", "entity_posture": "%\{Endpoint:IntrospectPosture\}\", "src_mac": "%\{Connection:Client-Mac-Address-NoDelim\}\", "role": "%\{Tips:Role\}\", "location": "%\{Radius:Aruba:Aruba-Location-Id\}\", "event_id": "3", "ssid": "%\{Connection:SSID\}\", "sponsor_name": "%\{Endpoint:Sponsor Name\}\", "sponsor_email": "%\{Endpoint:Sponsor Email\}\", "visitor_fullname": "%\{Endpoint:Visitor Full Name\}\", "visitor_phone": "%\{Endpoint:Visitor Phone\}\", "visitor_email": "%\{GuestUser:Email\}\", "visitor_company": "%\{GuestUser:Company Name\}\"}
```

6. IntroSpect Guest MAC Caching Logout Activity

This is a Logout Action used for cached Guest users. Following is the Content-Type posted from ClearPass to IntroSpect.

**Content-Type: JSON**

```
{"user_name": "%\{name\}\", "source": "%\{Connection:Dest-IP-Address\}\", "host_name": "%\{Authorization:[Endpoints Repository]:Hostname\}\", "device_family": "%\{Authorization:[Endpoints Repository]:OS Family\}\", "event_type": "logout", "user_type": "guest", "timestamp": "%\{Authorization:[Time Source]:Now\}\", "device_category": "%\{Authorization:[Endpoints Repository]:Category\}\", "device_name": "%\{Authorization:[Endpoints Repository]:Device Name\}\", "src_ip":
```
"%{ip}", "device_posture": "%{Authentication:Posture}", "entity_posture": "%{Endpoint:Intro-\nspectPosture}", "src_mac": "%{Connection:Client-Mac-Address-NoDelim}", "role": "%{Tips:Role}", "location": "%{Radius:Aruba:Aruba-Location-Id}", "event_id": "4", "ssid": "%{Connection:SSID}", "sponsor_name": "%{Endpoint:Sponsor Name}", "sponsor_email": "%{End-\npoint:Sponsor Email}", "visitor_fullname": "%{Endpoint:Visitor Full Name}", "visitor_phone": "%{Endpoint:Visitor Phone}", "visitor_email": "%{Endpoint:Visitor Email}", "visi-\ntor_company": "%{Endpoint:Visitor Company}"}

**Enforcement Profiles**

This step can be skipped, if the XML file posted on Aruba GitHub is successfully imported into the ClearPass. Refer Appendix D for more details.

The Enforcement Profiles are the actions or attributes sent by ClearPass. The Context Server Actions are tied to the Enforcement Profiles. Following is the example of the Generic Enforcement Profile with IntroSpect Login and Logout Action.

Notice the **Login Action** and **Logout Action** used. These are the **Context Server Actions** configured for generic user authentication in previous step.

*Figure 12: Enforcement Profile for Generic User Authentication*

Similarly, you can create enforcement profiles for guest user authentication and MAC caching based users authenticating on the network using their respective context server actions.

These enforcement profiles are tied down to a condition within the enforcement policies which is further used in a service.
Sample Service Configurations

The service configuration varies based on customer policies. Following is a summary of a sample service configuration for a generic 802.1X Authentication. This has to be modified based on the requirements.

**Figure 13: Summary of ClearPass Service used for Authentication**

The Enforcement Policy used in this Service leverages the Enforcement Profile “IntroSpect-Login-Logout-Profile” configured in the Previous step as shown below.

This Enforcement Profile is used for both the Quarantine and a Healthy endpoint connecting on the network as can be seen in the Policy below.

**Figure 14: Enforcement Policy used in the Service**

TimeStamp is a mandatory attribute for the post to be successful. Either of the workarounds in Figure 15 or 16 should be configured to get the value of Timestamp populated for the POST to IntroSpect.
For ClearPass to get this attribute it is important to add “Authorization:[Time Source]:Now EXISTS” as one of the conditions under Role Mapping or Enforcement Policy as shown below

**Figure 15: Time Source in Enforcement Policy**

![Image of Enforcement Policy](image1)

**Figure 16: Time Source in Role Mapping**

![Image of Role Mapping](image2)

The Timestamp value to be posted in the JSON will be empty and will result in an unsuccessful post if the above step is missed. You will not see the value of “Authorization:[Time Source]:Now” under the Authorization attributes in the Access Tracker as well.
Configuration steps for invoking action from IntroSpect

IntroSpect Operator Profile

An operator profile determines what actions an operator is permitted using ClearPass. An account attempting to authenticate gets an operator profile assigned. For security conscious customers, it is imperative to use a restricted operator profile having sufficient rights for the integration.

You can configure the Operator Profile as shown below. Navigate to **ClearPass Guest** and go to **Administration > Operator Logins > Profiles**. Create a new operator profile.

**DO NOT USE A SUPER ADMINISTRATOR** Operator Profile available by default.

You need to grant privileges for the following 3 services which are captured below

1. **API Services**: Select **Custom** and Allow **API Access**

2. **Guest Manager**: Select **Custom** and grant “**Full**” access to **Active Session**. Also, grant “**Read Only**” access for “**Active Sessions History**”

3. **Policy Manager**: Select **Custom** and grant “**Read, Write**” access to **Identity – Endpoints**

**Figure 17: Operator Profile – Part I**
Figure 18: Operator Profile – Part II

| Privileges | Policy Manager | Custom:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication - Methods</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Certificate - Trust List</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Certificates</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Dictionaries - Attributes</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Dictionaries - Context Server Actions</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Dictionaries - Fingerprint</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Events - Login Audit</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Events - System Events</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>External Servers - Endpoint Context Servers</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>External Servers - File Backup Servers</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>External Servers - Syslog Targets</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>External Servers - Syslog Expert Filters</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Identity - Biometrics</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
<tr>
<td>Identity - Local Users</td>
<td>No Access</td>
<td>Read, Write, Delete</td>
</tr>
</tbody>
</table>
API Client on ClearPass

An API client needs to be created on ClearPass for IntroSpect to authenticate and leverage ClearPass APIs. IntroSpect needs access to ClearPass APIs for updating the endpoint with the “IntroSpectPosture” attribute and to issue a Terminate session.

An API client can be created from ClearPass Guest under Administration > API Services > API Clients.

Create API client. Specify the **Client ID**. Use the **Operator Profile** created in the previous step. Copy the **Client Secret** and **Client ID** in a text file as it will be required for the next step. This Client Secret will not be displayed again.

**Figure 19: Create an API Client on ClearPass**

Note that currently we can only use the Grant Type as Client Credentials for this Integration. Copy the Client Secret as it will not be displayed again although it can be re-generated.
Add ClearPass Server

This is the final step for setting up the communication between the two systems. Navigate to Menu > Configuration > System > ClearPass Servers on IntroSpect. Specify the server hostname or IP address.

The Client ID and Client Secret are created on the ClearPass server in the section. These are required to access ClearPass REST APIs for adding IntroSpectPosture attribute to the endpoint. It also helps

Figure 20: Add ClearPass server in IntroSpect
Testing/Demo

In this section, we will walk through the two-way integration as described in the Introduction. The context information is posted from ClearPass to IntroSpect. We will also go through a demonstration of quarantining a user from the IntroSpect UI.

1. A regular user, part of Active Directory connects to the network using his device and gets authenticated against ClearPass Policy Manager. The authentication shows up in the Access Tracker as shown below.

   Points to Note:
   
   • The accounting information should be received for the post to be successful. Look for the accounting tab.
   
   • Look for the value of “Authorization:[Time Source]:Now” under Accounting attributes. It should be an epoch time value.
   
   • The attributes are posted using the Enforcement Profile “IntroSpect-Login-Logout-Profile”.

   Figure 21: Access Tracker 1
2. The attributes once posted successfully to IntroSpect gets written into the cache. IntroSpect will then look for either the user information or the IP information so that the data posted can be used for co-relation.

Note if IntroSpect does not have information about the user or IP that was posted by ClearPass from another log source like LDAP (for user info) or AMON/SPAN (for network traffic) it will not be able to use ClearPass data for user co-relation and will eventually discard it.

3. After waiting for an hour approximately, you will see the device context, location etc posted by ClearPass on the IntroSpect UI. This will be seen under the NAC Timeline which can be accessed from the Entity360 Page. The NAC Timeline shows the time when the entity/user is active on the device along with the device attributes posted from ClearPass.

The user details like Full Name, Title, Email, Department etc that you see below are fetched from the LDAP added as a source on IntroSpect.
A similar disconnect entry would be seen on the NAC Timeline for the entity as well upon receiving Accounting Stop.

4. Let us see the behavior as we Quarantine this endpoint from IntroSpect. From the Entity360 Page, we can trigger a Quarantine action for an endpoint as shown below.

**Figure 23: NAC Timeline**

![NAC Timeline Image]

**Figure 24: Quarantine an endpoint from IntroSpect**

![Quarantine Endpoint Image]
5. The next step is to select the MAC address of the device you want to Quarantine. You will see multiple MAC addresses associated with a user here.

You can select multiple MAC addresses or devices and Quarantine all of them. The behavior will be similar for all the MAC addresses selected.

Figure 25: Select the device to be Quarantined

6. IntroSpect Analyzer leverages the ClearPass REST APIs for Endpoints and updates the IntroSpectPosture attribute in the Endpoint repository. It also triggers a Terminate Session so that a new role can be pushed based on the IntroSpectPosture attribute.

Figure 26: Endpoint IntroSpectPosture token
The Enforcement Policy has a condition which says if “Endpoint:IntroSpectPosture EQUALS quarantine”, sends the **quarantined** role to the NAD. You can define your policy and role on the NAD to restrict access, send a web-portal page notifying the action to the user, restrict bandwidth or completely deny access.

**Figure 27: Quarantine Role on Access Tracker**
Let's take a look at this in a Guest user scenario. Here IntroSpect has no user or device details from any other log source. This data is only provided by ClearPass. IntroSpect needs to have conversation data for this device for the correlation to happen, else the data posted is discarded by IntroSpect.

1. A guest user connects to an SSID, registers himself and gets approved before connecting on the guest network. The authentication request shows up on the Access Tracker. The details of the access tracker are shown below

Note the highlighted areas in the screenshots below. These are the values which will be posted to IntroSpect using the Enforcement Profile “IntroSpect-Guest-Login-Logout-Profile”. The Accounting data should be available from the Network Access Device (NAD). The Accounting tab will be displayed as we receive the Accounting Start from the NAD.

Figure 28: Access Tracker 1
Figure 29: Access Tracker 2

Note the value of \textit{“Authorization:[Time Source]:Now”}. The POST fails if the value is missing.

Figure 30: Access Tracker 3
The device context is collected by ClearPass Profiler. This information is available in the Endpoint Repository which can be accessed from **Identity > Endpoints**. Filter the endpoint using the mac address. The highlighted attributes are posted from ClearPass to IntroSpect.

**Figure 31:** Endpoint details on ClearPass

Let's see the information posted on IntroSpect. The information will be processed by IntroSpect Analyzer and will take an hour (approximately) before it shows up. The context associated with the user posted by ClearPass is shown below.

**Figure 32:** Entity360 Summary
The NAC Timeline shows the time when the entity/user is active on the device along with the device attributes posted from ClearPass.

**Figure 33:** *Entity360 NAC Timeline*

A similar disconnect entry would be seen on the NAC Timeline for the entity as well upon receiving Accounting Stop posted by the Logout Action.
Appendix A – Troubleshooting and Support

Accessing Post-Auth v2 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.

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.

Set the Log Level for Async network services in DEBUG. This can be done under Administration > Server Manager > Log Configuration as shown below.

**Figure 34: Async network services in DEBUG**

After the Logs have been collected and exported from the system, expand the GZ file and locate the postauth.log file under async-netd in the following location ‘PolicyManagerLogs->async-netd’ as shown below.

**Figure 35: Policy Manager Logs**
Following are the examples of log entries for successful posts in postauth.log

**Login Action for AD User**

```
  "user_name": "a_user1",
  "source": "10.X.X.X",
  "host_name": "blr-arpitbhatt-t430s",
  "device_family": "Windows",
  "event_type": "login",
  "user_type": "normal",
  "timestamp": "1533187321",
  "device_category": "Computer",
  "device_name": "Windows Vista/7/2008",
  "src_ip": "10.X.X.X",
  "entity_posture": "%(Endpoint:IntrospectPosture)",
  "device_posture": "UNKNOWN",
  "src_mac": "2477037a9d6c",
  "role": 
  
  "[Employee], [User Authenticated]",
  "location": "Helios-Demo-Room",
  "event_id": "1",
  "ssid": "Demo-Corporate"
}
```

```
```

**Logout Action for AD User**

```
  "user_name": "a_user1",
  "source": "10.X.X.X",
  "host_name": "blr-arpitbhatt-t430s",
  "device_family": "Windows",
  "event_type": "logout",
  "user_type": "normal",
  "timestamp": "1533184333",
  "device_category": "Computer",
  "device_name": "Windows Vista/7/2008",
  "src_ip": "10.X.X.X",
  "entity_posture": "%(Endpoint:IntrospectPosture)",
  "device_posture": "UNKNOWN",
  "src_mac": "2477037a9d6c",
  "role": 
  
  "[Employee], [User Authenticated]",
  "location": "Helios-Demo-Room",
  "event_id": "2",
  "ssid": "Demo-Corporate"
}
```

```
```

**Login Action for Guest User**

```
  "user_name": "arpit7@aruba.com",
  "source": "10.X.X.X",
  "host_name": "amus-ipad",
  "device_family": "Apple",
  "event_type": "login",
  "user_type": "guest",
  "timestamp": "1533122605",
  "device_category": "SmartDevice",
  "device_name": "Apple iPad",
  "src_ip": "10.X.X.X",
  "device_posture": "Unknown",
  "entity_posture": "%(Endpoint:IntrospectPosture)",
  "src_mac": "98fe94714162",
  "role": 
  
  "[Guest], [User Authenticated]",
  "location": "Helios-Demo-Room",
  "event_id": "3",
  "ssid": "Demo-Visitor",
  "sponsor_name": "arpit7@aruba.com",
  "sponsor_email": "arpit@a.com",
  "visitor_email": "arpit7@aruba.com",
  "visitor_fullname": "Arpit",
  "visitor_phone": "14085138853",
  "visitor_company": "Aruba Networks"
}
```

```
```

**Logout Action for Guest User**

```
  "user_name": "arpit7@aruba.com",
  "source": "10.X.X.X",
  "host_name": "amus-ipad",
  "device_family": "Apple",
  "event_type": "logout",
  "user_type": "guest",
  "timestamp": "1533122605",
  "device_category": "SmartDevice",
  "device_name": "Apple iPad",
  "src_ip": "10.X.X.X",
  "device_posture": "Unknown",
  "entity_posture": "%(Endpoint:IntrospectPosture)",
  "src_mac": "98fe94714162",
  "role": 
  
  "[Guest], [User Authenticated]",
  "location": "Helios-Demo-Room"
}
```

```
```
"[Guest], [User Authenticated]", "location": "Helios-Demo-Room", "event_id": "4", "ssid": "Demo-Visitor", "sponsor_name": "arpit7@aruba.com", "sponsor_email": "arpit@a.com", "visitor_fullname": "Arpit", "visitor_phone": "14085138853", "visitor_email": "arpit7@aruba.com", "visitor_company": "Aruba Networks"}


The above logs collected has useful set of information under Systems Logs. Navigate to /var/log/httpd. Check ssl_access_log.

The logs below denote successful Quarantine actions triggered from IntroSpect.

```
10.43.8.39 - - [23/Aug/2018:20:09:41 +0530] "POST /api/oauth HTTP/1.1" 200 113 "-" "python-requests/2.7.0 CPython/2.7.10 Linux/2.6.32-696.16.1.e16.x86_64" TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 296020µs

10.43.8.39 - - [23/Aug/2018:20:09:43 +0530] "PATCH /api/endpoint/mac-address/2477037a9d6c HTTP/1.1" 200 193 "-" "python-requests/2.7.0 CPython/2.7.10 Linux/2.6.32-696.16.1.e16.x86_64" TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 337671µs

10.43.8.39 - - [23/Aug/2018:20:09:44 +0530] "GET /api/session?filter=%7B%22mac_address%22%3A%2222477037a9d6c%22%7D HTTP/1.1" 200 25796 "-" "python-requests/2.7.0 CPython/2.7.10 Linux/2.6.32-696.16.1.e16.x86_64" TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 2506916µs

10.43.8.39 - - [23/Aug/2018:20:09:48 +0530] "POST /api/session/a_user12477037A9D6C-5B7EC6F9-1F29A/disconnect HTTP/1.1" 200 71 "-" "python-requests/2.7.0 CPython/2.7.10 Linux/2.6.32-696.16.1.e16.x86_64" TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 2732249µs
```

For further advanced troubleshooting, we can also enable debug for API Framework under ClearPass Guest. The Application logs would show detailed API Trace. Contact Aruba support for assistance.
Appendix B – AMON Integration

In case of an all Aruba Infrastructure, one can leverage Aruba AMON to get quick Network data. It is always recommended to use the SPAN port as it gives richer metadata for analytics, however, setting up AMON is quick and is useful in some scenarios.

Here are the necessary steps to set AMON on an Aruba-OS Controller running 8.x.

1. Create an IntroSpect mgmt-server Profile. Enable Sessions, Inline DNS stats and Inline DHCP stats.

(WLC-Demo-01) [mynode] #show mgmt-server profile "introspect"

Thu Aug 02 12:16:04.194 2018

Mgmt Config profile "introspect"

--------------------------------
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stats</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tag</td>
<td>Disabled</td>
</tr>
<tr>
<td>Sessions</td>
<td>Enabled</td>
</tr>
<tr>
<td>Monitored Info - Add/Update</td>
<td>Disabled</td>
</tr>
<tr>
<td>Monitored Info - Deletion</td>
<td>Disabled</td>
</tr>
<tr>
<td>Monitored Info - Periodic Snapshot</td>
<td>Disabled</td>
</tr>
<tr>
<td>Wireless IDS Event Info</td>
<td>Disabled</td>
</tr>
<tr>
<td>Misc</td>
<td>Disabled</td>
</tr>
<tr>
<td>Location</td>
<td>Disabled</td>
</tr>
<tr>
<td>UCC Monitoring</td>
<td>Disabled</td>
</tr>
<tr>
<td>AirGroup Info</td>
<td>Disabled</td>
</tr>
<tr>
<td>Inline DHCP stats</td>
<td>Enabled</td>
</tr>
<tr>
<td>Inline AP stats</td>
<td>Enabled</td>
</tr>
<tr>
<td>Inline Auth stats</td>
<td>Enabled</td>
</tr>
<tr>
<td>Inline DNS stats</td>
<td>Enabled</td>
</tr>
<tr>
<td>WAN State Info</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
2. Add the IntroSpect Analyzer as the mgmt.-server.

(WLC-Demo-01) [mynode] (config) #mgmt-server primary-server 10.X.X.X profile introspect

3. Enable Firewall visibility. If fw_visibility is disabled, the AMON data does not get exported.

(WLC-Demo-01) [mynode] (config) #firewall-visibility;

(WLC-Demo-01) [mynode] #show firewall-visibility status

Thu Aug 02 12:20:09.405 2018

enabled
Appendix C – Integrating with Packet Processor

The above setup steps were based on ClearPass posting data to IntroSpect Analyzer. Hence ClearPass was added as a Log source on the Analyzer.

ClearPass can also post the data to a Packet Processor as long as it can communicate with the Packet Processor over port 443. In such scenarios, the Log source needs to be added on the Packet Processor. The log source once added on the Packet Processor will be as shown below.

**Figure 36: Log Source on Packet Processor**

The stats are available on Analyzer itself as shown below.

**Figure 37: Log Source Stats on Analyzer**
Appendix D – XMLs

There are several configuration components required in ClearPass for the Integration to work successfully. We have uploaded the XML files on Aruba GitHub which can be accessed here.

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

Importing this XML would create all the required enforcement profiles, context server actions and also define the endpoint context server.

- Download the file “clearpass-integration_aruba-introspect_all-profiles.xml”.
- Open this file in your favorite editor.
- Use the Find and Replace feature of the editor to replace “<<introspect-fqdn-or-ip>>” with the actual IP address or FQDN of the IntroSpect Analyzer. There are 14 such entries in this file.
- Replace “<<introspect-integration-email>>” and “<<introspect-integration-password>>” with actual user details created in section “User Account on IntroSpect”
- Save the file and Import.

Remove “:8443” from the xml file above if using the AWS instance of the Analyzer.

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

**Figure 38: Import Enforcement Profiles**

The above action will import the following on ClearPass

1. Post Authentication Enforcement Profiles
   a. IntroSpect Login Logout Enforcement Profile
b. IntroSpect Guest Login Logout Enforcement Profile

c. IntroSpect Guest MAC Caching Login Logout Enforcement Profile

2. Context Server Actions

a. IntroSpect Login Activity

b. IntroSpect Logout Activity

c. IntroSpect Guest Login Activity

d. IntroSpect Guest Logout Activity

e. Introspect Guest MAC Caching Login Activity

f. Introspect Guest MAC Caching Logout Activity

3. Endpoint Context Server

The above Enforcement Profiles imported are tied to the Context Server Actions which are associated with the Endpoint Context Server added. Enforcement Profiles can then be used in services to post information to IntroSpect server. Refer to the section “Sample Service Configurations” for further steps.