Check Point

ClearPass
## 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>Mar 2015</td>
<td>Danny Jump</td>
<td>Initial Published Version</td>
</tr>
<tr>
<td>1.1</td>
<td>Apr 2015</td>
<td>Danny Jump</td>
<td>Calculating dynamically the user-role that is sent from TIPS role. Added DEBUG commands</td>
</tr>
<tr>
<td>1.2</td>
<td>Jul 2015</td>
<td>Danny Jump</td>
<td>Update to cater for R77.xx RESTful API HotFix</td>
</tr>
<tr>
<td>1.3</td>
<td>Sept 2015</td>
<td>Danny Jump</td>
<td>Capturing new context attributes added in 6.5.3</td>
</tr>
<tr>
<td>2.0</td>
<td>Nov 2018</td>
<td>Arpit Bhatt</td>
<td>Based on version R80.XX. Removed old content</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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Audience</td>
<td>6</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>7</td>
</tr>
<tr>
<td>Configuring Check Point and ClearPass for REST APIs</td>
<td>8</td>
</tr>
<tr>
<td>ClearPass Configuration</td>
<td>8</td>
</tr>
<tr>
<td>Endpoint Context Server</td>
<td>8</td>
</tr>
<tr>
<td>Context Server Actions Login/Logout</td>
<td>8</td>
</tr>
<tr>
<td>Enforcement Profile</td>
<td>14</td>
</tr>
<tr>
<td>Check Point Configuration – AD user</td>
<td>15</td>
</tr>
<tr>
<td>Enable Identity Awareness</td>
<td>15</td>
</tr>
<tr>
<td>Adding an AD/LDAP Server</td>
<td>16</td>
</tr>
<tr>
<td>Create a Web API Host</td>
<td>17</td>
</tr>
<tr>
<td>Configure Identity Awareness-Web API</td>
<td>18</td>
</tr>
<tr>
<td>Check Point Configuration – Guest user account</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Radius Accounting Proxy</td>
<td>24</td>
</tr>
<tr>
<td>Configuring RADIUS Accounting Proxy on ClearPass</td>
<td>24</td>
</tr>
<tr>
<td>Configuring RADIUS Accounting on Check Point</td>
<td>25</td>
</tr>
<tr>
<td>Enable Identity Awareness</td>
<td>25</td>
</tr>
<tr>
<td>Add an AD/LDAP Server</td>
<td>25</td>
</tr>
<tr>
<td>Add a Network Object</td>
<td>25</td>
</tr>
<tr>
<td>Configure Identity Awareness-RADIUS Accounting</td>
<td>26</td>
</tr>
<tr>
<td>Appendix A – Troubleshooting and Support</td>
<td>29</td>
</tr>
<tr>
<td>Monitoring/Debugging Identity Awareness from the Check Point CLI</td>
<td>29</td>
</tr>
<tr>
<td>ClearPass Logs</td>
<td>30</td>
</tr>
<tr>
<td>Appendix B – XML</td>
<td>32</td>
</tr>
</tbody>
</table>
Figures

Figure 1: ClearPass Attributes sent to Check Point ................................................................. 6
Figure 2: Add an Endpoint Context Server ............................................................................... 8
Figure 3: Copy of Context Server Action .................................................................................. 9
Figure 4: Context Server – Action Tab ...................................................................................... 9
Figure 5: Context Server – Action Tab ...................................................................................... 10
Figure 6: Context Server – Content Tab ................................................................................... 10
Figure 7: Context Server – Attributes Tab ................................................................................ 11
Figure 8: Context Server for Guest user – Action Tab ............................................................. 11
Figure 9: Context Server for Guest user – Content Tab ............................................................ 12
Figure 10: Context Server for Guest user – Attributes Tab ..................................................... 12
Figure 11: Context Server – Action Tab .................................................................................... 13
Figure 12: Context Server – Content Tab .................................................................................. 13
Figure 13: Endpoint Context Server – Actions Tab................................................................... 14
Figure 14: Enforcement Profile – AD user ................................................................................ 14
Figure 15: Enable Identity Awareness ....................................................................................... 15
Figure 16: Add Active Directory server I .................................................................................. 16
Figure 17: Add Active Directory server II ............................................................................... 16
Figure 18: Add a Host I ............................................................................................................. 17
Figure 19: Add a Host II ............................................................................................................ 17
Figure 20: Configure Identity Awareness-Web API ................................................................. 18
Figure 21: Identity Web API settings ......................................................................................... 19
Figure 22: AD user authenticated on Check Point ................................................................... 20
Figure 23: AD user authenticated on Check Point details ........................................................ 20
Figure 24: non-AD user denied by Check Point ....................................................................... 21
Figure 25: Adding an Access Role to match the Aruba guest role ........................................... 22
Figure 26: Guest user authenticated on Check Point ............................................................... 22
Figure 27: Guest user authenticated on Check Point details .................................................... 23
Figure 28: Firewall Policy to deny access to internal network ............................................... 23
Figure 29: Adding a RADIUS Accounting Proxy Target on ClearPass .................................... 24
Figure 30: Enabling Accounting Proxy in a ClearPass Service .............................................. 24
Figure 31: Adding Accounting Proxy Target to a ClearPass Service ........................................ 25
Figure 32: Add a Network Object ............................................................................................. 26
Figure 33: Configure Identity Awareness-RADIUS Accounting ............................................. 26
Figure 34: Configure RADIUS Accounting ............................................................................. 27
Figure 35: Authenticated User on Check Point – RADIUS Accounting ................................... 28
Figure 36: Collecting ClearPass Logs ....................................................................................... 31
Figure 37: postauthctrl.log ....................................................................................................... 31
Figure 38: Import Context Server Actions-R80 ....................................................................... 32
Introduction

This document is intended to help field engineering, customers, and channel partners integrate ClearPass Policy Manager with Check Point next-generation firewalls. There are two methods of integration between ClearPass Policy Manager and Check Point. One uses HTTP JSON encoded REST APIs the other uses RADIUS Accounting.

Similar to the integration that exists between ClearPass and other vendors, Check Point supports at a basic level the ability to pass username and source IP address attributes. But other attributes shown below can also be passed. As a summary, this is a list of the attributes that can be passed from ClearPass to Check Point that have been tested in our lab.

**Figure 1: ClearPass Attributes sent to Check Point**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>✓</td>
</tr>
<tr>
<td>Username</td>
<td>✓</td>
</tr>
<tr>
<td>User Role</td>
<td>✓</td>
</tr>
<tr>
<td>Domain</td>
<td>✓</td>
</tr>
<tr>
<td>Device Type</td>
<td>✓ [b]</td>
</tr>
<tr>
<td>Machine OS</td>
<td>✓ [b]</td>
</tr>
<tr>
<td>Machine Name</td>
<td>✓ [a]</td>
</tr>
<tr>
<td>Health/Posture</td>
<td>✓</td>
</tr>
</tbody>
</table>

[a] = Available from HTTP REST API calls not from RADIUS Accounting.  
[b] = Requires Check Point R80.XX or R77.XX with HOTFIX's

Where it is practical, best practices will be documented, although not every conceivable use case or deployment can or will be covered here in this document.

Audience

The reader is assumed to be familiar with the ClearPass family of products, including Policy Manager, Insight, Guest and Onboard. Basic knowledge of IP networks and wide-area networking is also assumed. A general understanding and previous experience in the deployment/configuration of Check Point is also assumed. We also make the assumption that the firewall is already deployed. We will not cover the firewall deployment or configuration beyond the steps to integrate ClearPass and a basic policy configuration.
Software Requirements

The minimum software version required for ClearPass is 6.6.X. The previous versions are no longer supported. At the time of writing, ClearPass 6.7.7 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 Check Point Firewall should run one of the following versions and should have the Identity Awareness blade.

- R80.XX
- For other versions, contact Check Point support to get a required Hotfix for Check Point Identity Awareness Gateway

This guide includes settings and screenshots from a ClearPass server running 6.7.7 and a Check Point Gateway running R80.10.
Configuring Check Point and ClearPass for REST APIs

Configuration is required on both the ClearPass and Check Point nodes. Check Point has produced a document “sk104958” which also covers this topic. The following sections talk about the ClearPass and Check Point configuration.

ClearPass Configuration

Endpoint Context Server

First add a generic HTTP Endpoint Context Server. Go to Administration > External Servers > Endpoint Context Servers [Add].

Figure 2: Add an Endpoint Context Server

Add the appropriate Server Name (IP Address), this will be translated into the Server Base URL. No Username/Password credentials are required to communicate with the Check Point firewall. Authentication is performed via the PSK configured in a later step.

Context Server Actions Login/Logout

Now that the Firewall endpoint have been defined, the next step is to set the Check Point context server actions ‘Login & Logout’ to use this endpoint.

It's very important to modify both the Login and Logout Server Actions. These are what update the Firewall of a user's session going active/inactive. ClearPass will then update the Check Point firewall which will permit/deny this user. The firewall should not be updated of a session starting and not clear it when the user leaves.

There is a timeout value on the firewall but ensuring that the Context Server Logout action is performed is cleaner and more secure.
Create a copy of the supplied/original **Check Point Login/Logout** context server actions templates and modify the copied items. The default templates within ClearPass are for R77.XX but not R80.XX which requires a URL change. Either create a copy of the original ones and modify them as shown below or import them easily using the XMLs available on Aruba GitHub. Refer **Appendix B** for details.

Create a copy of all the three Context Server Actions by selecting them one at a time and using the option to copy as shown below. A copy would be created by appending ‘Copy_of_’ to the Action Name.

**Figure 3: Copy of Context Server Action**

There are two Context server actions that need to be modified for a regular AD user scenario. These can be found under **Administration > Dictionaries > Context Server Actions**. The first Context Server Action that needs to be modified is the ‘**Copy_of_Check Point Login – AD User**’.

Within the ‘**Action**' tab the ‘Server Name’ needs to be changed to that of the HTTP server added in the previous section. The default will be localhost, select as appropriate from the drop down. Change the **Action Name** and **Description** to indicate that the action is relevant for R80 to avoid confusion.

The below URL path is set to `/IA_API/v1.0/add-identity`. The URL path changes across release versions in Check Point which needs to be taken into consideration.

**Figure 4: Context Server – Action Tab**
Following table summarizes the URL used across multiple versions.

<table>
<thead>
<tr>
<th>Version</th>
<th>Login Action URL</th>
<th>Logout Action URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>R77</td>
<td>/_IA_MU_Agent/idasdk/add-identity</td>
<td>/_IA_MU_Agent/idasdk/delete-identity</td>
</tr>
<tr>
<td>R80</td>
<td>/_IA_API/v1.0/add-identity</td>
<td>/_IA_API/v1.0/delete-identity</td>
</tr>
</tbody>
</table>

Within the ‘Header’ tab, nothing needs to be changed beyond the supplied default. Below is a copy of the parameters in the default context server for reference.

**Figure 5: Context Server – Action Tab**

![Figure 5](image)

Note the attributes and the variables sent to the Check Point firewall within the ‘Content’ tab, the identity-source attribute is set permanently as ‘Aruba ClearPass Policy Manager’. There are several other important parameters within this section, shared-secret, session-timeout, calculate-roles, fetch-user-groups and fetch-machine-groups.

When using the Check Point Identity Awareness feature (RESTful API or RADIUS Accounting) the userID that is received by the firewall typically has to be verifiable as a valid user. Check Point will ensure the user exists within an authoritative Identity Store, like Active Directory. Hence it is required to specify “calculate-role”, “fetch-user-groups” and “fetch-machine-groups”. This is set to 1 for AD users. Note that “fetch-machine-groups” is only relevant for machine identities.

**Figure 6: Context Server – Content Tab**

![Figure 6](image)
To ensure the identity will not be verified against Check Point’s identity sources, the “fetch-user-groups” and “fetch-machine-groups” should be set to 0 (zero). Now, this is very important for Guest Users. Obviously for Guest users their userIDs do not exist within identity stores like Active Directory as they are transient users. Some guest accounts could exist within a directory but that is not usual. So as a part of the integration, identify these users and link them to a user group (a configurable Check Point attribute called access role).

The default Check Point Context Server Action for guest users includes the changes that are discussed above. The URL needs to be modified for the action in R80.XX.

Finally, the shared secret used here must match with the PSK configured on Check Point. The timeout setting has been set to 28800 seconds (8 hours) which can be changed if required, however the logout context-server-action is the action that should deal with logging out Users from the firewall. These values could be set directly within the Content tab or can be set in a more readable format under Attributes tab.

**Figure 7: Context Server – Attributes Tab**

![Endpoint Context Server Details](image)

A separate Context Server Action needs to be created for Guest user account.

Create a copy of the Context Server Action for guest user and modify the settings as shown below. Use the same URL for R80.XX as used in Figure 4.

**Figure 8: Context Server for Guest user – Action Tab**

![Endpoint Context Server Details](image)
The **Header** tab stays unchanged.

The important points to call out below are some of the additional fields that have been added, for example **user-groups**, this is set in our example to **aruba-guest**. We have also added **machine-groups**, this is set in our example to **aruba-guest-machine**. These groups will have to be created on the Check Point firewall. Take care as no validation is performed and the spelling needs to be exactly the same. The creation of this item on the firewall is covered later in section **Check Point Configuration – Guest user account**.

Another field added is **roles**. Note that the roles field is set to `['']`, that's a left and right square bracket.

The final change is that the two group fields, **fetch-user-groups** and **fetch-machine-group** are set to 0, that's a zero.

The fields are added in the **Content** tab and the values are specified under **Attributes**. Let's look at both of these tabs.

**Figure 9: Context Server for Guest user – Content Tab**

<table>
<thead>
<tr>
<th>Content-Type:</th>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content:</td>
<td><code>{&quot;shared-secret&quot;: &quot;%(shared-secret)&quot;}, {&quot;user&quot;: &quot;%(name)&quot;}, {&quot;ip-address&quot;: &quot;%(ip)&quot;}, {&quot;machine&quot;: &quot;%(machine)&quot;}, {&quot;identity-source&quot;: &quot;Aruba ClearPass Policy Manager&quot;}, {&quot;session-timeout&quot;: &quot;%(timeout)&quot;}, {&quot;user-groups&quot;: &quot;%(user-groups)&quot;}, {&quot;machine-groups&quot;: &quot;%(machine-groups)&quot;}, {&quot;roles&quot;: &quot;%(roles)&quot;}, {&quot;fetch-user-groups&quot;: 0}, {&quot;fetch-machine-groups&quot;: 0}</code></td>
</tr>
</tbody>
</table>

**Figure 10: Context Server for Guest user – Attributes Tab**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <code>{shared-secret}</code></td>
<td></td>
</tr>
<tr>
<td>2. <code>{timeout}</code></td>
<td>28800</td>
</tr>
<tr>
<td>3. <code>{user-groups}</code></td>
<td><code>['aruba-guest']</code></td>
</tr>
<tr>
<td>4. <code>{machine-groups}</code></td>
<td><code>['aruba-guest-machine']</code></td>
</tr>
<tr>
<td>5. <code>{roles}</code></td>
<td><code>[]</code></td>
</tr>
<tr>
<td>6. Click to add...</td>
<td></td>
</tr>
</tbody>
</table>
The next step is to modify the Logout Context Server Action. This action would not change for the AD or Guest user and can be used for both. Essentially, it is just sending an IP address using this action asking the Firewall to end the session.

Create a copy and modify the **Action** Tab for the Logout Action. Again, this is required to delete the identity of the user with the IP address and is triggered upon receiving Accounting Stop for NAS. The URL must be defined based on the version of Check Point code (R80.XX is used here)

**Figure 11: Context Server – Action Tab**

![Image of Action Tab]

The next step is to modify the **Content** tab to include the shared secret as shown below. The value of shared-secret must be the same as the one set during the Login Action. This can be set under Content or Attributes tab.

**Figure 12: Context Server – Content Tab**

![Image of Content Tab]

The **Header** tab can be left “as is” and need not require any changes.

The example shown here is for R80.XX. Use the default Check Point Login and Logout Context Server Action for R77.XX as described in the table on Page 10.
To check that all of the Context Server actions have been successfully configured, return to the Endpoint Context Server, and look in the 'Actions' tab, all the 3 actions configured (Login for AD and Guest user and Logout) must be listed as shown in the example below.

**Figure 13: Endpoint Context Server – Actions Tab**

![Endpoint Context Server – Actions Tab](image)

**Enforcement Profile**

Finally, a **Session Notification Enforcement profile** must be configured. Below is an example of a configured profile. Note that there are four `session-notify` attributes that must be added to the profile to make it complete, failure to add all four will result in a failed integration.

1. **Server-Type** [Generic HTTP]
2. **Server IP** [IP address of previously defined HTTP Context Server]
3. **Login Action** [Configured and assigned to the Context Server Login Action]
4. **Logout Action** [Configured and assigned to the Context Server Logout Action]

The Enforcement Profile can be added from **Configuration > Enforcement > Profiles > Add**. Select the **Template** as **Session Notification Enforcement** and use the details as shown in the summary below.

**Figure 14: Enforcement Profile – AD user**

![Enforcement Profile – AD user](image)
The Server IP is the Endpoint Context Server IP defined. Select the Login Action based on the user type that the enforcement profile is being used for. A separate enforcement profile needs to be created for the Guest user. The only thing that changes in the guest enforcement profile is the Login Action.

Once finished, upon receiving a ‘standard’ network authentication (e.g. 802.1X) request, ClearPass Policy Manager will post the userID attributes etc. to the firewall, the posting is pretty much real-time. UserID should appear within 2 seconds.

**Check Point Configuration – AD user**

The first part of this configuration is for scenarios where user belongs to an Active Directory or LDAP server so that it can be verified by Check Point on a gateway running R80.XX.

**Enable Identity Awareness**

Enable the Identity awareness blade and ensure a valid license is activated for the same. If not, kindly contact a Check Point sales representative.

Go to **Gateways & Servers**. Click on the Check Point firewall gateway and enable the **Identity Awareness** option as shown below.

**Figure 15: Enable Identity Awareness**
Adding an AD/LDAP Server

Select/un-select Identity Awareness in the previous step, the following screen will be shown where one can use the AD Query wizard to add the AD Server to the Check Point firewall.

Q? - Why would I want to do this? Well, the userID details that are sent by ClearPass Policy Manager need to either match a user-group or be verifiable with some other identity source, i.e. AD.

Figure 16: Add Active Directory server I

Add the required details, admin account, FQDN, etc. to add an AD to the Check Point firewall. Take notice of the successful completion message at the bottom of the window.

Figure 17: Add Active Directory server II
Create a Web API Host

A Web API client is the entity that would try to communicate with the REST APIs of the firewall which in this case is the ClearPass server IP. The host created here would then be validated with the shared secret configured in the next step when Identity Awareness is enabled.

Login to SmartConsole using an administrator account and add a new host. There are multiple ways to do this in the UI. Navigate to **Gateways & Servers**. In the right-hand side box, click **New > Host**.

**Figure 18: Add a Host I**

![Add a Host I](image)

Specify the **Name** and **IP address** of the ClearPass server trying to access the APIs.

**Figure 19: Add a Host II**

![Add a Host II](image)
Configure Identity Awareness-Web API

Click on the Check Point gateway object under Gateways & Servers. Navigate to the Identity Awareness. Enable Identity Web API and go to Settings as highlighted.

Figure 20: Configure Identity Awareness-Web API

The Identity Web API settings panel would then let us select the host created in the previous step and generate the client secret. The application has an ability to randomly generate a secret and also provides an option to input a string manually. The client secret configured here is what must match the shared secret used in the Login, Logout context server actions configured in ClearPass.
Click on the + sign in the green box to add the host.

**Figure 21: Identity Web API settings**

The settings also provide us with an ability to set the **Client Access Permissions**. Ensure the client can reach the APIs using the interface selected. For our lab, the portal is made accessible ‘**Through all interfaces**’.

Click on **OK** and save the settings.

Finally, the changes made needs to be applied. Click on ‘**Install Policy**’ from Smart Dashboard, to install and activate the configuration on the gateway.
Assuming the above configuration is in place, navigate to ‘Logs & Monitor’ and filter (blade:”Identity Awareness”) using the Identity Awareness Blade and look at the authenticated users on the system. Below, the user ‘fred’ has authenticated with the Identity Source being ‘Aruba ClearPass Policy Manager’.

**Figure 22: AD user authenticated on Check Point**

![Image of Check Point interface with user authentication details]

**Figure 23: AD user authenticated on Check Point details**

![Image of detailed user authentication information]

Note that the “User Groups” and “Machine Groups” can take a comma separated list, it's not mentioned above as our above example shows one group only.
Check Point Configuration – Guest user account

Next, let’s cover the scenario where the user is essentially a guest and Check Point cannot verify the user’s identity beyond what ClearPass sends. For a userID sent by ClearPass where the Check Point firewall is unable to verify the account, some additional configuration needs to be completed. Basically, Check Point needs to be notified that the userID belongs to a group that Check Point is aware of (i.e. a Guest group). This requires us to pre-create the group and then have ClearPass include the group information when it posts the userID to the Check Point firewall. Below example shows a user ‘abhatt’ attempting to authenticate. In this example, the user is a locally defined user in ClearPass, but is not known to Active Directory. The Check Point firewall tried to verify the userID exits but fails. From the log, it can be seen that this user is rejected. In essence, this simulated a guest (i.e. an unknown/unverifiable account) being denied by Check Point.

Figure 24: non-AD user denied by Check Point

To support Guest users, changes need to be made to the Login context server action to make it clear to the Check Point firewall that the userID sent from ClearPass is a GUEST and the firewall must not try to verify the userID but take it at as being a known and trusted user as sent by ClearPass.
The **user-groups** setting sent with the HTTP POST from ClearPass must match configuration on the Check Point firewall. The configuration must match an **access-role**, of the same name. To configure this, go to **Object Explorer** and navigate to **New > User > Access**.

**Figure 25: Adding an Access Role to match the Aruba guest role**

Let us now try to login using a guest user account. In the below example, a guest user attempts to authenticate in Check Point. Navigate to ‘**Logs & Monitor**’ and filter (blade:”Identity Awareness”) using the Identity Awareness Blade.

**Figure 26: Guest user authenticated on Check Point**
Now that users are being accepted and labeled in Check Point, policy can be used to reference the Guest users by the aruba-guest label. In the below example, I created an address-range object for our 10.0.0.0 internal network. In the simple rule below I used this to deny guests effectively accessing any of our corporate network objects.

**Figure 28: Firewall Policy to deny access to internal network**

This completes the Check Point firewall gateway configuration to enable the REST API integration between ClearPass and Check Point.
Configuring Radius Accounting Proxy

An additional integration method to support third party vendors can be achieved with the ability to configure a RADIUS Accounting Proxy. This allows ClearPass to proxy the RADIUS accounting data that is received to an external system such as an external firewall. When ClearPass processes an authentication request, as a part of the session configuration on ClearPass a RADIUS Accounting Proxy target can also be configured which allows it to forward the interim accounting updates it receives from the NAS to this external target.

Configuring RADIUS Accounting Proxy on ClearPass

Configure Accounting Proxy on ClearPass as shown below. First configure the targets, under Configuration> Network > Proxy Targets. It is the same as configuring RADIUS authentication proxy-ing.

Figure 29: Adding a RADIUS Accounting Proxy Target on ClearPass

![Adding a RADIUS Accounting Proxy Target on ClearPass](image)

Let's configure a Service definition to use the Accounting Proxy defined. The Accounting Proxy tab is not shown by default and needs to enabled as highlighted below.

Figure 30: Enabling Accounting Proxy in a ClearPass Service

![Enabling Accounting Proxy in a ClearPass Service](image)
Now that the target is defined and the Accounting Proxy is enabled the remaining configuration can be completed.

**Figure 31: Adding Accounting Proxy Target to a ClearPass Service**

RADIUS accounting data received from the NAS will be forwarded to the Accounting Proxy target. VSAs and IETF standard attributes standard attributes can be added to the data that is forwarded. However, to add a VSA one must have the Dictionary's for that vendor’s product installed/enabled within ClearPass. Some vendors have multiple RADIUS Dictionaries across their product ranges, so just because ClearPass has one for company X does not mean it will encompass all their products and the VSA’s they support.

**Configuring RADIUS Accounting on Check Point**

**Enable Identity Awareness**

Refer Figure 15 for configuration steps.

**Add an AD/LDAP Server**

Please note this step is required for the Active Directory uses so that the userID details that are sent by ClearPass are verified with some other identity source like AD.

Refer Figure 16 and Figure 17 for configuration steps.

**Add a Network Object**

Add the ClearPass server as a network object (it just needs a name and a IP address). Below is an example of creating a Network Host object. This can then be referenced in the RADIUS accounting section that follows.

Login to SmartConsole using an administrator account and add a new host. There are multiple ways to do this in the UI.
Navigate to **Gateways & Servers**. In the right-hand side box, click **New > Host**.

**Figure 32: Add a Network Object**

![New Host window showing ClearPass and Host details with IP address fields]

**Configure Identity Awareness-RADIUS Accounting**

Click on the Check Point gateway under **Gateways & Servers**. Navigate to the **Identity Awareness**. Enable **RADIUS Accounting** and go to **Settings** as highlighted.

**Figure 33: Configure Identity Awareness-RADIUS Accounting**

![Check Point Gateway window showing Identity Awareness and authorized clients settings]

Click on **Settings** and add the Network object, the message highlighted “Authorized clients are not selected” should go away once the settings are configured.
Let's configure the RADIUS Accounting settings as shown below.

Click on the + sign in the green box to add the host. Add a shared secret either generated automatically or can be specified manually in the space provided.

Note the **RADIUS Client Access Permissions**. Ensure the RADIUS proxy client can reach the server on port 1813 using the interface selected. For our lab, the portal is made accessible *Through all interfaces*.

Select the RADIUS Accounting attributes that Check Point will parse and map to.

Click on **OK** and save the settings.

**Figure 34: Configure RADIUS Accounting**

![RADIUS Accounting Settings](image)

Finally, the changes made needs to be applied. Click on *Install Policy* from Smart Dashboard, to install and activate the configuration on the gateway.
In the above settings, accounting attributes 31, 1 and 8 have been included. These are the three attributes ClearPoint will parse and map to Machine-Name, Username and Endpoint SRC IP address. The attributes that are required may differ.

Once this is configured, the Check Point firewall should be able to receive and parse the mapped attributes from the RADIUS accounting data.

Navigate to ‘Logs & Monitor’ and filter (blade:“Identity Awareness”) using the Identity Awareness Blade to look at the authenticated users on the system. Below the user ‘cam’ along with the endpoint IP (10.1.1.1) authenticated and the Identity Source shows as ‘Radius Accounting’.

**Figure 35: Authenticated User on Check Point – RADIUS Accounting**

The above solution provides for mapping THREE RADIUS accounting attributes. There is a long process to get a fourth Accounting attribute to be exposed. This allows for ClearPass to attach what can be thought of as a ‘user-role’ to the user name in the Accounting data. Check Point can then use this ‘user-role’ to enforce policy against different ‘classes’ of users based upon the ‘user-role’. Typically, RADIUS Accounting user group information is retrieved from identity servers (AD/LDAP servers or internal databases), but by utilizing this one can bypass the typical logic processing of the Check Point firewall and ‘force’ the firewall to trust the group/role information ClearPass sends.

The attribute is not exposed by default in 80.XX. It would require us to install a HotFix. The availability of the HotFix called ‘RADIUS Accounting Groups’, released in July 2014 must be checked with Check Point for the installed Check Point version. However, the best recommended method in that case would be to use the Identity Awareness Web API.
Appendix A – Troubleshooting and Support

Monitoring/Debugging Identity Awareness from the Check Point CLI

Several very useful commands are available to monitor the role/group associated of users that are being sent from ClearPass.

Access the cli, via an SSH command and run the Expert mode. Once the access is granted switch to the Expert mode, following commands are useful.

`pdp monitor ip a.b.c.d`

```
[Expert@restapi-gw:0]# pdp m ip 10.2.100.167

Session: 473d7552
Session UUID: {5EB93636-3FDC-7955-608E-5BCCCE7DFDA1}
Ip: 10.1.1.1
Machine: dannysipadmin (5bb0e37f)
  Groups: aruba-guest-machine
  Roles: aruba-guest
  Client Type: Identity Awareness API (Aruba ClearPass Policy Manager)
  Authentication Method: Trust
  Connect Time: Fri Apr 3 20:21:56 2015
  Next Reauthentication: Fri Apr 3 20:50:29 2015
  Next Connectivity Check: -

Users:
  djj {2fa55b51}
  Groups: aruba-guest
  Roles: aruba-guest
  Client Type: Identity Awareness API (Aruba ClearPass Policy Manager)
  Authentication Method: Trust
  Connect Time: Fri Apr 3 20:21:56 2015
  Next Reauthentication: Sat Apr 4 04:22:26 2015
  Next Connectivity Check: -

Packet Tagging Status: Not Active
Published Gateways: Local
**************************************************************************
```

The above shows the output for the user and machine authentication and the group/role assignment.
To check just on a user’s role/grouping the below command provides that insight.

`pdp m user [user-name]`

```
[Expert@restapi-gw:0]# pdp m user djj

Session: 473d7552
Session UUID: {5EB93636-3FDC-7955-608E-5BCCCE7DFDA1}
Ip: 10.1.1.1
Users:
djj {2fa55b51}
  Groups: aruba-guest
  Roles: aruba-guest
  Client Type: Identity Awareness API (Aruba ClearPass Policy Manager)
  Authentication Method: Trust
  Connect Time: Fri Apr 3 20:21:56 2015
  Next Reauthentication: Sat Apr 4 04:22:26 2015
  Next Connectivity Check: -

Packet Tagging Status: Not Active
Published Gateways: Local
*****************************************************************************
```

**ClearPass Logs**

ClearPass collects multiple log files that can assist the administrator in debugging ClearPass to Check Point integration problems. The most useful of these logs is the postauthctrl.log file. The process that triggers sending data via the REST API is performed by the post_authentication daemon which updates this log file.

To collect and access this log file takes multiple steps, please follow these steps:

Under **Administration > Server Manager > Server Configuration**, select the system for which the logs need to be collected from a cluster then click ‘**Collect Logs**’.

Collect only the highlighted ‘Logs from all Policy Manger services’ below to obtain the postauthctrl.log file.

This will save significantly on the log collection process and the corresponding download file is much smaller. For troubleshooting and analysis of the issue, engage Aruba TAC. Collect the System Logs and Policy Manager service logs. Attach them to the case created for faster resolution.
Download the Log file and navigate to the path shown below

Once postauthctrl.log file is located, there are certain entries that should be looked for as shown below. These provide an insight into the communication between ClearPass and the Check Point Firewall.


Appendix B – XML

The Context Server Actions for Login and Logout of Guest and AD user are not available by default for R80.XX. It can be easily imported into ClearPass using the XML file available on Aruba GitHub

https://github.com/aruba/clearpass-exchange-snippets/tree/master/firewall/check-point

- Download the XML file “clearpass-exchange_checkpoint_csa_r80.xml”.
- Open this file in your favorite editor.
- Use the Find and Replace feature of the editor to replace “<<Check Point Firewall IP>>” with the actual IP address of the Check Point firewall configured.
- Similarly Find and Replace “<<Shared Secret >>” with the string to be used.
- Save the file and Import.

The file can be imported from Administration > Dictionaries > Context Server Actions.

**Figure 38: Import Context Server Actions-R80**

The above action will import 3 Context Server Actions on ClearPass.