



Palo Alto Networks

aruba

a Hewlett Packard
Enterprise company

ClearPass

Integration Guide

ClearPass and Palo Alto Networks Integration Guide

Change Log

Version	Date	Modified By	Comments
1.0	May 2013	Danny Jump	Initial Integration Guide V1
2.0	June 2013	Danny Jump	Minor updates for ClearPass 6.1
3.0	Sept 2013	Danny Jump	Updates to support ClearPass 6.2, changes to post_auth and Troubleshooting section
4.0	Feb 2014	Danny Jump	Updates to support ClearPass 6.3, changes to post_auth and details on our HIP support
5.0	May 2015	Danny Jump	Updates to support changes in ClearPass 6.5
6.0	May 2017	Robert Filer	Wordsmith and edits to V6
6.0	May 2017	Danny Jump	Removed PAN-OS 5.x related content and added updates to support sending of ROLES [ClearPass 6.6.4] and some minor edits and updates from Aruba TAC/ERT.
7.0	Aug 2018	Arpit Bhatt	Removed content related to 6.5 and below. Added changes introduced in 6.7

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

Overview	8
Why is this Integration Important?.....	8
The Challenge	8
Background	8
Next-Generation Solution	9
Software Requirements.....	9
ClearPass Configuration.....	10
What's new in ClearPass 6.7?.....	10
What's new in ClearPass 6.6?.....	10
ClearPass Basic Configuration - All ClearPass Versions	11
ClearPass Basic Configuration – Enabling Insight & Profiling	11
ClearPass Basic Configuration - Interim Accounting.....	12
NAS/NAD Basic Configuration – Interim Accounting	12
ClearPass Configuration – Post-Authentication	14
Adding Palo Alto Networks Firewall & Panorama Context Servers	15
Adding Palo Alto Networks Firewall Context Servers in ClearPass 6.7	15
Adding Palo Alto Context Servers in ClearPass 6.6.5	16
Adding Palo Alto Networks Panorama Context Server Endpoint.....	17
Summary of Shared Context Attributes	18
Sending Updates to Palo Alto in 6.7 as part of Service Policy	19
Sending Updates to Palo Alto in 6.6 as part of Service Policy	20
Adding an Enforcement Profile to an Enforcement Policy.....	21
Adding an Enforcement Policy to a Service.....	21
Sending Health/Posture status to Palo Alto from ClearPass	22
Configuring OnGuard on ClearPass.....	22
Configuring Palo Alto to use Health/Posture context.....	22
Configuring TAGS for Health/Posture.....	23
Setting the ClearPass Posture/Health Delay Timer in 6.6	25
Sending ClearPass Roles and using them in Palo Alto	27
Configuring Palo Alto Networks Next-Generation Firewall	30
Configuring ClearPass to communicate with Palo Alto using the UserID API	30
Configuring a Policy on Palo Alto to use the ClearPass context data – generic info.....	31
Creating Device Profile Categories.....	31
Configuring Palo Alto Networks PAN-OS 6.x - Tags and HIP Objects.....	32
To create the Tags.....	33
Group TAGS in Address Groups	33
Create the HIP Objects	34
Other supported Attributes for HIP Object.....	34
PAN-OS 6.x DAG/TAG Limits.....	37
Faultfinding Tips (PANOS cli cmds/ClearPass Logs).....	38
UserID <-> IP Address Mapping.....	38
Dynamic Device (Tag) <-> IP Address Mapping	39
UserID <-> ClearPass Roles	39
UserID <-> Showing all Dynamic DAGs.....	40

ClearPass and Palo Alto Networks Integration Guide

Show HIP Reports.....	40
Some additional Debugging Commands.....	41
Show XMLAPI statistics	41
Real-Time debug monitoring of the UserID process	42
Check ClearPass Logs files	43
Sending login UserID + Source IP@, as user logs in.....	45
Adding IP@ to Category, as ClearPass profiles the IP@	45
Sending logoff UserID + IP@, as user logouts.....	45
Removing IP@ from Category as device logout.....	46
XML example of HIP Object	46
Conclusion	48

Figures

Figure 1: ClearPass and Palo Alto Networks Integration Overview.....	9
Figure 2: Checking Insight DB is enabled	11
Figure 3: Checking RADIUS Interim-Accounting is enabled on ClearPass	12
Figure 4: Enable RADIUS Interim accounting on Aruba Controller	12
Figure 5: Configuring RADIUS authentication on Cisco WLC	13
Figure 6: Configuring RADIUS accounting on Cisco WLC	13
Figure 7: Post Authentication run-times across different ClearPass versions	14
Figure 8: Summary of features across versions	15
Figure 9: Adding the Context Server mapping in ClearPass 6.7	16
Figure 10: Configuring the optional sending of roles and IP/Device mapping in ClearPass 6.6.5+	16
Figure 11: Appending DOMAIN/Full-username	17
Figure 12: Adding Palo Alto Networks Panorama as Endpoint Context Server	17
Figure 13: Attributes we can share with Palo Alto Networks endpoints	18
Figure 14: Adding an enforcement-profile for Palo Alto in ClearPass 6.7	19
Figure 15: Setting Palo Alto User Identification Timeout	19
Figure 16: Adding an enforcement-profile for Palo Alto in ClearPass 6.6	20
Figure 17: Adding a Session-Check one endpoint per enforcement profile.....	20
Figure 18: Trigger Palo Alto update on AD memberOf 'contains' rule	21
Figure 19: Palo Alto enforcement profile added to a service	21
Figure 20: Configuring TAGS on Palo Alto	23
Figure 21: Examples off "Not_Healthy" TAGS	23
Figure 22: Creating an Address-Group to match on ANYTHING unhealthy	24
Figure 23: Creating different Address-groups to check on individual failures	24
Figure 24: Adding an Address-group to a firewall policy.....	25
Figure 25: Setting Eager handler to 120 seconds when sending posture/health	25
Figure 26: Sending Posture Token using 6.7	26
Figure 27: Role Mapping example.....	27
Figure 28: User authentication with role mapping.....	27
Figure 29: Creating the TAGs	28
Figure 30: Adding TAGs to an Address-Group.....	28
Figure 31: Firewall rule with Address-Group match	29
Figure 32: Firewall dropping data against plm-role	29
Figure 33: Creating a restricted Admin-Role	30
Figure 34: Adding a User to Palo Alto Networks Firewall	31
Figure 35: ClearPass Fingerprints.....	32
Figure 36: Adding a TAG under PAN-OS 6.x	33
Figure 37: Grouping Tags into a Dynamic Address Group	33
Figure 38: Creating HIP Objects.....	34
Figure 39: ClearPass Fingerprints – Client Version	35
Figure 40: Utilizing Tags in a Firewall Rule.....	35
Figure 41: Building a security policy using endpoint type	36
Figure 42: Number of supported DAG's across Palo Alto Platforms.....	37
Figure 43: Signed in User's to their IP Mapping	38
Figure 44: Showing active Users relative to their IP Mapping and also policy matches	38

Figure 45: Showing active Users relative to their IP Mapping and Idle Timeout	38
Figure 46: Dynamic Object Category - IP Address Mapping.....	39
Figure 47: Showing ClearPass Role to DAG mapping	39
Figure 48: Showing configured DAGS and their assigned Policy.....	40
Figure 49: HIP Report for a user	40
Figure 50: HIP Database in Debug	41
Figure 51: XMLAPI Stats	41
Figure 52: List of ALL users registered through ID Manager	42
Figure 53: Collecting ClearPass Logs – limited data, but includes postauthctrl.log	43
Figure 54: Collection of ClearPass Logs complete	44
Figure 55: Where to locate postauthctrl.log.....	44

Overview

This document is intended to help field engineering, customers, and channel partners integrate ClearPass Policy Manager with Palo Alto Networks next-generation firewalls and its central management system, Panorama. Customers can now leverage the identity tracking features provided by ClearPass for known enterprise users using Active Directory and LDAP servers, and for unknown guest/public users that are used by Guest and Hotspot networks.

Why is this Integration Important?

Palo Alto Networks next-generation firewall offers contextual security for all users for a number of reasons, but especially for safe enablement of application access. Simple firewalling using IP addresses or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks.

As an example, it's no longer acceptable to just 'deny Twitter' or 'deny Facebook' access. Many organizations use social networking Web sites to advertise their products, solutions, and activities. Social networking has become an accepted marketing tool and many companies now opt to use this as a mainstream part of their marketing efforts. As such, legacy firewalls are not able to differentiate valid authorized users from casual social networking users. So today's challenge to allow Facebook based upon contextual data such as username makes it almost impossible for legacy firewalls to implement granularity in their security policy.

The Challenge

Historically, traditional firewalls make decisions based on Layer 3/4 and some Layer 7 information. For Web-based traffic, a decision can be made based upon a domain or a URL string. Today, enterprises want to make decisions based upon the user (or group) and associated permissions. For this to happen, the firewall needs to correlate between the user and the assigned IP address. The challenge is finding meaningful sources of user information covering the full spectrum of network activity, including known users, guests, and non-enterprise users.

Background

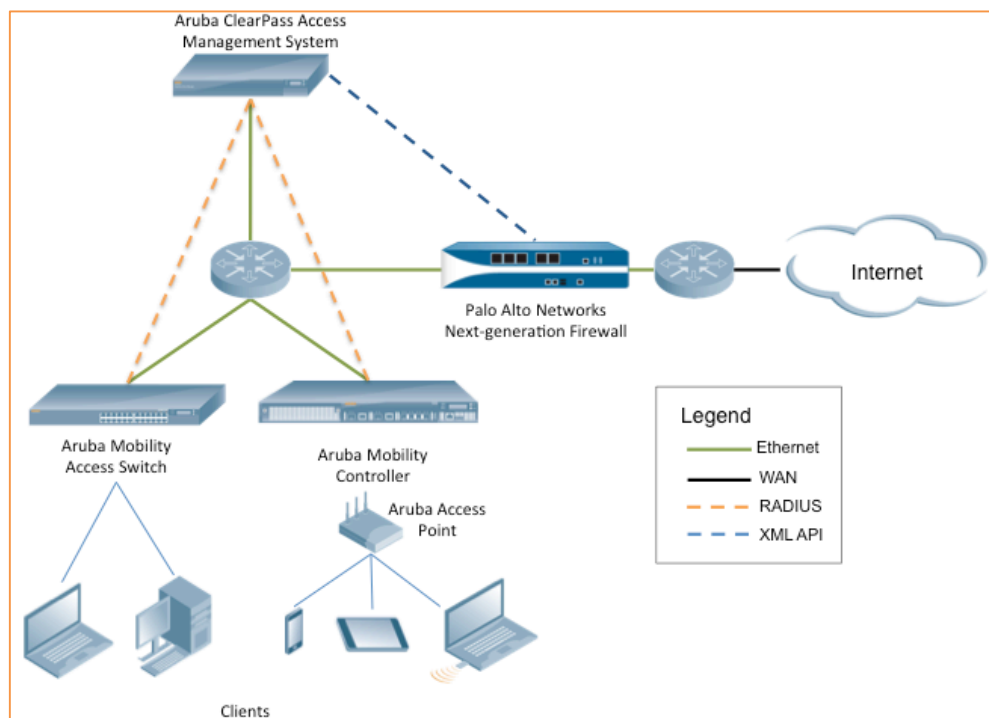
One of the core features of the Palo Alto Networks next-generation firewall is User-ID, which provides many methods for connecting to sources of identity information and associating them with firewall policy rules. For example, it has an option to gather user information from an Active Directory or LDAP server. In the past, this functionality required the use of a Palo Alto Networks User-ID agent running on a Windows workstation.

Similarly, an agent can be used to allow integration with a legacy Amigopod deployment to gather user information for the guest users. This integration allows Amigopod to send user information to a Palo Alto Networks firewall via the User-ID agent running on a Windows workstation. In both scenarios above, the past approaches required an agent which created dependencies that might not be easy to resolve in certain deployment scenarios. Now you can take advantage of the Palo Alto Networks and Aruba Networks ClearPass Policy Manager, making a more seamless integration possible.

Next-Generation Solution

Starting with the release of ClearPass Policy Manager 6.1, Aruba re-architected the integration between ClearPass and the Palo Alto Networks next-generation firewall to take advantage of the new XML APIs that were available in the PAN OS 5.x code release. This simplified the solution significantly by making it more efficient and streamlined. The requirement to download and configure a separate plug-in was eliminated and instead the solution was fully integrated into the ClearPass core product.

Figure 1: *ClearPass and Palo Alto Networks Integration Overview*



Software Requirements

The minimum software version required on ClearPass Policy Manager is 6.1.0, released in April 2013. The minimum software version on the Palo Alto Networks firewall is PAN-OS 5.0.0, released in November 2012.

However, it is recommended that you regularly review software updates to utilize the benefits from the latest fixes and feature updates from Aruba and Palo Alto Networks.

To avail the latest features of this integration, use ClearPass version 6.7.3 and above. At the time of writing, version 6.7.5 is available and is the recommended release.

ClearPass Configuration

Configuring ClearPass Policy Manager for Palo Alto Networks firewall integration is a fairly simple, straightforward process. Step-by-step instructions are outlined in the following sections. The configuration has been separated into several sections, the first being to highlight the new functionality in ClearPass 6.6, then several sections covering the integration.

The ClearPass Policy Manager Exchange framework was enhanced in 6.5 and subsequently in 6.6 and now provides integration with additional 3rd party vendors. This allows ClearPass to push the endpoint source IP address, username and other attributes such as Health/Posture and Role to other 3rd party firewalls (e.g. Checkpoint, Fortinet, and iboss).

What's new in ClearPass 6.7?

The core functionality still remains the same for this Integration. There are two changes in terms of ClearPass Policy Manager posting data to Palo Alto Firewall.

ClearPass now adds an ability for the administrator to select the Context Server Action that can be posted at Login and Logout. In previous versions, ClearPass would post all the information to Palo Alto Firewall however, ClearPass provides an option to select the relevant actions that need to be posted which may vary for every environment. For example, a customer may not want the HIP data and would only like to get the user-ip correlation. In previous versions, ClearPass posts all the information collected. Hence this improves efficiency and reduces overhead.

Starting in PAN-OS 8.0 Palo Alto Firewalls requires a mandatory value for the User Identification Timeout. This value is set to 45 mins by default on the Firewall. ClearPass now posts this value to the Firewalls along with the other details. Failure to send this value would result in the post being rejected by the Firewall. Hence customers running PAN-OS 8.0 should upgrade to ClearPass 6.7 for the Integration to work.

What's new in ClearPass 6.6?

No new functionality was added in the initial 6.6.0 ClearPass release. However, in the 6.6.4 release new functionality was added that had been requested from a number of customers/partners. Everyone should be familiar with the concept of ClearPass assigning a ROLE as part of user or device authentication. This is a point in time calculation based upon a multitude of meta-data that represents elements of the user, device, location, time, health, etc. Being able to share this ROLE (think label) with other parts of the security landscape simplifies the creation of a ubiquitous security policy across differing vendors and platforms. Palo Alto has never had the ability to consume this ROLE/label and subsequently utilize this in a form where it can be used to enforce security policy.

Starting in 6.6.4 the ability to send the ROLE (label) as a Dynamic-Access-Group (DAG) tag was added. With the tag now holding the ROLE, policy can be built within the Palo Alto firewall based upon the tag. This significantly simplifies the policy integration between ClearPass and a Palo Alto firewall.

In ClearPass 6.6.5, a new option was exposed to OPTIONALLY send the ROLE information and the generic IP/User mapping. There are some restrictions within the lower-end VM firewalls limiting the number of supported DAGs. Sending significant numbers of ROLES could cause resource related issues.

ClearPass Basic Configuration - All ClearPass Versions

ClearPass Basic Configuration – Enabling Insight & Profiling

Before starting the configuration of the Palo Alto Networks services/profiles, etc., ensure that basic configuration items are completed. Insight must be enabled on at least one node in the cluster for the Palo Alto Networks integration to function.

Under **Administration > Server Manager > Server Configuration > System**, check both the ‘**Enable Insight**’ and ‘**Enable this server for endpoint classification**’ settings.

Figure 2: Checking Insight DB is enabled

Administration » Server Manager » Server Configuration - ccppm6dot6-160

Server Configuration - ccppm6dot6-160 (10.60)

System Services Control Service Parameters System Monitoring Network FIPS

Hostname: ccppm6dot6-160

FQDN: ccppm6dot6-160.ns-tme.com

Policy Manager Zone: default

Enable Profile: ☒ Enable this server for endpoint classification

Enable Performance Monitoring Display: ☒ Enable this server for performance monitoring display

Insight Setting: ☒ Enable Insight ☒ Enable as Insight Master Current Master: ccppm6dot6-160(10.60)

OnConnect Setting: ☒ Enable OnConnect Primary master

Enable Ingress Events Processing: ☒ Enable Ingress Events processing on this server

Span Port: -- None --

Why INSIGHT must be enabled - The Insight Application must be running. It is used to collate the records that feed the API used to send information to Palo Alto. 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** to share the device context. 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, for example on the network to plan port-spans/port-taps to forward data to a ClearPass node with a port configured as a port-span.

ClearPass Basic Configuration - Interim Accounting

Next, ensure that ClearPass is logging the RADIUS Interim-Accounting Updates it receives from the NAD. This can be checked at **Administration > Server Manager > Server Configuration > Service Parameters**. The default is **FALSE**. Ensure its configured as **TRUE** as shown below

Figure 3: Checking RADIUS Interim-Accounting is enabled on ClearPass

Administration » Server Manager » Server Configuration - cppm161

Server Configuration - cppm161 (10.)

System Services Control **Service Parameters** System Monitoring Network FIPS

Select Service: Radius server

Parameter Name	Parameter Value	Default Value	Allowed Values
EAP-FAST			
Master Key Expire Time	1 weeks	1 weeks	
Master Key Grace Time	3 weeks	3 weeks	
PACs are valid across cluster	TRUE	TRUE	
Proxy			
Maximum Response Delay	5 seconds	5	1-5
Maximum Reactivation Time	120 seconds	120	60-3600
Maximum Retry Counts	5 retries	5	2-10
Accounting			
Log Accounting Interim-Update Packets	TRUE	FALSE	

NAS/NAD Basic Configuration - Interim Accounting

Ensure RADIUS interim accounting is enabled on the NAS device. Also, it's very important to ensure that the **calling-station-ID** is set to use the MAC address of the client (this is the default for Aruba controllers). If the NAS device is configured to use the system IP address, ClearPass will not be able to collate the data correctly within Insight, and thus will be unable to send the correct data to the Palo Alto Networks Firewall or Panorama system.

For **Aruba controllers**, enable RADIUS Interim accounting as shown below on the AAA Profile.

Figure 4: Enable RADIUS Interim accounting on Aruba Controller

aruba MOBIILITY CONTROLLER | WLAN7210 Log out admin

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
WIP
AirWave
NETWORK
Controller
VLANs
Ports
IP
SECURITY
> **Authentication**
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP
Bandwidth Calculator
Threshold

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Keynote-AAA-Profile
keynote-clm-aaa_prof
Lab-Open-AAA-Profile
mac-auth-160
MFA-Demo-aaa_prof
netcaler
ngm-guest-profile
NoAuthAAAProfile
np-panw-profile
Onboard-AAA-Profile
open-guest
TechPG-Guest-AAA-Profile
TechPG-Open-AAA-Profile
TechPG-Secure-AAA-Profile
TME-DUO-GUEST-AAA-Profile
TME-DUO-ONBOARD-AAA-Profile
TME-DUO-SECURE-AAA-Profile
TME-IW-GUEST-Profile
TME-IW-SECURE-Profile
TME-MFA-AAA-Profile
tme-pan-secure

AAA Profile > tme-pan-secure Show Reference Save As Reset

Initial role	logon
MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest
Download Role from CPPM	<input type="checkbox"/>
Set username from dhcp option 12	<input type="checkbox"/>
L2 Authentication Fail Through	<input type="checkbox"/>
Multiple Server Accounting	<input type="checkbox"/>
User idle timeout	<input type="checkbox"/> Enable seconds
Max IPv4 for wireless user	2
RADIUS Roaming Accounting	<input type="checkbox"/>
RADIUS Interim Accounting	<input checked="" type="checkbox"/>
User derivation rules	--NONE--
Wired to Wireless Roaming	<input checked="" type="checkbox"/>
SIP authentication role	--NONE--
Device Type Classification	<input checked="" type="checkbox"/>
Enforce DHCP	<input type="checkbox"/>
PAN Firewall Integration	<input type="checkbox"/>
Open SSID radius accounting	<input type="checkbox"/>



An example of checking this on a Cisco wireless-controller is below. Note that the IP address is used by default. Ensure this is configured as shown below.

For **Cisco controllers**, ensure RADIUS Authentication and RADIUS Accounting are configured as shown below, taking special notice that the **Call-Station-ID Type** is set to **System MAC Address**.

Figure 5: Configuring RADIUS authentication on Cisco WLC

The screenshot shows the Cisco WLC Security page. The 'SECURITY' tab is selected. In the left sidebar, 'AAA' is expanded, and 'RADIUS' is selected. The 'RADIUS Authentication Servers' section is highlighted. The 'Call Station ID Type' is set to 'System MAC Address'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen'. A table lists three RADIUS servers.

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	192.168.5.217	1812	Disabled	Enabled <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.2.51.113	1812	Disabled	Enabled <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	10.2.50.178	1812	Disabled	Enabled <input checked="" type="checkbox"/>

Figure 6: Configuring RADIUS accounting on Cisco WLC

The screenshot shows the Cisco WLC Security page. The 'SECURITY' tab is selected. In the left sidebar, 'AAA' is expanded, and 'RADIUS' is selected. The 'RADIUS Accounting Servers' section is highlighted. The 'MAC Delimiter' is set to 'Hyphen'. A table lists three RADIUS servers.

Network User	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	1	192.168.5.217	1813	Disabled	Enabled <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	2	10.2.51.113	1813	Disabled	Enabled <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	4	192.168.5.220	1813	Disabled	Enabled <input checked="" type="checkbox"/>

ClearPass Configuration – Post-Authentication

The data that ClearPass collates and writes to the Insight DB is extracted and written to the Palo Alto Networks Firewall or Panorama endpoint by the post_authentication daemon. The running of this daemon is controlled by system/cluster-wide configuration discussed below. The version of ClearPass in use, will dictate the frequency at which this daemon runs.

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 the Palo Alto Networks endpoint. The process to gather all the contextual data into a format that ClearPass sends has been streamlined over several releases. Once the data is gathered there is a process which POSTs this data to the Palo Alto Networks Firewall. This batch process is called the post_authentication daemon and is discussed below.

The below table shows the settings of the post_authentication daemon.

Figure 7: Post Authentication run-times across different ClearPass versions

ClearPass Version	Max / Min / Default Values	Recommended Value	Expected delay in endpoint appearing in Palo Alto
6.2 / 6.3 / 6.4	300 sec / 10 sec / 30 sec	10 sec **	10-15 seconds
6.5 / 6.6 / 6.7	300 sec / 3 sec / 30 sec	10 sec **	10-15 seconds



Lowering the Eager handler must be done with care such that it does not affect other system functions. See page 24 for more details.

Adding Palo Alto Networks Firewall & Panorama Context Servers

Minor differences exist in the GUI Context Server configuration depending on the version of ClearPass in use. These mainly relate to capability enhancements between ClearPass and Palo Alto Networks firewalls.

Figure 8: *Summary of features across versions*

ClearPass Version	Addition	Comments	Example
6.7	Control the data to be sent to the Firewall. Send User Identification Timeout	ClearPass provides an option to select the context that needs to be posted to the Firewall.	Administrator can select to send the USER IP correlation but not send the HIP or posture data to the Firewall.
6.6.5	Ability to send roles	ClearPass can send a role which will be mapped into a TAG on the firewall. This TAG can then be mapped to Address Group to define policies	User danny is assigned a role of PLM on ClearPass and hence mapped to the TAG PLM on the Firewall. This TAG is mapped to Address Group where policies can be defined.

Adding Palo Alto Networks Firewall Context Servers in ClearPass 6.7

Navigate to **Administration > External Server > Endpoint Context Servers > Add Context Server** and select **Palo Alto Networks Firewall**, enter the required IP address of the Palo Alto Networks Firewall, and a username/password pair that ClearPass will use to send user/endpoint context data.

Starting in 6.7, Context Server Actions that can be triggered in the Enforcement Profile are configurable. The role and device profile information have been moved from the Context-Server and are now optional context-server-actions. These can be seen on the Actions tab associated with a Palo Alto Firewall context-server as highlighted below.

Figure 9: Adding the Context Server mapping in ClearPass 6.7

Modify Endpoint Context Server	
Server Actions	
Server Type:	Palo Alto Networks Firewall
Server Name:	X.X.X.X
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Authentication Method:	Basic
Username:	cppm-api
Password:
Verify:
Username Transformation:	None
Validate Server:	<input type="checkbox"/> Enable to validate the server certificate

Adding Palo Alto Context Servers in ClearPass 6.6.5

As discussed above in 'What's new in ClearPass 6.6?', the ability to control the sharing of Roles and IP/Device mapping was added. The endpoint profile information has always been sent, and when roles were introduced in 6.6.4, they were sent as well. In 6.6.5 a new option was exposed to be selective in the sending of IP/device mapping and roles as shown below.

Figure 10: Configuring the optional sending of roles and IP/Device mapping in ClearPass 6.6.5+

Modify Endpoint Context Server	
Server	
Server Type:	Palo Alto Networks Firewall
Server Name:	10.2.100.10
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Username:	cppm-api
Password:
Verify:
Username Transformation:	Use Full Username
GlobalProtect:	<input type="checkbox"/> GlobalProtect Enabled on Palo Alto Networks Firewall
ClearPass Profiler:	<input checked="" type="checkbox"/> Enable sending of endpoint profile information
ClearPass Role:	<input type="checkbox"/> Enable sending of applicable role information
UserID Post URL:	https://{server_ip}/api/?type=user-id&action=set&key={key}
Validate Server:	<input type="checkbox"/> Enable to validate the server certificate

Sending of Roles is disabled by default

Configuring the username on the Palo Alto configuration above is documented in a later section, "Configuring Palo Alto Networks Next-Generation Firewall".



Do **not** change the Server Base URL or UserID Post URL. Although the fields can be modified, they are specifically formatted to work with a Palo Alto Networks firewall or Panorama system.

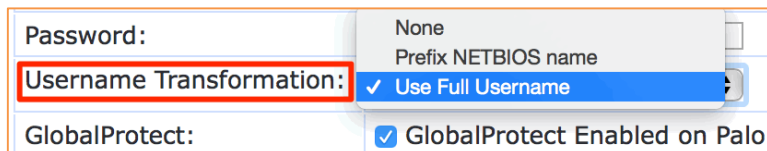
The username posted from ClearPass to Palo Alto can be transformed using the **User Transformation** option while adding the Context Server Action.

None – User ID updates and HIP Reports will only have an entry for the username.

Prefix NetBIOS Name – User ID updates will have an entry as NetBIOS **Name\username**; the HIP Report will also have NetBIOS **Name\username**, and will include NetBIOS Name as domain field.

Use Full Username – User ID updates will have an entry as Full Username propagated by policy server. If authentication is against AD it will be similar to above NetBIOS **Name\username**, else Some Other **Domain\username** in case of say Guest Captive Portal or Username@somedomain which is not accepted by Palo Alto, HIP Report will have same entry, but the domain field will not be sent.

Figure 11: Appending DOMAIN/Full-username



A screenshot of a configuration interface showing a dropdown menu for 'Username Transformation'. The menu is open, showing three options: 'None', 'Prefix NETBIOS name', and 'Use Full Username'. The 'Use Full Username' option is selected and highlighted in blue. A red rectangle highlights the 'Username Transformation' label and the dropdown menu.

Password:	None
Username Transformation:	Prefix NETBIOS name
	✓ Use Full Username
GlobalProtect:	✓ GlobalProtect Enabled on Palo



The Palo Alto Networks firewall can only accept the UserID in the format **domain\username**. Policies on the Palo Alto can then be configured to use the “**domain**” portion of the **domain\username** if required.

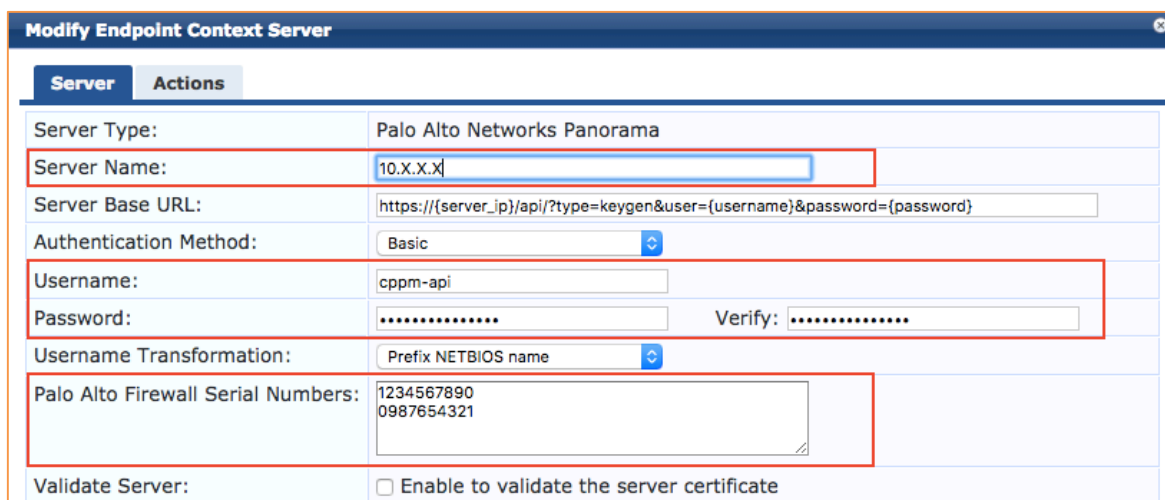
Adding Palo Alto Networks Panorama Context Server Endpoint

Palo Alto Networks Panorama is the centralized management system for the next generation Palo Alto Firewalls. ClearPass has an option to integrate directly with Panorama, which in turn will forward the information to multiple Firewalls it manages.

Under **Administration > External Server > Endpoint Context Servers > Add Context Server > [choose] Palo Alto Networks Panorama**, enter the required IP address of the Palo Alto Networks Panorama server and a username/password pair that ClearPass will use to send the information. The User Transformation settings remain the same as described in the previous page. In addition, it's very important that you configure the serial numbers of the Palo Alto Networks firewalls that are under management by the Panorama appliance as shown below, e.g. 1234567890 in Figure 14.

Configuring the username used below is discussed in a later section “*Configuring Palo Alto Networks Next-Generation Firewall*”.

Figure 12: Adding Palo Alto Networks Panorama as Endpoint Context Server



A screenshot of the 'Modify Endpoint Context Server' form in the ClearPass interface. The form is titled 'Modify Endpoint Context Server' and has a 'Server' tab selected. The form contains several fields: 'Server Type' (Palo Alto Networks Panorama), 'Server Name' (10.X.X.X), 'Server Base URL' (https://{server_ip}/api/?type=keygen&user={username}&password={password}), 'Authentication Method' (Basic), 'Username' (cppm-api), 'Password' (masked), 'Verify' (masked), 'Username Transformation' (Prefix NETBIOS name), 'Palo Alto Firewall Serial Numbers' (1234567890, 0987654321), and 'Validate Server' (checkbox). A red rectangle highlights the 'Server Name', 'Server Base URL', 'Username', 'Password', 'Verify', 'Username Transformation', and 'Palo Alto Firewall Serial Numbers' fields.

Server	Actions
Server Type:	Palo Alto Networks Panorama
Server Name:	10.X.X.X
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Authentication Method:	Basic
Username:	cppm-api
Password:
Verify:
Username Transformation:	Prefix NETBIOS name
Palo Alto Firewall Serial Numbers:	1234567890 0987654321
Validate Server:	<input type="checkbox"/> Enable to validate the server certificate

Summary of Shared Context Attributes

The following table details the contextual attributes ClearPass Policy Manager currently shares with the Palo Alto Networks firewalls.

Figure 13: *Attributes we can share with Palo Alto Networks endpoints*

Attribute	ClearPass 6.5.x	ClearPass 6.6.4+
UserID	✓	✓
Source IP	✓	✓
User Role	✗	✓ [4]
Device Type	✓	✓
Domain Name	✓ [1] [2]	✓ [1] [2]
Host Name	✓ [1]	✓ [1]
Per-Class Health/Posture	✓ [3]	✓ [3]

Note: [1] These attributes are passed from ClearPass to the Palo Alto Networks endpoint via HIP Objects. The Palo Alto Networks firewall MUST have a Global Protect License installed to be able to utilize the received HIP data and thus use it in its policy enforcement.



Note: [2] The Domain Name can be passed starting in ClearPass 6.3.0 with the UserID XML API or via the HIP Objects enabled by use of the GlobalProtect License.

Note: [3] To capture the Health/Posture context for an endpoint requires that OnGuard be installed on that endpoint. OnGuard is available for Windows/Mac OS X/Ubuntu. The ability to send this endpoint context was added in ClearPass 6.5.

Note: [4] Implicit sharing of TIPS roles with Palo Alto was initially added in ClearPass 6.6.4. In 6.6.5 the option to select if this data was shared with a Palo Alto along with sending the IP/Device mapping was exposed in the Context Server configuration.

After completing the steps in the previous sections, there are a couple of final steps to ensure that as users are authenticated with ClearPass, information is sent to update the Palo Alto Networks endpoint. This is performed using post_authentication Session Restrictions profiles discussed next.

Sending Updates to Palo Alto in 6.7 as part of Service Policy

In ClearPass 6.7, changes were made where one can select the Context Server Actions that can be posted to the Firewall using the Enforcement Profile. As a result, we have to change the post_authentication Enforcement Profile that will be used to post the data.



For ClearPass systems upgrading from 6.6, automatic migration of the enforcement profile type will be performed.

Adding this new enforcement profile is different from the previous ClearPass version. An example of the Enforcement Profile to send all the data is shown below. The Login and Logout actions that need to be sent can be selected.

Figure 14: Adding an enforcement-profile for Palo Alto in ClearPass 6.7

Configuration » Enforcement » Profiles » Edit Enforcement Profile - PAN-update-node (dot14)

Enforcement Profiles - PAN-update-node (dot14)

Summary Profile Attributes

Profile:

Name:	PAN-update-node (dot14)
Description:	PAN-update-node
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name	Value
1.	Session-Notify	Server Type	= Palo Alto Networks Firewall
2.	Session-Notify	Server IP	= 10.
3.	Session-Notify	Login Action	= Send Login Info
4.	Session-Notify	Logout Action	= Send Logout Info
5.	Session-Notify	Login Action	= Send HIP Report (Global Protect)
6.	Session-Notify	Login Action	= Register Device
7.	Session-Notify	Logout Action	= Unregister Device
8.	Session-Notify	Login Action	= Register Role
9.	Session-Notify	Logout Action	= Unregister Role

Starting in PAN-OS 8.0, the PAN XML APIs make it mandatory to post the value of User Identification Timeout along with the correlation data posted. This value is set to 45 mins by default on Palo Alto Firewall.

This is set to the same default value in ClearPass as well. The value can be configured under **Administration > Server Manager > Server Configuration > Service Parameters** as shown below.

Figure 15: Setting Palo Alto User Identification Timeout

Administration » Server Manager » Server Configuration - cppm161

Server Configuration - cppm161 (10.)

System Services Control **Service Parameters** System Monitoring Network FIPS

Select Service: Async network services

Parameter Name	Parameter Value	Default Value	Allowed Values
Ingress Event			
Batch Processing Interval	10 seconds	30	10-300
Command Control			
CoA Delay	2 seconds	2	0-15
Enable SNMP Bounce Action	FALSE	FALSE	
Post Auth			
Number of request processing threads	20 threads	20	20-100
Lazy handler polling frequency	5 minutes	5	3-10
Eager handler polling frequency	10 seconds	30	3-300
Connection Timeout	10 seconds	10	10-300
Palo Alto User Identification Timeout	45 minutes	45	1-3600

Sending Updates to Palo Alto in 6.6 as part of Service Policy

Starting ClearPass 6.5, changes were made to expand the Policy Manager Exchange Framework. This resulted in a new post_authentication profile type "**Session Notification Enforcement**" being created.



For ClearPass systems upgrading from 6.4 or earlier, automatic migration of the previous ClearPass enforcement profile (Session Restrictions Enforcement profiles) to the new enforcement profile type will be performed.

Adding this new enforcement profile for Palo Alto is slightly different from previous ClearPass versions. An example is shown below. Note that you have to specify two attributes of type **Session-Notify**, a **Server-Type** and a **Server IP**. If you have not previously defined the Palo Alto context server endpoint, then when trying to configure this step nothing will be available in the Value drop-downs.

Figure 16: Adding an enforcement-profile for Palo Alto in ClearPass 6.6

Configuration » Enforcement » Profiles » Edit Enforcement Profile - PAN-update-node

Enforcement Profiles - PAN-update-node

Summary	Profile	Attributes
Profile:		
Name:	PAN-update-node	
Description:	PAN-update-node	
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Session-Notify	Server Type	= Palo Alto Networks Firewall
2. Session-Notify	Server IP	= 10.2.100.10

If you don't see the IP address of a Palo Alto Networks endpoint, then it's likely a step was missed in one of the earlier sections, such as adding the endpoint under the Context Servers.



If multiple Palo Alto Networks Firewall / Panorama need to be configured then you **must** create **multiple** separate Enforcement Profiles, one per device. The option exists as shown below to add multiple Palo Alto Networks endpoints to a single enforcement profile, however this configuration is invalid.

Figure 17: Adding a Session-Check one endpoint per enforcement profile

Configuration » Enforcement » Profiles » Edit Enforcement Profile - pan-enforcement

Enforcement Profiles - pan-enforcement

Summary	Profile	Attributes
Attributes:		
Type	Name	Value
1. Session-Check	IP-Address-Change-Notify	= 10.2.100.10
2. Session-Check	IP-Address-Change-Notify	= 10.2.100.15

Adding an Enforcement Profile to an Enforcement Policy

Completing the configuration from this point is standard ClearPass workflow. An enforcement policy needs to be created with the enforcement action to call the enforcement-profile, or an existing policy needs to be modified to add this new profile. The example below is based upon an AD group membership match for the user.

Following this, add the enforcement policy to a service profile. In the below example, ClearPass will send an update when the authenticated user is a member of the AD Group **ns-tme**.

Figure 18: Trigger Palo Alto update on AD memberOf 'contains' rule

The screenshot shows the 'Configuration » Enforcement » Policies » Edit - update-pan-firewall' page. The 'Summary' tab is selected. The 'Enforcement' section shows the policy name 'update-pan-firewall', description, enforcement type 'RADIUS', and default profile '[Allow Access Profile]'. The 'Rules' section shows a single rule with the condition '(Authorization:win28k:memberOf CONTAINS ns-tme)' and the action 'PAN-update-node (dot10), [Allow Access Profile]'.

Enforcement Policies - update-pan-firewall	
Summary	
Enforcement:	
Name:	update-pan-firewall
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Allow Access Profile]
Rules:	
Rules Evaluation Algorithm:	First applicable
Conditions	Actions
1. (Authorization:win28k:memberOf CONTAINS ns-tme)	PAN-update-node (dot10), [Allow Access Profile]

Adding an Enforcement Policy to a Service

Next, an example of adding the Enforcement policy to a Service.

Figure 19: Palo Alto enforcement profile added to a service

The screenshot shows the 'Configuration » Services » Edit - PANW Service' page. The 'Enforcement' tab is selected. The 'Enforcement Policy' dropdown is set to 'update-pan-firewall'. The 'Enforcement Policy Details' section shows the description, default profile '[Allow Access Profile]', and rules evaluation algorithm 'first-applicable'. The 'Conditions' section shows a single rule with the condition '(Authorization:win28k:memberOf CONTAINS ns-tme)' and the 'Enforcement Profiles' section shows the profile 'PAN-update-node (dot10) [Allow Access Profile]'.

Services - PANW Service	
Summary	
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	update-pan-firewall Add new E
Enforcement Policy Details	
Description:	
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	first-applicable
Conditions	Enforcement Profiles
1. (Authorization:win28k:memberOf CONTAINS ns-tme)	PAN-update-node (dot10) [Allow Access Profile]

Sending Health/Posture status to Palo Alto from ClearPass

ClearPass can now send OnGuard Posture/Health context to Palo Alto. This was introduced in the ClearPass 6.5 release. To take advantage of this feature requires several items to be configured.



The configuration of OnGuard is beyond the scope of this document.

Adding this functionality ClearPass provides additional valuable health/posture context about the endpoint to Palo Alto to allow it to make more enhanced granular policy enforcement decisions.

The OnGuard client has the ability to report multiple individual attributes about a health/posture class (listed below), as an example for Antivirus: is the AV Product current/back level, is the AV engine current/back level, has the signature data-file been updated in the last X hours, when was the last scan performed, is real-time scanning enabled?

The complete list of classes checked are as follows; note that different checks can happen based upon the Client OS.

- Client Version Check
- File Check
- Processes Check
- Services Check
- Virtual machine Check
- Firewall Check
- AntiVirus Check
- AntiSpyWare Check
- Network Connection Check
- Hotfixes Check
- Installed Applications
- Disk Encryption Check

ClearPass then evaluates this information and sends it to the Palo Alto, at an individual class level with a posture token that can be one of the following as configured in OnGuard:

healthy / quarantined / checkup / transition / infected / unknown per class.

For the Palo Alto to take advantage of this context requires configuration both on ClearPass and within Palo Alto.

Configuring OnGuard on ClearPass

The configuration of the OnGuard client and Policy is beyond the scope of this document. In brief, use the standard ClearPass wizards to build the basic service policy definitions and then create your posture policies as required per platform: Windows/OSX/Linux.

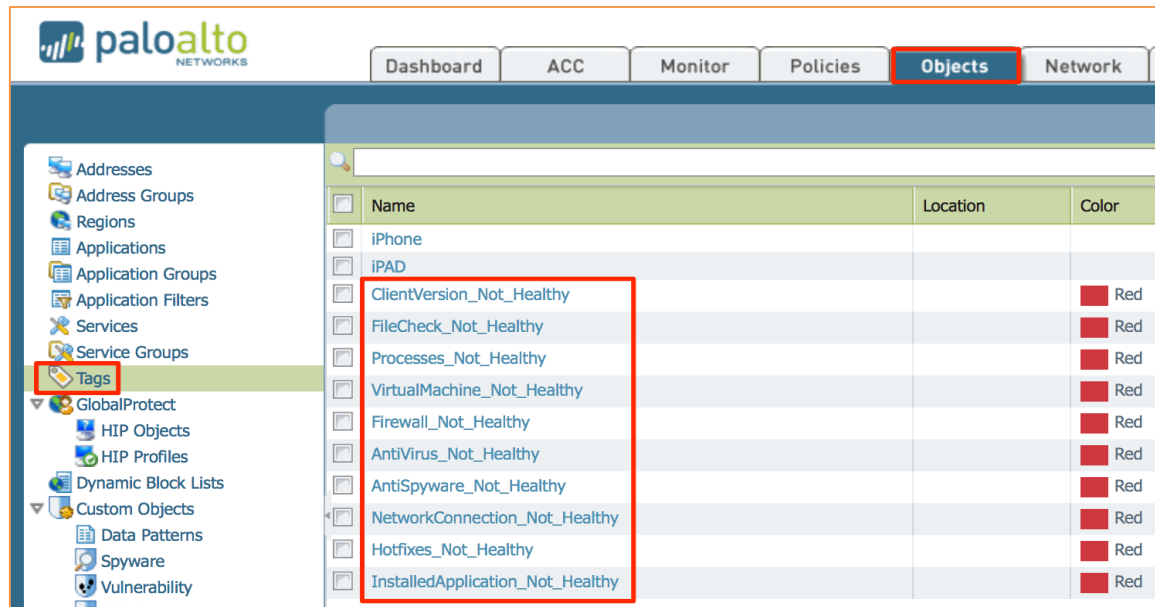
Configuring Palo Alto to use Health/Posture context

Within the Palo Alto firewall utilize TAGS and ADDRESS-GROUPS to match the data posture/health context being sent. These items need to be pre-created on the Palo Alto.

Configuring TAGS for Health/Posture

Under the **Device Tab->TAGS [Add]** create the following tags. The names and case have to be a 100% match to the list below, else the data sent by ClearPass will not match and the policy enforcement will fail.

Figure 20: Configuring TAGS on Palo Alto



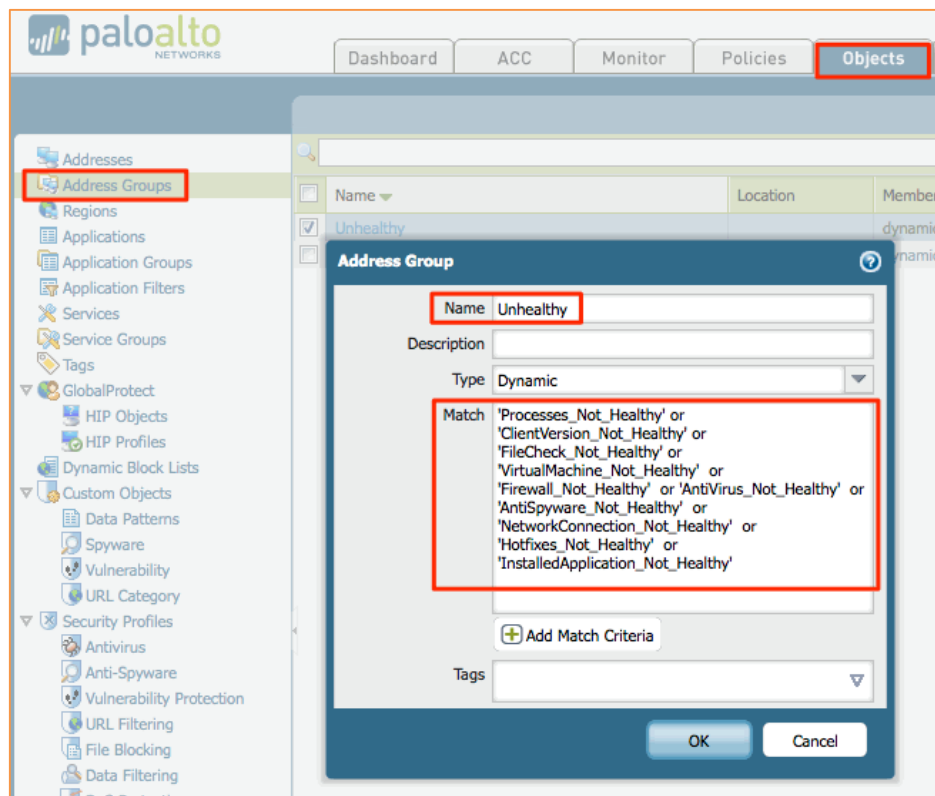
Below is a list that can be copied as a reference for the above TAGS when configuring them in the Palo Alto firewall.

Figure 21: Examples off "Not_Healthy" TAGS

```
ClientVersion_Not_Healthy
FileCheck_Not_Healthy
Processes_Not_Healthy
VirtualMachine_Not_Healthy
Firewall_Not_Healthy
AntiVirus_Not_Healthy
AntiSpyware_Not_Healthy
NetworkConnection_Not_Healthy
Hotfixes_Not_Healthy
InstalledApplication_Not_Healthy
```

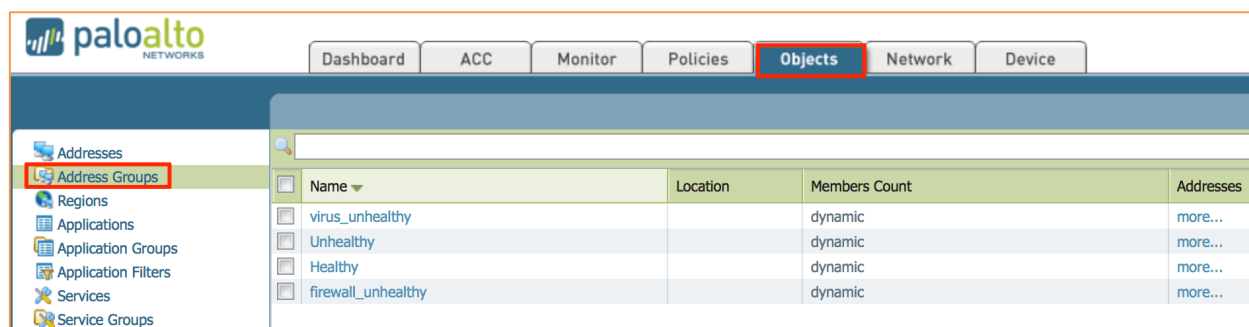
Create the TAGS with “**_Not_Healthy**” extensions. Use the **_Not_Healthy** TAG to capture and enforce when devices are outside the policy, not when they are compliant. After creating the TAGS assign them to an Address Group, as below. Address Groups are a collection of TAGS, but the Address-Group match can be built using Boolean AND / OR conditions to make for very granular and specific policy rules. See the Address Group example below that looks for ANYTHING un-healthy to trigger a match.

Figure 22: *Creating an Address-Group to match on ANYTHING unhealthy*



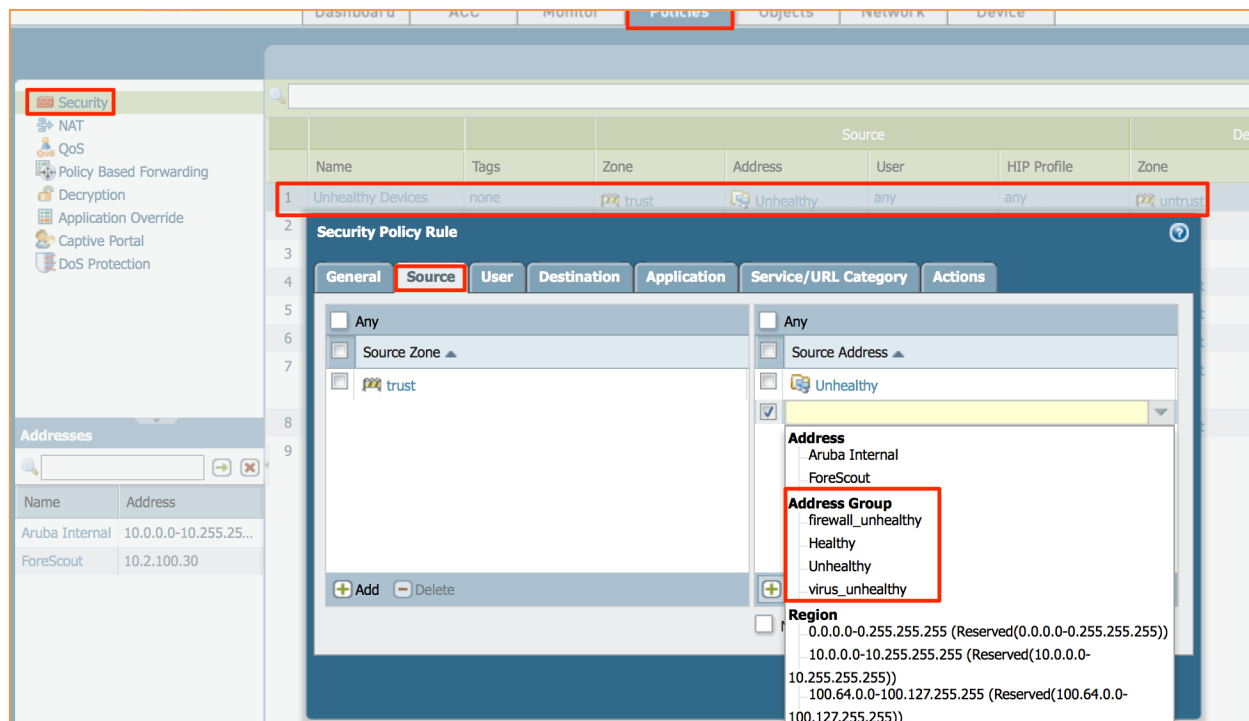
During testing, additional checks were defined as shown below; they are self-explanatory.

Figure 23: *Creating different Address-groups to check on individual failures*



Once the Address Groups have been created, multiple can exist according to how you need to enforce/restrict endpoints based upon their health/posture context. These can then be applied to policies within the Palo Alto firewall.

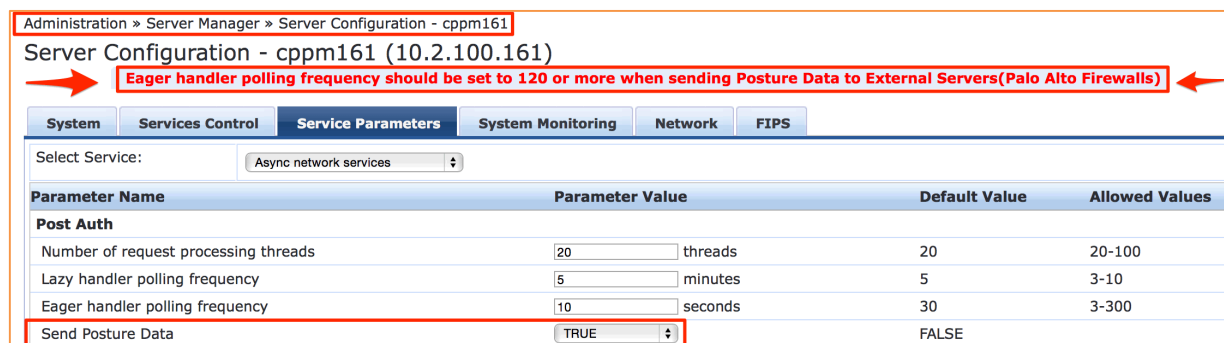
Figure 24: Adding an Address-group to a firewall policy



Setting the ClearPass Posture/Health Delay Timer in 6.6

When ClearPass is sending OnGuard posture/health status to a Palo Alto firewall, you must set the post_authentication eager timer to a MINIMUM of 120 seconds. This is required to allow the OnGuard client time to receive the policy analysis required for the endpoint and then trigger the local processing on the endpoint to analyze and post the results back to ClearPass. For this reason it is strongly recommended the eager-timer is set to a minimum of 120 seconds.

Figure 25: Setting Eager handler to 120 seconds when sending posture/health



The above option does not exist in 6.7. One can leverage the Context Server Action in the Enforcement Profile to send Posture data in 6.7 as shown below.

Figure 26: *Sending Posture Token using 6.7*

Configuration » Enforcement » Profiles » Edit Enforcement Profile - PAN-update-node (dot14)

Enforcement Profiles - PAN-update-node (dot14)

Post Authentication Eager handler polling frequency must be greater than 120 seconds for Register Posture action

Summary
Profile
Attributes

	Type	Name	Value		
1.	Session-Notify	Server Type	= Palo Alto Networks Firewall		
2.	Session-Notify	Server IP	= 10.2.100.14		
3.	Session-Notify	Login Action	= Send Login Info		
4.	Session-Notify	Logout Action	= Send Logout Info		
5.	Session-Notify	Login Action	= Send HIP Report (Global Protect)		
6.	Session-Notify	Login Action	= Register Device		
7.	Session-Notify	Logout Action	= Unregister Device		
8.	Session-Notify	Login Action	= Register Role		
9.	Session-Notify	Logout Action	= Unregister Role		
10.	Session-Notify <input type="text" value=""/>	Login Action <input type="text" value=""/>	= Register Posture <input type="text" value=""/>		
11.	Click to add...				



This is a tradeoff in that the user information will not be posted into the Palo Alto for quite a while. This may cause other access issues, e.g. if the firewall is waiting for user/IP mapping to allow access to resource this can be delayed.

Sending ClearPass Roles and using them in Palo Alto

Starting in ClearPass 6.6.4, the capability was added to send the Aruba Role calculations to Palo Alto such that this can be used within the Policy Enforcement on the firewall. Using roles simplifies the security interoperability between ClearPass and Palo Networks. As an example, ClearPass is able to understand the concept of a location, be that from a switch or from within the wireless network such as an Aruba AP Group. This location information cannot historically be shared directly with the firewall, but using roles the location can be used in a firewall policy to restrict access from or to a secure or restricted resource/application.

Sending roles to Palo Alto was detailed on Page 14 (note that the default is NOT to send roles). Once this has been enabled there is nothing else that is required on ClearPass.

ClearPass uses Palo Alto Dynamic Access Groups [DAGs] as the method to send the roles into the firewall policy engine. To utilize the DAGs in Palo Alto, the configuration must match the roles transmitted by ClearPass. As an example of the configuration, assume you want to match a user and assign a role of PLM.

Figure 27: Role Mapping example

Configuration » Services » Edit - Secure-Access with Cylance and MSFT-Intune {Remedy}

Services - Secure-Access v [redacted]

Summary Service Authentication Authorization **Roles** Enforcement

Role Mapping Policy: prod_mgmt Modify

Role Mapping Policy Details

Description:

Default Role: [Guest]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authorization:win28k-tme.ns-tme.com:memberOf CONTAINS PLM)	PLM
2. (Authorization:win28k-tme.ns-tme.com:memberOf CONTAINS TME)	TME
3. (Authorization:win28k-tme.ns-tme.com:memberOf CONTAINS SE)	root

Here in Access-Tracker you see the user **cam** authenticating and being assigned a role **PLM**.

Figure 28: User authentication with role mapping

Login Status:	ACCEPT
Session Identifier:	R0000108d-01-5907674e
Date and Time:	May 01, 2017 09:50:22 PDT
End-Host Identifier:	60672001E42A (Computer / Windows / Windows 8/10)
Username:	cam
Access Device IP/Port:	10.2.100.20:0 (10.2.100.20 / Aruba)
System Posture Status:	UNKNOWN (100)

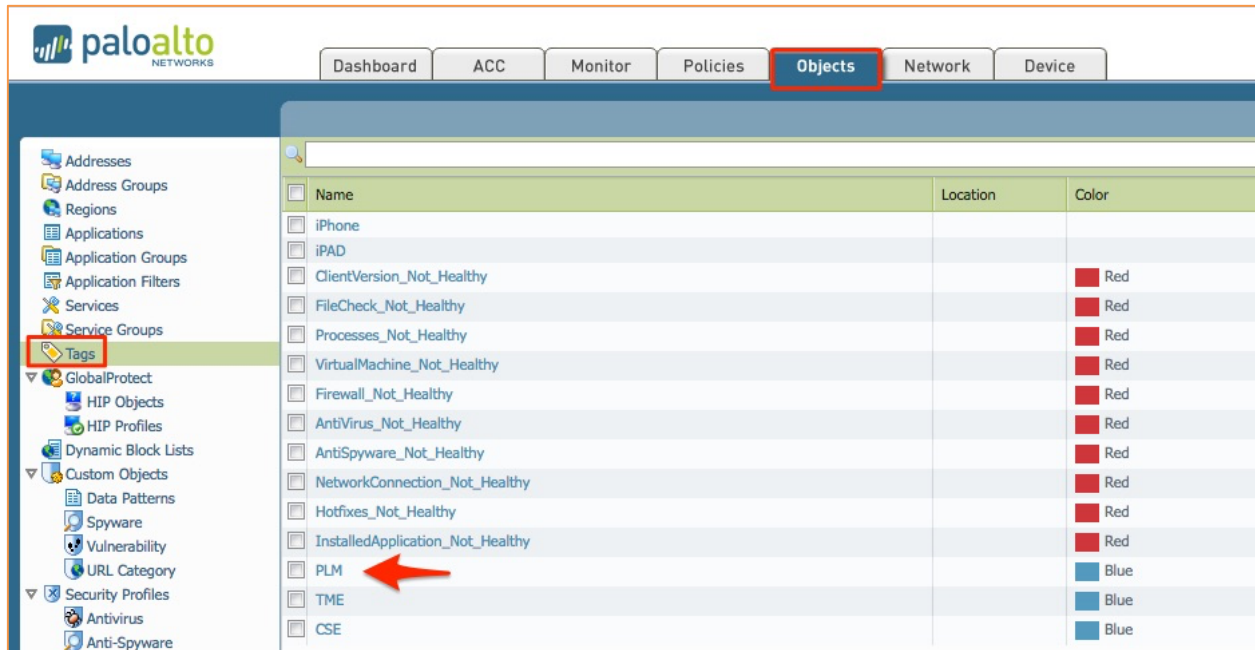
Policies Used -

Service:	Secure-Access with Cylance and MSFT-Intune {Remedy}
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:win28k-tme.ns-tme.com
Authorization Source:	win28k-tme.ns-tme.com, InTune-authZ-endpoint-check
Roles:	PLM, [User Authenticated]
Enforcement Profiles:	panw-user-device-update-cppm10, InTune-unmanaged-device-ArubaRole

Above you can see the user 'cam' was authenticated and assigned two roles, PLM and [User Authenticated].

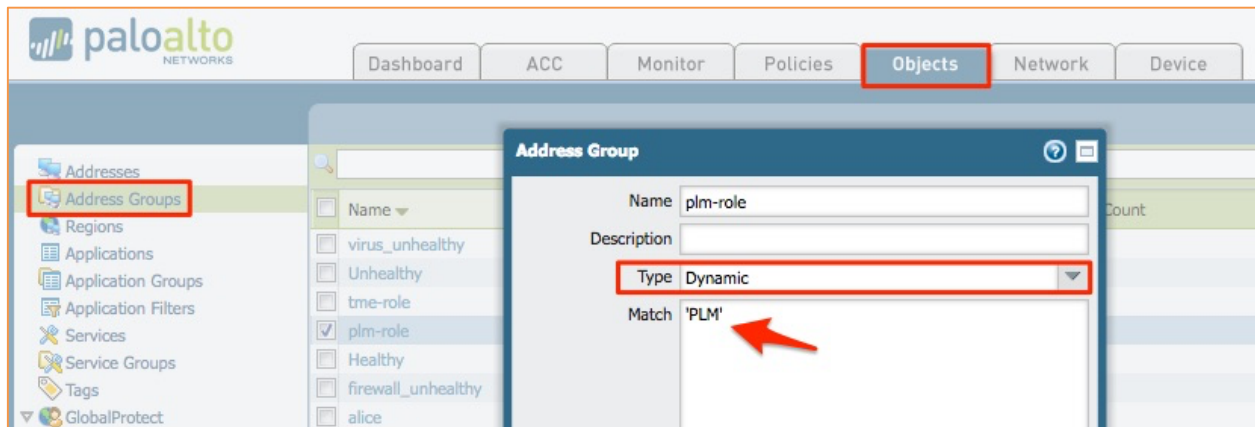
On the Palo Alto, you need to create TAGS to match the roles being sent from ClearPass. Note these are case specific.

Figure 29: Creating the TAGs



After building the TAGs, these need to be 'grouped' into one or more Address-Groups. The Address-Groups are then used to match in the firewall policies.

Figure 30: Adding TAGs to an Address-Group



The below firewall rule uses the Address-Group to match on the PLM-role and has an action of Drop.

Figure 31: Firewall rule with Address-Group match

	Name	Tags	Type	Zone	Source			Destination		Application	Service	Action	Profile	Options
					Address	User	HIP Profile	Zone	Address					
1	Unhealthy Devices	none	universal	trust	Unhealthy	any	any	untrust	any	any	application-d...	⛔	none	
2	drop-ipad	none	universal	any	any	any	HIP-iPad	any	any	twitter	application-d...	⛔	none	
3	test	none	universal	any	any	any	HIP-iPad	any	any	any	application-d...	⛔	none	
4	match-plm	none	universal	trust	plm-role	any	any	untrust	any	any	any	⛔	none	
5	match-tme	none	universal	trust	tme-role	any	any	untrust	any	any	any	✅	none	

Finally, below is the firewall rule dropping traffic based upon the PLM traffic.

Figure 32: Firewall dropping data against plm-role

(rule eq match-plm)														
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	
	05/01 11:27:39	drop	trust	untrust	10.2.100.215	cam	172.217.17.131	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:39	drop	trust	untrust	10.2.100.215	cam	172.217.17.131	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:39	drop	trust	untrust	10.2.100.215	cam	172.217.5.106	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:38	drop	trust	untrust	10.2.100.215	cam	172.217.5.106	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:36	drop	trust	untrust	10.2.100.215	cam	172.217.17.131	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:36	drop	trust	untrust	10.2.100.215	cam	172.217.17.131	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:30	drop	trust	untrust	10.2.100.215	cam	104.92.126.97	80	not-applicable	deny	match-plm	policy-deny	62	
	05/01 11:27:29	drop	trust	untrust	10.2.100.215	cam	104.92.126.97	80	not-applicable	deny	match-plm	policy-deny	62	
	05/01 11:27:27	drop	trust	untrust	10.2.100.215	cam	216.58.194.202	443	not-applicable	deny	match-plm	policy-deny	62	
	05/01 11:27:26	drop	trust	untrust	10.2.100.215	cam	216.58.194.202	443	not-applicable	deny	match-plm	policy-deny	62	
	05/01 11:27:26	drop	trust	untrust	10.2.100.215	cam	208.78.70.9	53	not-applicable	deny	match-plm	policy-deny	79	
	05/01 11:27:24	drop	trust	untrust	10.2.100.215	cam	52.72.89.177	443	not-applicable	deny	match-plm	policy-deny	66	
	05/01 11:27:24	drop	trust	untrust	10.2.100.215	cam	172.217.17.99	443	not-applicable	deny	match-plm	policy-deny	62	
	05/01 11:27:24	drop	trust	untrust	10.2.100.215	cam	172.217.17.99	443	not-applicable	deny	match-plm	policy-deny	62	
	05/01 11:27:24	drop	trust	untrust	10.2.100.215	cam	104.92.126.97	80	not-applicable	deny	match-plm	policy-deny	66	

Configuring Palo Alto Networks Next-Generation Firewall

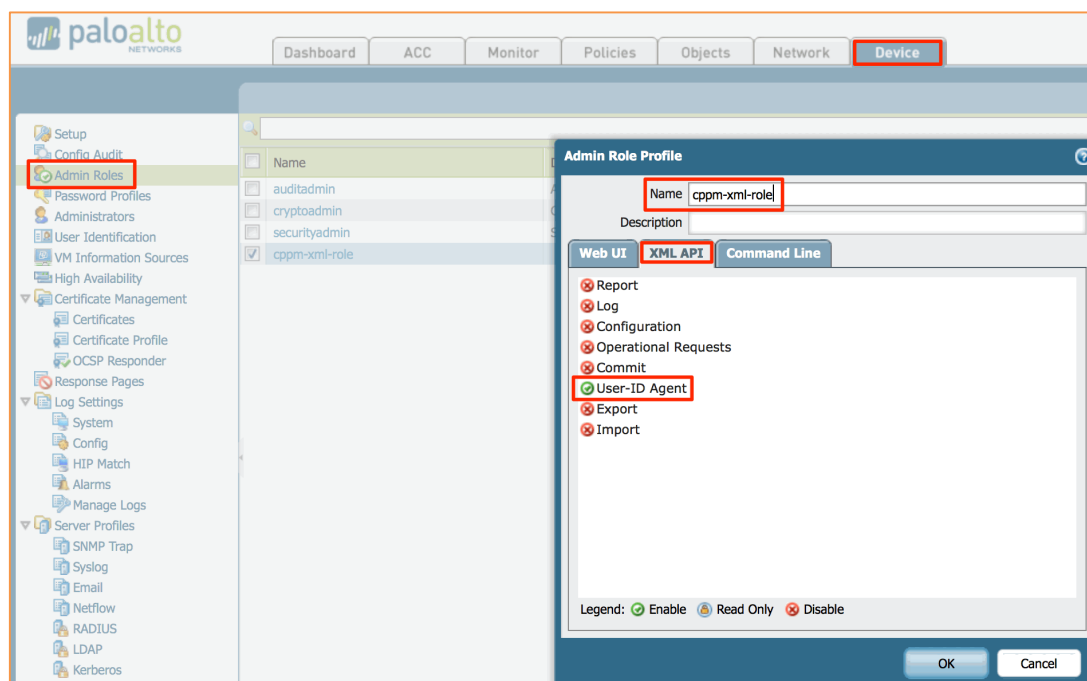
Multiple steps need to be completed to take advantage of the integration and many use cases exist in the scope of this integration in how to utilize the context sent by ClearPass to manage and control a user's and a device's access. Below is the documentation for how to configure a Palo Alto to allow ClearPass to send data and then for the Palo Alto Firewall to be able to use this data/context to make enforcement decisions.

Configuring ClearPass to communicate with Palo Alto using the UserID API

For ClearPass to send data to a Palo Alto, you should create a dedicated account within the Palo Alto Networks firewall/Panorama system. It's possible to use the built-in **admin** account, however this is not recommended. Create a new account that will be used solely for the purpose of ClearPass communication. Create a role-based account; this account can be limited to **only** communicating with the Palo Alto Networks firewall via the XML API.

Under the **Device** tab and **Admin Roles** create an admin-role as below. Ensure that you disable all the options on the Web UI Tab and the XML API **except** the **User-ID Agent** as shown below.

Figure 33: Creating a restricted Admin-Role

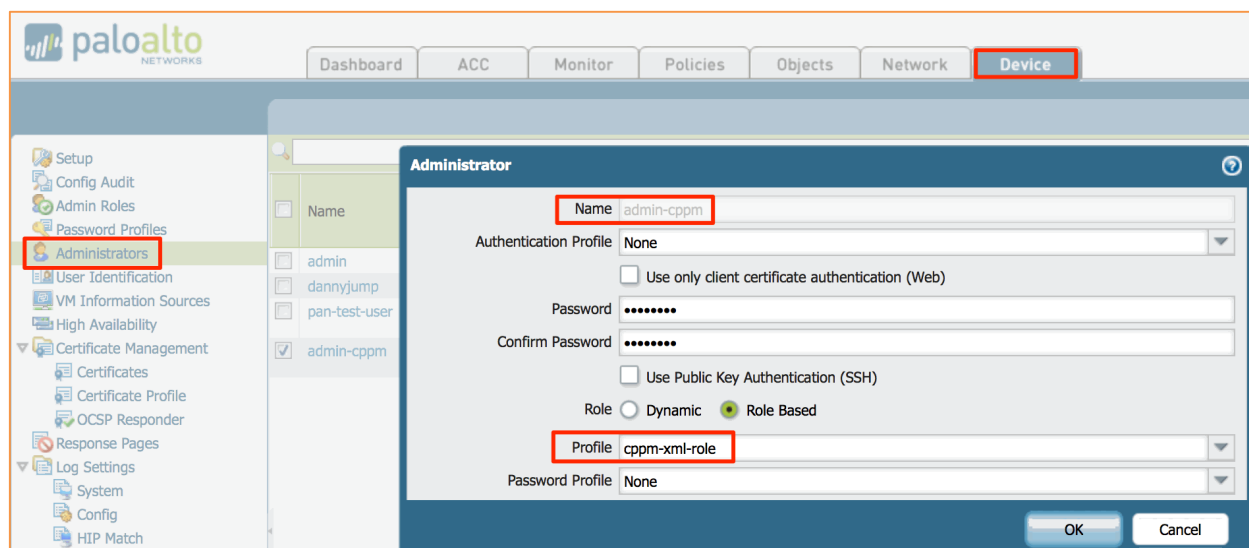


Next create the actual Admin userid. This will be used when defining the Palo Alto endpoint on ClearPass in the Context-Server definition. Again, under the **Device** tab but this time under **Administrators** create an admin user.



The account name created here must match that configured in the endpoint context server on ClearPass when adding the Palo Alto Networks endpoints as a Context Server.

Figure 34: Adding a User to Palo Alto Networks Firewall



In this example, add an admin user account called **admin-cppm**. See how it references the profile **cppm-xml-role** created in the previous step. This profile is limited to the User-ID agent APIs.

Configuring a Policy on Palo Alto to use the ClearPass context data – generic info....

In PAN-OS 6.0+, create TAGS and then combine these identifiers together under an Address Group. Then use Boolean logic like AND / OR to combine multiple tags in the Address Group. Then through the XMLAPI, 'attach' the client's IP address to the tags.

A Palo Alto Networks firewall can then enforce a policy utilizing the dynamic object's TAGs; in essence an object type that is not tied to a fixed IP address. ClearPass can complement a Palo Alto Networks firewall by supplying the dynamic object data and mapping an endpoint to a Tag.

Creating Device Profile Categories

Device categories need to be manually created in PAN-OS. Starting in ClearPass 6.3 the granularity of the endpoint information ClearPass is able to send to the Palo Alto Networks endpoint was enhanced. Prior to this release ClearPass only sent the Device Category, e.g. Computer or SmartDevice. Now, utilizing the power of the Profiler to classify the endpoint, ClearPass can also send the Device Family and Device Name to the Palo Alto Networks firewall.

A device profile is a hierarchical model consisting of 3 elements – **Device Category**, **Device Family**, and **Device Name** – derived by Profile from endpoint attributes.

Device Category - This is the broadest classification of a device. It denotes the type of the device. Examples include Computer, SmartDevice, Printer, Access Point, etc.

Device Family - This element classifies devices into a family and is organized based on the type of operating system or vendor. For example, when the category is Computer, ClearPass Policy Manager could show a **Device Family** of Windows, Linux, or Mac OS X, and when the Category is SmartDevice, ClearPass Policy Manager could show a **Device Family** of Apple or Android.

Device Name - Devices in a family are further organized based on more granular details, such as operating system version. For example, in a **Device Family** of Windows, ClearPass Policy Manager could show a **Device Name** of Windows 7 or Windows 2008 Server.

This hierarchical model provides a structured view of all endpoints accessing the network. As a reference, the list of Device Category, Family, or Name of a device that was authenticated in ClearPass can be viewed under **Administration > Dictionaries > Fingerprints**.

Figure 35: ClearPass Fingerprints

Administration » Dictionaries » Fingerprints

Device Fingerprints

Filter: Category contains [] Go Clear Filter Show 10 records

#	Category ▲	Family	Name
11.	Access Points	Buffalo	Buffalo AP
12.	Access Points	HP	HP ProCurve AP
13.	Access Points	Cisco	Cisco AP
14.	Access Points	Enterasys/Trapeze	Enterasys/Trapeze AP
15.	Barcode Scanner	Symbol	Symbol Scanner
16.	Barcode Scanner	Intermec	Intermec Scanner
17.	Computer	Windows	Windows 95
18.	Computer	Windows	Windows 2008

Configuring Palo Alto Networks PAN-OS 6.x - Tags and HIP Objects

There are two methods that can be used to match devices and users within Palo Alto firewall policies using context that is sent from ClearPass. The first method is Tags and the second is HIP.

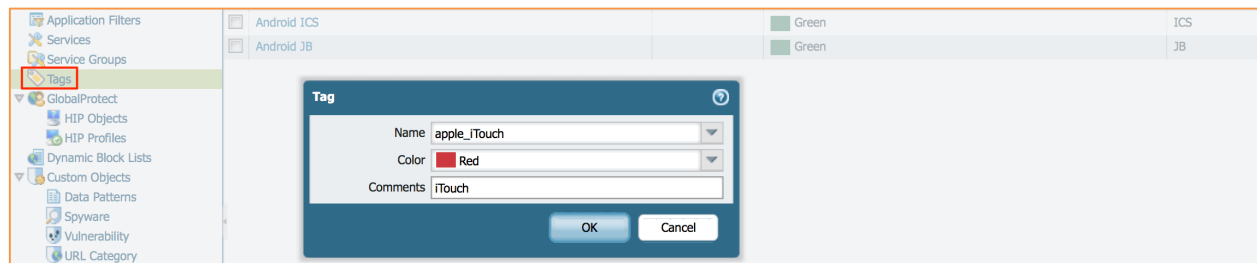
Tags can be manually (static) or automatically (dynamically) created. Use static tags as you know what they will be. Dynamically created tags are typically unknown. Once you decide on the Categories of devices required by ClearPass, create them on the Palo Alto firewall as Tags.



Profiling must be enabled or ClearPass is unable to send HIP level data.

To create the Tags select the **Object** Tab, then **Tags** and then on the bottom LHS click **+ Add** to add a new Tag. Below are a number of example Tags that have been created.

Figure 36: Adding a TAG under PAN-OS 6.x



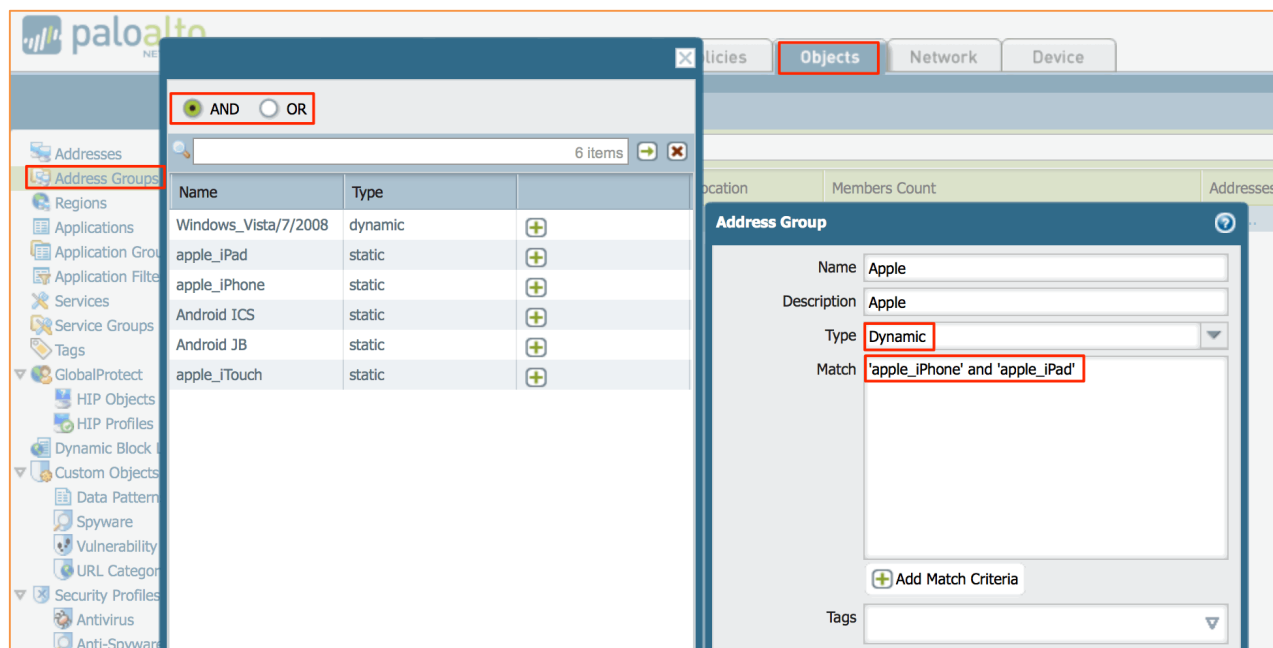
Group TAGS in Address Groups

After creating the individual Tags you have the option of grouping them. In this example, multiple Tags for different Apple types are created, then grouped under a generic Apple grouping in an Address Group.



Boolean logic can also be applied to the match criteria to enhance the selection of a match. When creating the Address group, the Address Group created must be type **'dynamic'** as shown below.

Figure 37: Grouping Tags into a Dynamic Address Group



Create the HIP Objects

Select the **Object** Tab, then under **GlobalProtect**, you will find the HIP Objects and HIP Profiles. On the bottom LHS click **"Add"**. This adds a new HIP Object. HIP Profiles are a collection of HIP Objects in a similar way that Address Groups are a collection of Tags. When creating a HIP Object, use **only** the options on the **General** Tab in the match, the below example shows using the Host OS.

Figure 38: Creating HIP Objects

The screenshot displays the 'HIP Object' configuration window. On the left, a sidebar lists various security features: General, Mobile Device, Patch Management, Firewall, Antivirus, Anti-Spyware, Disk Backup, Disk Encryption, Data Loss Prevention, and Custom Checks. The 'General' tab is currently active. The main configuration area is divided into sections. The 'Configuration' section has fields for 'Name' (set to 'iPad') and 'Description'. Below this, the 'Host Info' section is expanded and checked, showing dropdown menus for 'Domain' (None), 'OS' (Contains), 'Client Version' (None), and 'Host Name' (None). The 'Mobile Device Network Info' section shows a 'Network' dropdown set to 'None'. A small note at the bottom of the window states: 'This match criteria applies to mobile devices only.'

Other supported Attributes for HIP Object

Domain is used as in the context of the attribute **Domain\Username** when a user logs-in.

Client Version comes from the attribute **Name** in the ClearPass fingerprints DB, see below.

Host Name is in the context of the attribute profiled from the endpoint.

The below screenshot shows an example fingerprint database with a small subset of device-types that can be matched against for HIP context. The current shipping fingerprint database includes over 400 fingerprints. These are periodically updated through a bi-weekly fingerprint update. These updates are automatically pushed to all Internet-connected ClearPass nodes with an active subscription license. Customers are actively encouraged to send newly discovered fingerprints to Aruba by opening a TAC case.

Figure 39: ClearPass Fingerprints – Client Version

Administration » Dictionaries » Fingerprints

Device Fingerprints

Filter: Category contains

#	Category ▲	Family	Name
21.	Computer	Linux	Chrome OS
22.	Computer	Linux	FortiOS
23.	Computer	Windows	Windows XP
24.	Computer	Solaris	Solaris
25.	Computer	Linux	SUSE
26.	Computer	Linux	Debian/Ubuntu/Knoppix
27.	Computer	Windows	Windows 95
28.	Computer	Linux	Fedora
29.	Computer	Windows	Windows 2008
30.	Computer	Apple Mac	Mac OS X
31.	Computer	Windows	Windows ME
32.	Computer	Windows	Windows

Using the above user/endpoint context, the Palo Alto Networks firewall can make more granular decisions on how traffic should be processed.

Figure 40: Utilizing Tags in a Firewall Rule

paloalto NETWORKS

Dashboard ACC Monitor **Policies** Objects Network Device

Security

Name	Tags	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action
1 Deny Apple	apple_iPad apple_iPhone apple_iTouch	any	any	any	any	any	Drop apple	any	application-d...	

Historically, traditional firewalls classify traffic based on port number and IP address. However, port number is no longer a meaningful way to classify traffic, because any application can use any port number. The Palo Alto Networks next-generation firewall classifies traffic by application, and enforces policy based on the context of business elements such as application, user, and content.

The following rule shows the use of device types rather than IP address as a source in the Trust zone, making an enforcement decision against the match of context type of the endpoint rather than on the MAC address or IP address.



This device-data would be shared by ClearPass Policy Manager.

Figure 41: Building a security policy using endpoint type

Name	Tag	Zone	Address	User	HIP Profile	Zone	Address
my-facebook	none	any	any	any	any	any	any
tcp-80	none						
skype-probe	none						
allwsksype	none						
denyskypetcp	none						
denyskypeudp	none						
denytcp	none						
allowfb	none						
Allow_WWW_Access	none						
Block_VoIP_Corporate	none						
Allow_FB_Android	none						
allow	none						

Security Policy Rule

General

Source

User

Destination

Application

Service/URL Category

Actions

Any

Source Zone ▲

trust

+ Add - Delete

Any

Source Address ▲

Network_Camera

SmartDevice

Game_Console

+ Add - Delete

Negate

PAN-OS 6.x DAG/TAG Limits

The following page is credited to Palo Alto, find it here

<https://www.paloaltonetworks.com/documentation/60/virtualization/virtualization/about-the-vm-series-firewall/use-dynamic-address-groups-in-policy.html>

Dynamic address groups allow you to create policy that automatically adapts to changes—adds, moves, or deletions of servers. It also enables the flexibility to apply different rules to the same server based on its role on the network or the different kinds of traffic it processes.

A dynamic address group uses Tags as a filtering criteria to determine its members. A tag is a string or attribute that the firewall uses to match on and determine its group members. Tags use logical and & or operators for defining the filtering criteria.

Tags can be defined statically on the firewall and/or registered (dynamically) to the firewall. All entities that have the tags and match the defined criteria become members of the dynamic group. The difference between static and dynamic tags is that static tags are part of the configuration on the firewall, and dynamic tags are part of the runtime configuration. This implies that a commit is not required to update dynamic tags; the tags must however be used in policy and the policy must be committed on the device.

The IP address and associated tags for an entity can be dynamically registered on the firewall using the XML API or the VM Monitoring Agent on the firewall; each registered IP address can have up to 32 tags. Within 60 seconds of the API call, the firewall registers the IP address and associated tags, and automatically updates the membership information for the dynamic address group(s). Because the members of a dynamic address group are automatically updated, using dynamic address groups in lieu of static address objects, allows you to adapt to changes in your environment without relying on a system administrator to make policy changes and committing them on the firewall.

Use the following table to verify the maximum number of IP addresses that can be registered for each model of firewall:

Figure 42: *Number of supported DAG's across Palo Alto Platforms*

Platform	Maximum number of dynamically registered IP addresses
PA-7050, PA-5060, VM-1000	100,000
PA-5050	50,000
PA-5020	25,000
PA-4000 Series, PA-3000 Series	5000
PA-2000 Series, PA-500, PA-200, VM-300, VM-200, VM-100	1000

Faultfinding Tips (PANOS cli cmds/ClearPass Logs)

There are several commands and log-files available within the Palo Alto Networks Firewall and ClearPass to assist an administrator in identifying communication and integration problems.

The first section covers some useful cli commands to assist in debugging the Palo Alto Networks environment specifically related to receiving data feeds from ClearPass.

UserID <-> IP Address Mapping

To look at the user's that are logged in and their IP address mapping, use the following command: **show user ip-user-mapping all**

Figure 43: Signed in User's to their IP Mapping

```
admin@PA-500> show user ip-user-mapping all
```

IP	Vsys	From	User	IdleTimeout(s)	MaxTimeout(s)
10.4.28.110	vsys1	XMLAPI	bob1	Never	Never
10.4.28.200	vsys1	XMLAPI	bob2	Never	Never
10.2.101.231	vsys1	Unknown	unknown	0	3
192.168.11.104	vsys1	XMLAPI	wgjtest	Never	Never
10.17.24.77	vsys1	Unknown	unknown	3	6
172.31.99.191	vsys1	XMLAPI	gjwang	Never	Never
Total: 6 users					

Use the command **show user ip-user-mapping ip [ip address]** to show additional information where user attributes are being used by Palo Alto policies.

Figure 44: Showing active Users relative to their IP Mapping and also policy matches

```
admin@PA-3020> show user ip-user-mapping ip 10.2.100.178
```

IP address: 10.2.100.178 (vsys1)
User: alice
From: XMLAPI
Idle Timeout: Never
Max. TTL: Never
Groups that the user belongs to (used in policy)
HIP profiles that user belong to (used in policy)
HIP profile(s): HIP-iPad



The value of **Idle Timeout** shown above will be **Never** for PAN-OS 7. Starting PAN-OS 8.0, this is set to 45 minutes by default as shown in "Figure 17".

Following is the output of the same command in a setup running PAN-OS 8 and ClearPass 6.7 and above.

Figure 45: Showing active Users relative to their IP Mapping and Idle Timeout

```
admin@PALO-VFW-8X> show user ip-user-mapping ip 10.2.100.207
```

IP address: 10.2.100.207 (vsys1)
User: abhatt
From: XMLAPI
Idle Timeout: 2636s
Max. TTL: 2636s
Group(s): abhatt(85729)

Dynamic Device (Tag) <-> IP Address Mapping

Use the following command: `debug user-id dump registered-ip all`

Figure 46: *Dynamic Object Category - IP Address Mapping*

```
admin@PA-500> debug user-id dump registered-ip all

Identifier                               Vsys  Address
-----
Apple_iOS_Device                        1    : 10.2.101.167
thisbetterwork                          1    : 10.1.200.127
                                         1234:5678:90ab:cdef:2234:2678:20ab:2def
abcd                                    1    : 10.1.200.127
                                         1234:5678:90ab:cdef:2234:2678:20ab:2def
Computer                               1    : 0.0.0.1
                                         0.0.0.10
                                         0.0.0.43
                                         0.0.0.67
                                         10.2.101.163
                                         10.4.28.109
                                         10.13.23.105
                                         10.15.214.178
Routers                                1    : 0.0.0.55
SmartDevice                             1    : 0.0.0.28
                                         10.4.28.110
HTC_Android                             1    : 10.2.101.161
dyn-obj                                 1    : 10.1.200.127
                                         1234:5678:90ab:cdef:2234:2678:20ab:2def

Total: 8 objects 19 IP entries
*: IP entries received from user-id agent

admin@PA-500>
```

UserID <-> ClearPass Roles

Use the following command: `debug user-id dump registered-ip all`

Figure 47: *Showing ClearPass Role to DAG mapping*

```
admin@PA-3020> show object registered-ip all

vsys: (null), ip: (null), tag: (null)
current download interval (sec): 60
new changes since last download: no
registered IP                               Tags
-----
10.2.100.202 #                               "bill"
                                              "Windows"
                                              "TME"
                                              "[User Authenticated]"

10.2.100.212 #                               "PLM"

Total: 2 registered addresses
*: received from user-id agent #: persistent
```

UserID <-> Showing all Dynamic DAGs

To show the pre-configured DAG groups and their use in policy, use the following command: **show object dynamic-address-group all**

Figure 48: Showing configured DAGs and their assigned Policy

```
admin@PA-3020> show object dynamic-address-group all

Dynamic address groups in vsys vsys1:
-----
-----defined in vsys -----
  Unhealthy
    filter: 'Processes_Not_Healthy' or 'ClientVersion_Not_Healthy' or 'FileCheck_Not_Healthy' or 'VirtualMachine_Not_Healthy' or 'Firewall_Not_Healthy' or 'AntiVirus_Not_Healthy' or 'AntiSp
ware_Not_Healthy' or 'NetworkConnection_Not_Healthy' or 'Hotfixes_Not_Healthy' or 'InstalledApplication_Not_Healthy'
    members: total 0

  Healthy
    filter: 'VirtualMachine_Healthy' or 'Processes_Healthy'
    members: (not in use)

  virus_unhealthy
    filter: 'AntiVirus_Not_Healthy'
    members: (not in use)

  firewall_unhealthy
    filter: 'Firewall_Not_Healthy'
    members: (not in use)

  plm-role
    filter: 'PLM'
    members: total 1
             10.2.100.212 (R)

  tme-role
    filter: 'TME'
    members: total 1
             10.2.100.202 (R)

-----defined in shared-----
0: address object; R: registered ip; D: dynamic group; S: static group
```

Show HIP Reports

To display the HIP data related to an endpoint (assuming it is available) use the command: **debug user-id dump hip-report computer <c> ip <i> user <u>**. Note you have to supply specific values for **computer**, **IP**, and **user**.

Figure 49: HIP Report for a user

```
admin@PA-3020> debug user-id dump hip-report computer dannysipadmini user alice ip 10.2.100.178

<?xml version="1.0" encoding="UTF-8"?>
<hip-report>
  <md5-sum>9ca33e110b0da9704e36dbec3301699a</md5-sum>
  <user-name>alice</user-name>
  <host-name>dannysipadmini</host-name>
  <ip-address>10.2.100.178</ip-address>
  <generate-time>18/05/2015 09:54:45</generate-time>
  <categories>
    <entry name="host-info">
      <host-name>dannysipadmini</host-name>
      <os>Apple iPad</os>
      <os-vendor>Apple</os-vendor>
    </entry>
  </categories>
</hip-report>
```

Some additional Debugging Commands

Showing the HIP Database: debug user-id dump hip-profile-database

Figure 50: HIP Database in Debug

```
admin@PA-3020> debug user-id dump hip-profile-database
Total number of hipmask in database: 145
Total number of logout records in database: 258
Total size of hip reports: 1349KB used / 879616KB
Entry      : 1
User       : yahoo.com\bhprasad
Computer   : 10.4.28.110
IP         : 10.4.28.110
TTL        : Never
VSYs       : vsys1
MDS        : 4f64dd29d3d40b2c26b8a27f4c052e36
Mobile ID  :
NDM MDS    :
Last Checkin Time :
Jail Broken : 0
From XMLAPI

Entry      : 2
User       : aruba-apj2
Computer   : android-d3b79b6d93ce23df
IP         : 10.2.100.200
TTL        : Never
VSYs       : vsys1
MDS        : b94a5694236ec6d1d1c11fea8ec4756f
Mobile ID  :
NDM MDS    :
Last Checkin Time :
Jail Broken : 0
From XMLAPI

Entry      : 3
User       : ns-tme\carlos
Computer   : dannysipadmini
IP         : 10.2.100.165
TTL        : Never
VSYs       : vsys1
MDS        : 975d3b76f961dde86cfa953861b0c356
Mobile ID  :
NDM MDS    :
Last Checkin Time :
Jail Broken : 0
From XMLAPI
```

Show XMLAPI statistics

The below is a high-level view of the XMLAPI statistics. If there is zero activity here then you can assume some serious configuration or network problems exist between ClearPass and the Palo Alto Networks devices.

debug user-id dump xmlapi-stats

Figure 51: XMLAPI Stats

```
admin@PA-500> debug user-id dump xmlapi-stats

vsys: vsys1
num of input                : 98
num of user login           : 58
num of user logout          : 29
num of dynamic address object register : 8
num of dynamic address object unregister: 8
num of user group           : 0

admin@PA-500> 
```

Real-Time debug monitoring of the UserID process

A very effective way to monitor the XMLAPI process in real-time is using the following commands. This will set up an interactive (**like tail -f**) rolling update for the UserID process.

debug user-id on debug

debug user-id set userid all

tail follow yes mp-log useridd.log



Remember to disable the logging **debug user-id off**

The final debug command for the Palo Alto Networks Firewall shows all of the UserID Manager Data. This shows all users that have been registered through the XMLAPI process.

debug user-id dump idmgr type user all

Figure 52: List of ALL users registered through ID Manager

```
admin@PA-3020> debug user-id dump idmgr type user all
```

ID	Name
1	ns-tme\carlos
2	carlos
3	davidh
4	alice
5	ns-tme\cam
6	ns-tme\danny
7	ns-tme\bob
8	ns-tme\djump
9	djump
10	ns-tme\alice
11	ns-tme\verytemp
12	ns-tme\john
13	john
14	ns-tme\jack
15	danny
16	socialwifilogin\bob@socialwifilogin.net
17	socialwifilogin\bob
18	socialwifilogin\cam
19	rfiler
20	cam
21	socialwifilogin.net\bob
22	aruba-apj
23	bob

Check ClearPass Logs files

ClearPass collects multiple log files that can assist the administrator in debugging ClearPass to Palo Alto Networks integration problems. The most useful of these logs is the **postauthctrl.log** file. The process that triggers sending data via the XMLAPI is performed by the post_authentication daemon which updates this log file. Checking this log file can provide a valuable insight into the workings of this process on the ClearPass side and possible issues related to the communication with Palo Alto Networks endpoint.

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

Under **Administration -> Server Manager -> Server Configuration**, select your system if you have a cluster then click '**Collect Logs**'.

Once this process has completed, download this tar file and open with an appropriate application. For MacOS, **finder** will allow you to extract the file to a folder for analysis with the built-in Archive Utility. For Microsoft Windows multiple applications exist, but a really good utility is **7-Zip** <http://www.7-zip.org>.



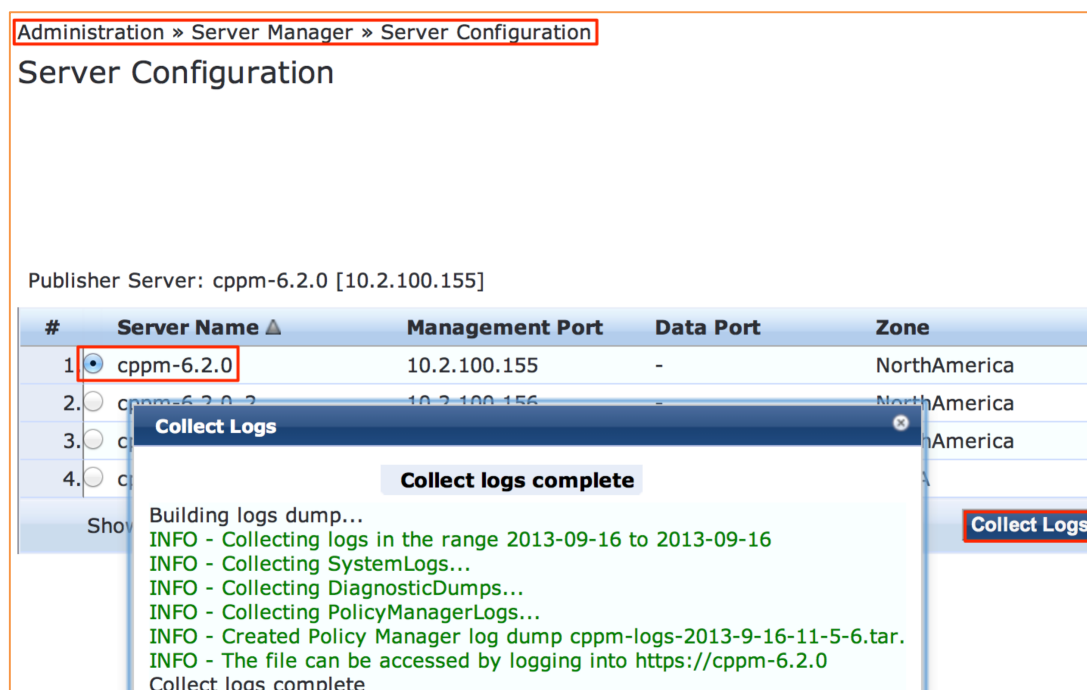
You only need to collect as highlighted below '**Logs from all Policy Manager services**' to obtain the postauthctrl.log file.

This will save significantly on the log collection process and the corresponding download file is much smaller. If you are not able to analyze an issue and you engage Aruba TAC, it is likely they will want System logs in addition to the Policy Manager services logs.

Figure 53: Collecting ClearPass Logs – limited data, but includes postauthctrl.log

The screenshot shows the 'Server Configuration' page in the ClearPass web interface. A 'Collect Logs' dialog box is open. The breadcrumb path 'Administration » Server Manager » Server Configuration' is at the top. The dialog box has a title bar 'Collect Logs' and a close button. It contains an 'Output file name' field with a note that a '.tar.gz' extension will be added. Below this is a section 'Collect the following logs' with four checkboxes: 'System logs' (unchecked), 'Logs from all Policy Manager services' (checked and highlighted with a red box), 'Capture network packets Duration of dump: 60 secs.' (unchecked), and 'Diagnostic dumps from Policy Manager services' (unchecked). There is also an option to 'Back up CPPM configuration data' (unchecked). Below this section is a 'Specify date range' section with a 'For number of days until today' field set to '1', and fields for 'Start date in yyyy-mm-dd format' and 'End date in yyyy-mm-dd format'. At the bottom of the dialog are 'Start' and 'Cancel' buttons. On the left side of the main page, there is a table with columns '#', 'Server', and 'Publisher Server'. The first row shows '1.' and 'CPPM63'. On the right side, there is a 'Profile' section with 'Enabled' and a 'Collect Logs' button.

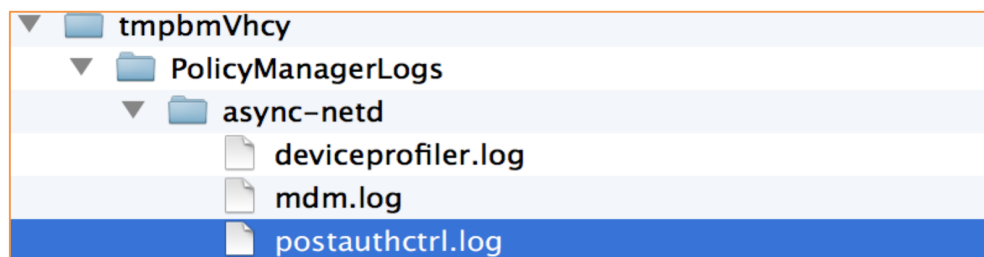
Figure 54: Collection of ClearPass Logs complete



After you have opened the archive, the **postauthctrl.log** file can be found in the following path:

PolicyManagerLogs/async-netd/postauthctrl*.log

Figure 55: Where to locate postauthctrl.log



Once you have located the postauthctrl.log file, there are certain entries you will want to look for; several examples are shown below. These provide an insight into the XMLAPI communication between ClearPass and the Palo Alto Networks Firewall. Once a user has associated and been authenticated, if the service match that authenticates the user has a post_authentication Palo Alto Networks trigger then you should be able to match that session to an entry in this log file.

Below are five **example** messages sent from ClearPass to a Palo Alto Network endpoint. You would expect to find these or very similar ones within the postauthctrl file. The last one shown is specific for HIP Objects.

Sending login UserID + Source IP@, as user logs in

```
<uid-message>

  <version>1.0</version>

  <type>update</type>

  <payload>

    <login>

      <entry name="dannyj" ip="10.4.28.110"/>

    </login>

  </payload>

</uid-message>
```

Adding IP@ to Category, as ClearPass profiles the IP@

```
<uid-message>

  <version>1.0</version>

  <type>update</type>

  <payload>

    <register>

      <entry identifier="SmartDevice" ip="10.4.28.110"/>

    </register>

  </payload>

</uid-message>
```

Sending logoff UserID + IP@, as user logouts

```
<uid-message>

  <version>1.0</version>

  <type>update</type>

  <payload>

    <logout>

      <entry name="dannyj" ip="10.4.28.110"/>

    </logout>

  </payload>

</uid-message>
```

```
</payload>
```

```
</uid-message>
```

Removing IP@ from Category as device logout

```
<uid-message>
```

```
<version>1.0</version>
```

```
<type>update</type>
```

```
<payload>
```

```
<unregister>
```

```
<entry identifier="SmartDevice" ip="10.4.28.110"/>
```

```
</unregister>
```

```
</payload>
```

```
</uid-message>
```

XML example of HIP Object

Sending username, domain-name, host-name, IP@ and client-version (OS-type).

```
<uid-message>
```

```
<version>1.0</version>
```

```
<type>update</type>
```

```
<payload>
```

```
<login>
```

```
<entry name="ClearPasseccert\certuser1" ip="192.168.100.1"><hip-report>
```

```
<md5-sum>aaea39d589a1f7540d137e56a6d60b31</md5-sum>
```

```
<user-name>certuser1</user-name>
```

```
<domain>ClearPasseccert</domain>
```

```
<host-name>toshi-driver-32</host-name>
```

```
<ip-address>192.168.100.1</ip-address>
```

```
<generate-time>06/03/2014 12:01:31</generate-time>
```

```
<categories><entry name="host-info">
```

```
<host-name>toshi-driver-32</host-name>
```

```
<domain>ClearPassECCERT</domain>  
  
<client-version>Windows 7</client-version>  
  
</entry></categories>  
  
</hip-report></entry>  
  
</login>  
  
</payload>  
  
</uid-message>
```

Conclusion

Aruba's ClearPass in conjunction with Palo Alto Networks can provide administrators with full context and visibility about the users and devices on the network to deliver end-to-end safe application enablement. We continue to evolve ClearPass to provide more contextual information about endpoints and users to Palo Alto Networks firewalls to allow them to make more advanced policy decisions with regard to the network and its users.