TECHNICAL NOTE
CLEARPASS PROFILING QUICK START GUIDE

REVISION HISTORY

<table>
<thead>
<tr>
<th>Revised By</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dennis Boas</td>
<td>Aug 2016</td>
<td>Version 1 – initial release</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

ClearPass Profiling Quick Start Guide ........................................................................................................... 1  
Introduction .................................................................................................................................................. 3  
Enable ClearPass Device Profiling ............................................................................................................... 3  
**Passive Collectors** .................................................................................................................................. 3  
  DHCP ...................................................................................................................................................... 3  
  HTTP User-Agent .................................................................................................................................... 4  
    Aruba Controller Configuration ............................................................................................................. 4  
    ClearPass IF-MAP Enable ..................................................................................................................... 5  
**Cisco Device Sensor** ............................................................................................................................... 5  
  Basic Configuration needed .................................................................................................................... 5  
  Enable ClearPass Interim Accounting ..................................................................................................... 5  
  Configure Cisco Switch ............................................................................................................................. 6  
**MAC OUI** ................................................................................................................................................ 7  
TCP Fingerprinting ..................................................................................................................................... 7  
**Active Collectors** .................................................................................................................................... 7  
**Subnet Scan** ........................................................................................................................................... 8  
  Set Scan Interval ..................................................................................................................................... 8  
  Configure ClearPass Profile Settings ...................................................................................................... 8  
**Example Profile Results** ....................................................................................................................... 13
Introduction

ClearPass uses a series of collectors to profile devices. These collectors receive information about each device and profile it for Device Category, Device OS family, Device Name, and Host Name. These device attributes can then be used to assign the correct authorization roles to the device. Configuring profiling is a two-step process: (1) the network infrastructure has to be configured to send device profiling information to ClearPass, and (2) ClearPass needs to be enabled to process the information. This paper presents a quick start guide for how to configure a basic ClearPass test environment. For more detailed information on ClearPass profiling refer to the ClearPass Profiling Tech Note on the Aruba support site. https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=7961

Enable ClearPass Device Profiling

Enable device profiling on at least one ClearPass node in each zone.

Passive Collectors

Passive Collectors monitor and analyze information either sent directly to ClearPass or received on a ClearPass span port.

DHCP

The DHCP collector analyzes DHCP DISCOVER and REQUEST messages and uses DHCP fingerprints to profile the sending device. The ClearPass DHCP collector is automatically enabled when Enable Profiling is selected. Network switches and controllers need to be configured to forward the DHCP packets to ClearPass. ClearPass will use the DHCP packets to profile the device, but ClearPass is not a DHCP server.

Example switch configurations.
• HPE-3800 switch running KA_16_010007
  DHCP Relay Configuration:
  - `vlan <id>`
  - `ip helper-address <ClearPass Server IP address>`
  - `dhcp-snooping vlan <id>`

• Cisco 3750 switch running IOS Version 12.2(55)SE4
  DHCP Relay Configuration:
  - `ip dhcp relay information trust-all`
  - `ip dhcp snooping vlan <vlan range>`
  - `interface vlan <ID>`
  - `ip address <ip and mask>`
  - `ip helper-address <ClearPass IP address>`

Note: If the ClearPass server has a span port configured it will also use DHCP packets received on that port for profiling. Switches or network taps can be configured to mirror traffic to the ClearPass span port.

HTTP User-Agent

In some cases, DHCP fingerprints alone cannot fully classify a device. A common example is the Apple family of smart devices; DHCP fingerprints cannot distinguish between an Apple iPad and an iPhone. In these scenarios, User-Agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.

User-Agent strings are collected from:

• ClearPass Guest
• ClearPass Onboard
• Aruba controller through IF-MAP interface

Guest and Onboard automatically collect User-Agent strings. The IF-MAP interface needs to be enabled on the ClearPass server and configured on the Aruba Controller.

Aruba Controller Configuration

Configure the IF-MAP interface on the Aruba controller:

```
(host) (config) #ifmap
(host) (config) #ifmap cppm
(host) (CPPM IF-MAP Profile) #server host <host> port <port> username <username> passwd <passwd>
(host) (CPPM IF-MAP Profile) #enable
```
ClearPass IF-MAP Enable

Enable IF-MAP profiling on ClearPass by going to Administration > Server Manager > Server Configuration > Cluster-Wide Parameters

Cisco Device Sensor

The Device Sensor feature is used to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), DHCP and HTTP User-Agent info. All these attributes are sent to ClearPass using RADIUS accounting packets. Upon receiving the accounting data, the RADIUS server will post these inputs to profiler for analysis. This allows endpoints to be profiled without needing IP helper configurations or SPAN ports.

Basic Configuration needed:

- Enable ClearPass Interim Accounting packets update
- Accounting configuration on Cisco NAD
- Enable IOS sensor on Cisco NAD

Enable ClearPass Interim Accounting

Enable logging of RADIUS Accounting packets by going to Administration > Server Manager > Server Configuration > [SERVER] > Service Parameters > RADIUS Server
Configure Cisco Switch

Cisco switch Device Sensor configuration:

```bash
device-sensor filter-list dhcp list dhcp-list
option name host-name [Supported Value 1 : dhcp option 12]
option name parameter-request-list [Supported Value 2 : dhcp option 55]
option name class-identifier [Supported Value 3 : dhcp option 60]

device-sensor accounting
device-sensor notify all-changes

device-sensor filter-list lldp list lldp-list
tlv name system-description [Supported Value 1 : TLV 0006 - lldp_sys_description]

device-sensor filter-list cdp list cdp-list
tlv name version-type [Supported Value 1:TLV0005 - cdp_sys_description]
tlv name platform-type [Supported Value 2:TLV0006 - cdp_cache_platform]

device-sensor filter-spec dhcp include list dhcp-list
device-sensor filter-spec lldp include list lldp-list
device-sensor filter-spec cdp include list cdp-list

Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end

Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```
For additional details refer to the Cisco Device Sensor Configuration Guide.


**MAC OUI**

A connecting device’s MAC OUI is automatically collected and can be useful for classifying endpoints. An example is Android devices, where DHCP fingerprints can only classify a device as a generic Android device, but cannot provide more detail about the vendor. Combining the DHCP information with the MAC OUI, the profiler can classify a device as HTC Android, Samsung Android, Motorola Android, etc. The MAC OUI is also useful to profile devices such as printers which may be configured with static IP addresses.

**TCP Fingerprinting**

When enabled, ClearPass will analyze the SYN, SYN-ACK handshakes using the open source TCP fingerprint databases pf0.fp and pf0fa.fp (SYN, and SYN-ACK respectively). Looking at the SYN packet allows ClearPass to determine which device (client) is connecting. Looking at the SYN-ACK allows ClearPass to derive what the actual server (target) is. TCP Traffic must be mirrored by network switches and controllers to the SPAN port on the ClearPass server.

To enable this feature on a 500 or 5K appliance, the Data Port must not be in use. On a 25K appliance, one of the other spare interfaces can be used. Within a VM environment, if the DATA Port is being used then the ability to use TCP Fingerprinting is not an option.

**Active Collectors**

Active collectors use protocols like SNMP, SSH and WMI to collect device attributes for use in profiling. Active collection is especially useful for discovering and profiling statically addressed devices.
Subnet Scan

ClearPass uses subnet scans to discover and profile devices with statically assigned IP addresses. Scans are automatically run every day or can be run on demand.

For each scanned address ClearPass will:

- If port 22 is open, attempt to use SSH to login and gather additional data
- If port 135 is open, attempt to use WMI to login and gather additional data
- If port 161 is open, attempt to query SNMP information
- If port 135 and 3389 is open, assume that the endpoint is Windows-based

Set Scan Interval

By default subnet scans are run once a day but the interval is configurable by going to Administration > Server Manager > Server Configuration > Cluster-Wide Parameters

Configure ClearPass Profile Settings

To configure Subnet scans, you must configure Profile Settings in Configuration > Profile Settings:

- Define the subnets to scan
- Add SNMP credentials
- Add SSH credentials
- Add WMI Domain credentials
Configure Subnets
Select the Policy Manager Zone and add the subnet or subnets for scanning. Subnets are added as a comma separated list. Note: do not end the line with a carriage return. To scan a single host use the /32 mask.

Configure SNMP Credentials
On the SNMP Configuration tab, click Add SNMP Configuration. You can add as many IP subnets or IP addresses as needed. Each can have its own set of credentials. In this example, we have configured two subnets with different SNMP credentials.
It is also possible to configure multiple sets of credentials for the same subnet as shown below.
Configure SSH Credentials

SSH credentials are configured per subnet or with multiple sets of credentials per subnet. Go the SSH Configuration tab and click Add Configuration.
Configure WMI Credentials

To add WMI credentials, go to the WMI Configuration tab and click Add Configuration. WMI credentials are used to sign into Windows Domain-joined machines and probe for additional profile information. Multiple credentials can be configured for each subnet and Domain.
Initiate On Demand Scan

Configure an on-demand subnet scan by clicking the On-Demand Subnet Scan link. Enter a comma-separated list of subnets and click Submit.

Example Profile Results

In this example the host IP is dynamically assigned so DHCP fingerprinting can be used. In addition, the profiler found port 3389 open. Port 3389 is used by Windows Remote Desktop.
This example shows a server with a statically assigned IP address. This means that DHCP fingerprinting is not an option. The server does support SNMP so the SNMP System Description is used to profile the server. **Note that the Server Name is also shown but is not used in the standard fingerprint. Device name could be used in a user-defined custom fingerprint.**

This switch is statically addressed and since we don't see any SNMP attributes, either SNMP is not enabled or the more likely reason is that the SNMP credentials are not correct. The CLI credentials were accepted and the SSH device name provides the profiling information.
This RAP was profiled based on CDP, SNMP and DHCP attributes.