

---

TECHNICAL NOTE



# CLEARPASS ACTIVE PROFILING

## DEVICE DISCOVERY AND SUBNET SCANS

Revised By	Date	Changes
Dennis Boas	Oct 2016	Version 1a – updated for 6.6.2

## TABLE OF CONTENTS

Clearpass Active Profiling .....	1
Device Discovery and Subnet scans .....	1
Introduction .....	3
Device Discovery Techniques .....	3
Device Discovery .....	3
Subnet Scans .....	4
Configure Credentials .....	4
SNMP Configuration .....	4
SSH Configuration .....	5
WMI Configuration .....	6
NMAP Scan.....	6
NMAP Scan Configuration.....	7
Using NMAP scan results for Authorization.....	7
Configure Subnet Scan .....	9
On Demand Subnet Scan .....	10
Trigger Endpoint Scans .....	11
Configure Device Discovery .....	13
Configure Network Device.....	13
Add Seed Device .....	14
Discovered Devices .....	15
Discovered Endpoints .....	17
Importing Discovered Devices .....	18
Troubleshooting .....	20
Event Viewer .....	20
Log Configuration .....	20
Debug Web Page .....	21
Additional Resources .....	23

## Introduction

This technical note is intended to help field engineers, customers, and partners understand, configure and deploy ClearPass Device Discovery and ClearPass subnet scanning. These features are used to discover and profile network access devices and endpoints. A critical element of network security is discovering what devices are connecting to the network and making sure that they are given the correct level of network access. Once a new device is discovered it can be profiled and authorized access based on attributes such as Host Name, Device Category, Device OS Family and Device Name. For example, network cameras and printers require access to different network resources and are often assigned to different VLANs. After the printer or camera is profiled, ClearPass will authorize and enforce the correct level of access and assign the correct VLAN. Discovering and profiling devices with statically assigned addresses requires different techniques than those that are used with dynamically addressed devices. ClearPass provides a set of tools to automate the discovery and profiling of both dynamically and statically addressed devices.

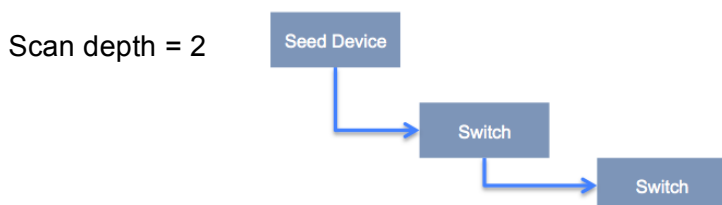
## Device Discovery Techniques

Device discovery techniques can be broadly categorized as either active or passive. Active techniques involve a series of focused probes directed at network access devices or more generalized subnet scans. Active techniques are primarily used for discovering and profiling statically addressed devices. Passive techniques involve monitoring message exchanges such as DHCP requests, TCP exchanges or analyzing the user agent information from a HTTP connect packet. Passive techniques work best with dynamically addressed devices. Agents such as OnGuard can also provide endpoint profiling information. This Tech Note focuses on active discovery techniques.

## Device Discovery

Device Discovery is a two-step process that identifies and profiles network access devices (switches and routers) and the endpoints (servers, computers, IoT devices, etc.) that are connected to them.

Step 1 uses SNMP to read information from the Bridge, ARP, LLDP and CDP MIBs on a network access seed device (switch or router). This information is used to discover neighboring network access devices. This process is repeated for each neighboring device until the scan depth limit is reached. Scan depth is configurable from one to five layers. The discovered network access devices can be imported into the ClearPass Network Device Table.



Step 2 uses the IP to MAC mapping information from the ARP tables of the network access devices to generate a scan of each of the connected endpoints. This scan looks for specific open ports and then use SNMP, SSH and WMI to profile the endpoint.

- If port 22 is open use SSH to login and collect profiling information
- If port 135 is open use WMI to login and collect profiling information
- If port 161 is open use SNMP to collect profiling information
- If port 135 and port 3389 are both open assume the endpoint is Windows based

After the discovered endpoints are profiled, the Endpoints Table is updated with the new information.

## Subnet Scans

Instead of probing network access devices to discover connected endpoints, subnet scans probe all addresses in the selected subnets. When an endpoint is detected;

- If port 22 is open use SSH to login and collect profiling information
- If port 135 is open use WMI to login and collect profiling information
- If port 161 is open use SNMP to collect profiling information
- If port 135 and port 3389 are open assume the endpoint is Windows based

If the discovered endpoint has a statically assigned address it is profiled and the new information is added to the Endpoints Table.

## Configure Credentials

The SNMP, SSH and WMI credentials used by both Device Discovery and subnet scans are configured in **Configuration >> Profile Settings**.

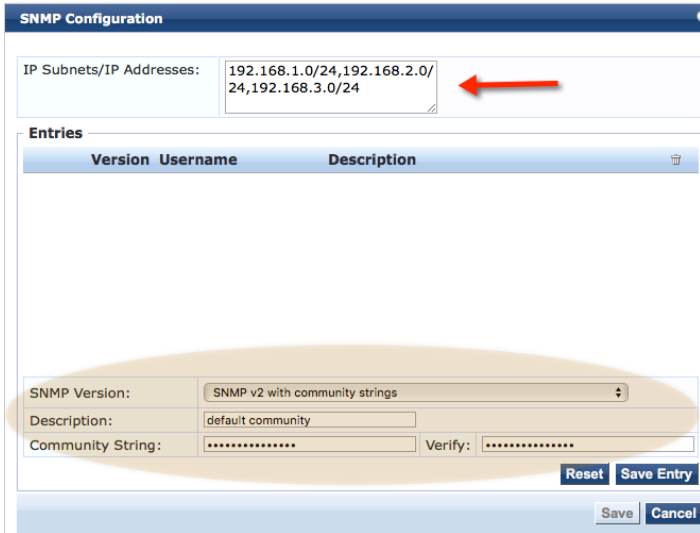
### Profile Settings

Subnet Scans	SNMP Configuration	SSH Configuration	WMI Configuration
Specify the IP subnets to be scanned for discovering hosts and their capabilities -			
Policy Manager Zone		IP Subnet to Scan	
1. Click to add...			

The first step in configuring Device Discovery and subnet scans is to enter the access credentials in the configuration tabs

## SNMP Configuration

Enter the subnets to be used for Device Discovery or subnet scans in a comma separated list. Do not end the list with a carriage return. Then add the SNMP credentials that should be used for the subnets.



**SNMP Configuration**

IP Subnets/IP Addresses: 192.168.1.0/24,192.168.2.0/24,192.168.3.0/24

**Entries**

Version	Username	Description
---------	----------	-------------

SNMP Version: SNMP v2 with community strings

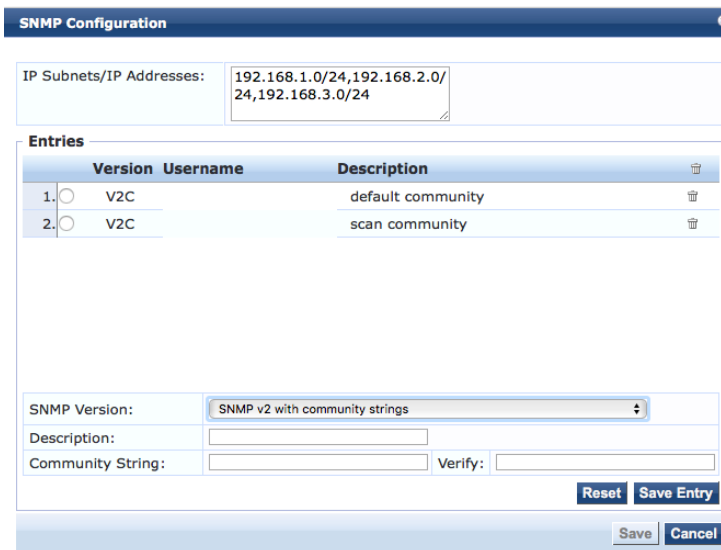
Description: default community

Community String: \*\*\*\*\* Verify: \*\*\*\*\*

Reset Save Entry

Save Cancel

You can add multiple sets of credentials. If Port 161 is open ClearPass will attempt to use each set of credentials to profile the device or endpoint.



**SNMP Configuration**

IP Subnets/IP Addresses: 192.168.1.0/24,192.168.2.0/24,192.168.3.0/24

**Entries**

Version	Username	Description
1. <input type="radio"/> V2C		default community
2. <input type="radio"/> V2C		scan community

SNMP Version: SNMP v2 with community strings

Description:

Community String: Verify:

Reset Save Entry

Save Cancel

## SSH Configuration

Under the SSH Configuration tab enter the subnets to be used. Then add the CLI login credentials and the Enable password. If port 22 is open, ClearPass will use these credentials to login and gather profiling information.

**Configuration**

IP Subnets/IP Addresses: 192.168.1.0/24,192.168.2.0/24,192.168.3.0/24

**Entries**

	Username	Description	
1.	<input type="radio"/> manager		
2.	<input type="radio"/> admin		

No Configuration present

Username:   
 Password:  Verify Password:   
 Enable Password: ☐ Enable Password Verify: ☐  
 Description:

## WMI Configuration

Under the WMI tab enter the subnets to be used. Then add the Active Directory domain credentials. Multiple domains can be configured. If port 135 is open, ClearPass will attempt to use the WMI protocol to gather profiling information.

**Configuration**

IP Subnets/IP Addresses: 192.168.1.0/24,192.168.2.0/24,192.168.3.0/24

**Entries**

	Username	Description	
1.	<input type="radio"/> selabs.com/administrator	Primary Domain	

Domain:   
 Username:   
 Password:  Verify Password:   
 Description:

## NMAP Scan

ClearPass release 6.6.2 added the option of using NMAP scans and signatures for device profiling. NMAP scans return host open ports and host services for scanned endpoints. This information is used for device profiling and is posted to the Endpoint (Fingerprints tab).

## Configuration >> Identity >> Endpoints

**Edit Endpoint**

Endpoint   Attributes   **Fingerprints**

**Endpoint Fingerprint Details**

Host Services:	17 -- tcpwrapped 21 -- ftp - Aruba router ftpd 22 -- ssh - OpenSSH Version: 5.8 80 -- http - Apache httpd 443 -- tcpwrapped 1723 -- pptp - Aruba Version: (Firmware: 2) 4343 -- http - Apache httpd 8080 -- http - Apache httpd 8081 -- http - Apache httpd 8082 -- http - Apache httpd 8088 -- http - Apache httpd
Host Open Ports:	17, 21, 22, 80, 443, 1723, 4343, 8080, 8081, 8082, 8088
SSH device name:	Aruba3600-US
SNMP Device Name:	Aruba3600
SNMP System Description:	ArubaOS (MODEL: Aruba3600-US), Version 6.4.3.6 (52927)

## NMAP Scan Configuration

NMAP scans are enabled in the Profiler Tab under **Administration >> Server Manager >> Server Configuration >> Cluster-Wide Parameters**.

**Cluster-Wide Parameters**

General   Cleanup Intervals   Notifications   Standby Publisher   Virtual IP   Mode   Database   **Profiler**

Parameter Name	Parameter Value	Default Value
Profile subnet scan interval	24 hours	24
Profiler Scan Ports	135,3389 TCP ports	135,3389
Process wired device information from IF-MAP interface	TRUE	FALSE
Enable Endpoint Port Scans using Nmap	TRUE	FALSE

**WARNING :** Setting this value to TRUE enables active scan of the host for open ports. This can be resource intensive. Also, 'Profiler Scan Ports' value is ignored when Nmap scan is enabled.

Restore Defaults   Save   Cancel

## Using NMAP scan results for Authorization

The NMAP information shown in the Fingerprints tab can be used for endpoint authorization. In this example we will use a MAC Auth service and create a simple role to determine the format of the NMAP information.

## Services - lab Device MAC Authentication

Summary	Service	Authentication	Roles	Enforcement
Role Mapping Policy: <span>lab test MANP fingerprint</span> <span>Modify</span>				
<b>Role Mapping Policy Details</b>				
Description:				
Default Role: AP				
Rules Evaluation Algorithm: first-applicable				
Conditions				Role
1. (Authorization:[Endpoints Repository]:Fingerprint EXISTS )				[Guest]

This role will match any existing fingerprint. After forcing a MAC authentication, we can examine the Authorization attributes in Access Tracker. This will show the format of the returned attributes.

Request Details	
Summary	Input
Username:	000b866ebe68
End-Host Identifier:	000B866EBE68 (Switch / Aruba / Aruba Controller)
Access Device IP/Port:	192.168.1.207:8214 (mas / Aruba)
<b>RADIUS Request</b>	
<b>Authorization Attributes</b>	
Authorization:[Endpoints Repository]:Fingerprint	{ "host": { "services": [ "17:tcpwrapped", "21:ftp - Aruba router ftpd", "22:ssh - OpenSSH Version: 5.8", "80:http - Apache httpd", "443:tcpwrapped", "1723:pptp - Aruba Version: (Firmware: 2)", "4343:http - Apache httpd", "8080:http - Apache httpd", "8081:http - Apache httpd", "8082:http - Apache httpd", "8088:http - Apache httpd", "ports": [ "17", "21", "22", "80", "443", "1723", "4343", "8080", "8081", "8082", "8088" ], "snmp": { "sys_descr": "ArubaOS (MODEL: Aruba3600-US), Version 6.4.3.6 (52927)", "name": "Aruba3600", "ssh": { "device_name": "Aruba3600-US", "tcp": { "device": "", "fp": "" } } } }
<b>Computed Attributes</b>	
◀ Showing 1 of 1-7 records ▶ <span>Change Status</span> <span>Show Configuration</span> <span>Export</span> <span>Show Logs</span> <span>Close</span>	

Using this information, we can create a role (LAB SSL 5.8) to authorize access if the endpoint is using SSH version 5.8



Role Mapping Policy:	NMAP Signatures	Modify
<b>Role Mapping Policy Details</b>		
Description:		
Default Role:	Restrict access	
Rules Evaluation Algorithm:	first-applicable	
<b>Conditions</b>	<b>Role</b>	
1. (Authorization:[Endpoints Repository]:Fingerprint CONTAINS 22:ssh - OpenSSH Version: 5.8)	Lab SSL 5.8	

To test our new role mapping, re-authenticate the endpoint. Access Tracker now shows the correct role being applied

<b>Summary</b>	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000005-02-57fd1f5c		
Date and Time:	Oct 11, 2016 13:20:28 EDT		
End-Host Identifier:	000B866EBE68 (Switch / Aruba / Aruba Controller)		
Username:	000b866ebe68		
Access Device IP/Port:	192.168.1.207:8214 (mas / Aruba)		
System Posture Status:	UNKNOWN (100)		
<b>Policies Used -</b>			
Service:	lab Device MAC Authentication		
Authentication Method:	MAC-AUTH		
Authentication Source:	Local:localhost		
Authorization Source:	[Endpoints Repository]		
Roles:	Lab SSL 5.8, [User Authenticated]		
Enforcement Profiles:	lab Device Bandwidth Limit, lab Device Do Expire, lab Device Expire Post Login, [Update Endpoint Known], lab Device Session Timeout		
Service Monitor Mode:	Disabled		

Note: NMAP scans are triggered by Device Discovery, periodic subnet scans and on-demand subnet scans.

## Configure Subnet Scan

If the Subnet Scan tab is configured, ClearPass will automatically scan the configured subnets once a day. To configure subnet scans, go to **Configuration > Profile Settings** and select a Policy Manager Zone for the scan.

<b>Subnet Scans</b>	SNMP Configuration	SSH Configuration	WMI Configuration
Specify the IP subnets to be scanned for discovering hosts and their capabilities -			
<b>Policy Manager Zone</b>	<b>IP Subnet to Scan</b>		
1. <input type="text"/>	<input type="text"/>		
2. default			
LA			
Boston			

After selecting the correct, add the subnets in a comma separated list. ClearPass will automatically scan the configured subnets once every 24 hours.

Subnet Scans | SNMP Configuration | SSH Configuration | WMI Configuration

Specify the IP subnets to be scanned for discovering hosts and their capabilities -

Policy Manager Zone	IP Subnet to Scan
1. Boston	192.168.1.0/24,192.168.2.0/24,192.168.3.0/24
2. Click to add...	

You can change the scan interval under **Administration >> Server Manager >> Server Configuration >> Cluster Wide Parameters**.

Cluster-Wide Parameters

General | Cleanup Intervals | Notifications | Standby Publisher | Virtual IP Configuration | Mode | Database

Parameter Name	Parameter Value	Default Value
Policy result cache timeout	5 minutes	5
Free disk space threshold value	30 %	30
Free memory threshold value	20 %	20
Profile subnet scan interval	24 hours	24
Endpoint Context Servers polling interval	60 minutes	60
Automatically check for available Software Updates	TRUE	TRUE
Login Banner Text		
Admin Session Idle Timeout	30 minutes	30
Performance Monitor Rendering Port	80	80
Multi Master Cache Durability	OFF	OFF
CLI Session Idle Timeout	360 minutes	360
Disable TLSv1.0 support	None	None
Profiler Scan Ports	135,3389 TCP ports	135,3389
Process wired device information from IF-MAP interface	TRUE	FALSE
Disable Change Password for TACACS	FALSE	FALSE

Restore Defaults | Save | Cancel

## On Demand Subnet Scan

On Demand Subnet Scans can be run as needed and are recommended after adding new devices to the network.

### Profile Settings

On-Demand Subnet Scan

Subnet Scans | SNMP Configuration | SSH Configuration | WMI Configuration

Specify the IP subnets to be scanned for discovering hosts and their capabilities -

Policy Manager Zone	IP Subnet to Scan
1. Boston	192.168.1.0/24,192.168.2.0/24,192.168.3.0/24
2. Click to add...	

Initiate On-Demand Subnet Scan

Specify the IP subnets to be scanned for discovering hosts and their capabilities now -

Subnets to scan

192.168.1.0/24

Submit Cancel

Select **On-Demand Subnet Scan**, then enter the subnets to scan and click **Submit**. For both On Demand and automatic scans the endpoint table will only be updated if Static IP is True.

EndPoint		Attributes	
MAC Address	000b866ebe68	IP Address	192.168.1.212
Description		Static IP	TRUE
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname	Aruba3600
MAC Vendor	Aruba Networks	Device Category	Switch
Added by	Policy Manager	Device OS Family	Aruba
Online Status	Not Available	Device Name	Aruba Controller
Connection Type		Added At	Aug 18, 2016 17:17:56 EDT
		Updated At	Aug 18, 2016 17:19:08 EDT
		Show Fingerprint	<input checked="" type="checkbox"/>
<b>Endpoint Fingerprint Details</b>			
SSH device name:	Aruba3600-US		
SNMP Device Name:	Aruba3600		
SNMP System Description:	ArubaOS (MODEL: Aruba3600-US), Version 6.4.3.6 (52927)		

A subnet scan added the above endpoint entry. Notice that Static IP is True and the Fingerprint shows that both SNMP and SSH were used to profile the device.

## Trigger Endpoint Scans

An SNMP or NMAP scan can be manually triggered from the endpoint table. This can be useful if ClearPass was not able to classify the endpoint. In the following example; Device Category, OS Family and Device Name are all unknown.

Edit Endpoint			
Edit Endpoint			
EndPoint		Attributes	
MAC Address	007f283780e2	IP Address	192.168.1.1
Description		Static IP	TRUE
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname	-
MAC Vendor	Actiontec Electronics, Inc	Device Category	Unknown
Added by	Policy Manager	Device OS Family	Unknown
Online Status	Not Available	Device Name	Unknown
Connection Type		Added At	Aug 18, 2016 23:19:01 EDT
		Updated At	Aug 20, 2016 00:20:32 EDT
		Show Fingerprint	<input checked="" type="checkbox"/>
<b>Endpoint Fingerprint Details</b>			
TCP Fingerprint:			
TCP Device Category:			
<div>Save</div> <div>Cancel</div>			

By selecting the table entry and clicking Trigger Server Action an NMAP or SNMP scan can be manually initiated

## Endpoints

[Add](#)  
[Import](#)  
[Export All](#)

Filter: MAC Address contains [ ] Go Clear Filter Show 10 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
11.	685b3586f585		Unknown	Unknown	Unknown	No
12.	34ab3736abea	jane-boass-ipad	SmartDevice	Apple	Unknown	Yes
13.	308d99336a40		Unknown	Unknown	Unknown	No
14.	247703e0d1a0		Unknown	Unknown	Unknown	No
15.	101f74266296	new-host-3	Printer	HP	Unknown	Yes
16.	00a0966a7874		Unknown	Unknown	Unknown	No
17.	007f283780e2		Unknown	Unknown	Unknown	No
18.	0024a05378d0		Unknown	Unknown	Unknown	No
19.	002180dc70d8		Unknown	Unknown	Unknown	No
20.	0019bbeebde2		Unknown	Unknown	Unknown	No

Showing 11-20 of 30 Authentication Records Trigger Server Action Update Fingerprint Export Delete

The NMAP scan below shows open ports, Network Applications and Device category. In this case NMAP's confidence is 100%. If this is correct, selecting Update will update the endpoint table

**Trigger Server Action**

Server Action has been successfully initiated

Server Action: Nmap Scan

Context Server: localhost

Server Type: Generic HTTP

Action Description: Perform Nmap Scan for selected endpoint

**Action Result**

Device Category: Linux 2.6.9 - 2.6.31(100%)

Network Apps: telnet, http, unknown, https, telnets

Open Ports: 23, 80, 234, 443, 992

Update Cancel

The endpoint entry now shows the correct Device Category, Device OS Family and Device Name. The fingerprint shows that NMAP profiled the endpoint.

**Edit Endpoint**

EndPoint Attributes

MAC Address	007f283780e2	IP Address	192.168.1.1
Description		Static IP	TRUE
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname	-
MAC Vendor	Actiontec Electronics, Inc	Device Category	Computer
Added by	Policy Manager	Device OS Family	Linux
Online Status	Not Available	Device Name	Linux Computer
Connection Type		Added At	Aug 18, 2016 23:19:01 EDT
		Updated At	Aug 20, 2016 01:11:06 EDT
		Show Fingerprint	<input checked="" type="checkbox"/>

**Endpoint Fingerprint Details**

TCP Fingerprint:

TCP Device Category:

Nmap Device Type: Linux 2.6.9 - 2.6.31

Save Cancel

The other type of scan that can be triggered is SNMP. Subnet scans only profile statically addressed endpoints. With triggered scans, SNMP can be used to gather additional profile information for dynamically addressed endpoints.

Trigger Server Action

Server Action has been successfully initiated

Server Action: SNMP Scan

Context Server: localhost

Server Type: Generic HTTP

Action Description: Perform SNMP Scan for selected endpoint

Action Result

System Name : HP-3800-48G-PoEP-4SFP+

System Description : HP J9574A 3800-48G-PoE+-4SFP+ Switch, revision KA.16.01.0007, ROM KA.15.10 (/ws/swbuildm/rel\_richmond\_qaoff/code/build/tam(swbuildm\_rel\_richmond\_qaoff\_rel\_richmond)) (Formerly ProCurve)

Start Action Cancel

Typically SNMP scans are most effective for network devices since they generally support SNMP.

You can only trigger one NMAP or SNMP scan at a time. If the scans do not show up in the pull down menu, make sure you don't have more than one endpoint entry selected.

## Configure Device Discovery

After the Profile Credentials are configured, the next step is to configure the network seed device. Multiple seed devices can be configured. In a geographically dispersed deployment, configure at least one seed device for each location. A core or distribution layer switch is a good choice for a seed device.

### Configure Network Device

Go to **Configuration >> Network >> Devices** and click on the **SNMP Read Settings** tab.

- Enable ClearPass to use SNMP to access this device
- Select SNMP version
- Configure access credentials (community string)
- Enable Force Read, causes all nodes in cluster to read information from this device
- Enable Read ARP Table Info to extract MAC to IP mappings

## Add Seed Device

In **Monitoring >> Profiler and Discovery >> Network Discovery**, click on **Start Network Discovery Scan** to add the seed devices.

Monitoring » Profiler and Discovery » Network Discovery  
Network Discovery



- Set scan depth from 1 to 5 layers
- Add IP address of Seed Device
- Enable Probe ARP Entries
- Start Discovery

After Discovery has started the progress bar will show the status as “In Progress”.

Filter: Seed Devices contains [ ] Go Clear Filter Show 10 records

#	Seed Devices	Server	Start Time	End Time	Endpoints	Devices	Status	Action
1.	192.168.1.207	CPPM_6_6_1	2016-08-19 22:40:03		13	2	IN PROGRESS	

Showing 1-1 of 1

In this example Discovery is complete and two devices and 13 endpoints have been discovered.

Filter: Seed Devices contains [ ] Go Clear Filter Show 10 records

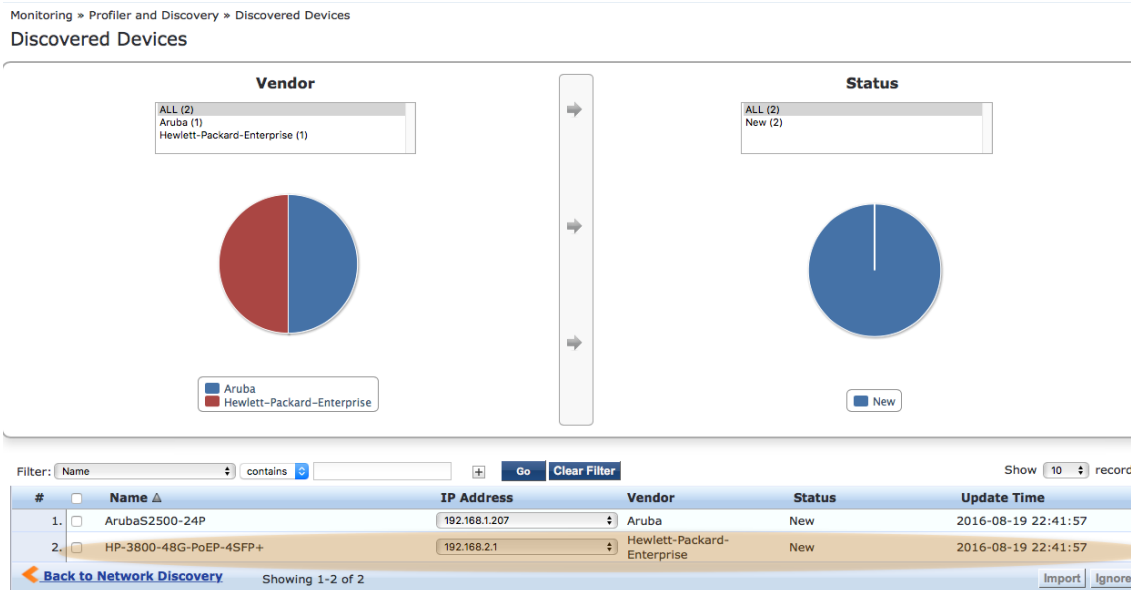
#	Seed Devices	Server	Start Time	End Time	Endpoints	Devices	Status	Action
1.	192.168.1.207	CPPM_6_6_1	2016-08-19 22:40:03	2016-08-19 22:42:11	13	2	COMPLETED	

Showing 1-1 of 1

Devices are defined as Network Access Devices (switches and routers), Endpoints are servers, computers, Printers, IoT devices, etc.

## Discovered Devices

The Discovered Devices page shows the results of the Device Discovery scan. In this example two switches were discovered. Clicking on the device opens the device details view.



The detail view reveals that port 5 of the HP-3800 is connected to the Aruba S2500 switch.

Network Device Details

Sys Name:	HP-3800-48G-PoEP-4SFP+
Vendor:	Hewlett-Packard-Enterprise
Sys Location:	
Sys Contact:	
Sys Description:	HP J9574A 3800-48G-PoE+-4SFP+ Switch, revision KA.16.01.0007, ROM KA.15.10 (/ws/swbuildm/rel_richmond_qaoff/code/build/tam(swbuildm_rel_richmond_qaoff_rel_richmond)) (Formerly ProCurve)
Status:	Imported
Update Time:	Fri Aug 19 2016 18:41:57 GMT-0400 (EDT)
IP Address:	192.168.2.1 192.168.1.209

Neighbor Device Details:-

#	IP Address	Name	Port	Device	Description
1.	192.168.1.207	ArubaS2500-24P	5	Switch	ArubaOS (MODEL: ArubaS2500-24P-US), Version 7.1.3....

Close

Examining the detailed view for the Aruba S2500 switch shows the connection back to the HP-3800 is via port 0 and that port 8 is connected to an address outside of the subnets configured in the SNMP Profile. For this reason, the profile information for 169.254.70.20 is incomplete and the device type is Unknown.

Network Device Details

Sys Name:	ArubaS2500-24P
Vendor:	Aruba
Sys Location:	
Sys Contact:	
Sys Description:	ArubaOS (MODEL: ArubaS2500-24P-US), Version 7.1.3.2 (34362)
Status:	New
Update Time:	Fri Aug 19 2016 18:41:57 GMT-0400 (EDT)
IP Address:	192.168.1.207

Neighbor Device Details:-

#	IP Address	Name	Port	Device	Description
1.	169.254.70.20	9c:1c:12:c2:8f:5c	gigabitethernet0/0/8	Unknown	ArubaOS (MODEL: 135), Version 6.4.2.6-4.1.1.11 (52...
2.	192.168.1.209	HP-3800-48G-PoEP-4SFP+	gigabitethernet0/0/0	Switch	HP J9574A 3800-48G-PoE+-4SFP+ Switch, revision KA....

Close

This unknown device is not listed as a discovered device since it's not part of the profiled subnets shown below.

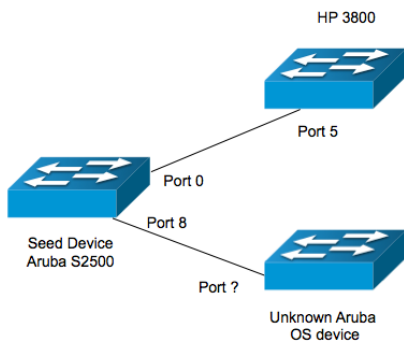


SNMP Configuration

IP Subnets/IP Addresses:

192.168.1.0/24,192.168.2.0/24,192.168.3.0/24

The network topology revealed by Device Discovery looks like this;



## Discovered Endpoints

Discovered endpoints are shown on the Monitoring >> Profiler and Discovery >> Endpoint Profiler page. In this example one server was discovered and profiled, clicking on the server opens the detail view.

Monitoring > Profiler and Discovery > Endpoint Profiler

Endpoint Profiler

24 Total Devices

0(0%) Smartdevices

0(0%) Computers

24(100%) Unmanaged Devices

Filter: All Endpoints

Device Category

Server (1)

Switch (1)

Access Points (2)

Unknown (20)

Server

Switch

Access Points

Unknown

Device Family

ClearPass (1)

ClearPass

Device Name

ClearPass VM (1)

ClearPass VM

Change Selection

Mark Known

Mark Unknown

Mark Disabled

#	MAC Address	Hostname	Device Category	Device OS Family	Status
1.	000c2914c4f9	CPPM_6_6_1	Server	ClearPass	Unknown

[Back to Network Discovery](#)
Showing 1-1 of 1
[Authentication Records](#)

The fingerprint shows that the ClearPass VM server was profiled using SNMP.

**View Endpoint**

EndPoint	Attributes
MAC Address	000c2914c4f9
Description	
Status	Unknown
MAC Vendor	VMware, Inc.
Added by	Policy Manager
IP Address	192.168.1.251
Static IP	TRUE
Hostname	CPPM_6_6_1
Device Category	Server
Device OS Family	ClearPass
Device Name	ClearPass VM
Added At	Aug 19, 2016 13:34:11 UTC
Updated At	Aug 20, 2016 00:21:24 UTC
Show Fingerprint	<input checked="" type="checkbox"/>

**Endpoint Fingerprint Details**

TCP Fingerprint:

TCP Device Category:

SNMP System Description: ClearPass CP-VA

## Importing Discovered Devices

Device Discovery automates the process of adding new network devices to the ClearPass Network Device table. Go to **Monitoring >> Profiler and Discovery >> Discovered Devices**.

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

#	Name	IP Address	Vendor	Status	Update Time
1.	ArubaS2500-24P	192.168.1.207	Aruba	New	2016-08-19 22:41:57
2.	HP-3800-48G-PoEP-4SFP+	192.168.2.1	Hewlett-Packard-Enterprise	New	2016-08-19 22:41:57

[Back to Network Discovery](#) Showing 1-2 of 2 [Import](#) [Ignore](#)

To add the HP3800 switch, select its device entry and click **Import**.

**Network Device Details**

RADIUS Shared Secret: [ ] Verify: [ ]

TACACS+ Shared Secret: [ ] Verify: [ ]

Override Vendor: ☐

Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799

**Note:** Names with special characters other than -, \_, { }, [ ], ( ), dot and space will be replaced by underscore

[Import](#) [Cancel](#)

Configure the RADIUS and TACACS+ shared secrets and enable CoA. The network device will be added to the ClearPass network device table and the description will show that it was added by Network Discovery.

You can see the results of the import in **Configuration >> Network >> Devices**.

Filter: 

Name

 contains 

+

Go

Clear Filter

Show

10

 records

#	<input type="checkbox"/>	Name ▲	IP or Subnet Address	Description
1.	<input type="checkbox"/>	HP-3800-48G-PoEP-4SFP_	192.168.2.1	Added by Network Discovery
2.	<input type="checkbox"/>	MAS	192.168.1.207	

Showing 1-2 of 2

ExportDelete

# Troubleshooting

## Event Viewer

To verify the discovery scan completed successfully check the event viewer. SNMP service shows the network scan completing successfully but also shows read device information errors.

Monitoring » Event Viewer

### Event Viewer

Select Server: CPPM\_6\_6\_1 (192.168.1.251)

Filter: Source contains snmp Go Clear Filter Show 10 records

#	Source	Level	Category	Action	Timestamp
1.	SnmpService	INFO	NetworkScan	Success	Aug 19, 2016 22:41:57 UTC
2.	SnmpService	WARN	ReadDeviceInfo	Failed	Aug 19, 2016 22:41:57 UTC
3.	SnmpService	WARN	ReadDeviceInfo	Failed	Aug 19, 2016 22:41:39 UTC

Showing 1-3 of 3

SNMP was unable to get profiling information for 192.168.1.251. The most common reasons for this type of failure is either lack of SNMP support on the device or incorrect SNMP credentials.

System Event Details	
Source	SnmpService
Level	WARN
Category	ReadDeviceInfo
Action	Failed
Timestamp	Aug 19, 2016 22:41:57 UTC
Description	SNMP GET failed for device 192.168.1.251 with error=No response received SNMP GET failed for device 192.168.1.251 with error=No response received Failed to detect SNMP Config No snmp settings found to read the device info
Close	

## Log Configuration

Go to **Administration >> Server Manager >> Log Configuration** and select **ClearPass Network Services**. Set **SNMP request processing** to **DEBUG** level.

Administration » Server Manager » Log Configuration

Select Server: 1921

Service Log Configuration	
Select Service:	ClearPass network services
Module Log Level Settings:	Enable to override default log level
Default Log Level:	WARN
Module Name	Log Level
1. Database	INFO
2. Common framework	INFO
3. NetworkServices base	INFO
4. SNMP request processing	DEBUG
5. SNMP library	INFO
6. PostureService request processing	INFO
7. Auth request processing	INFO
8. DHCP message processing	INFO
9. IF-MAP request processing	INFO

This log entry shows that the SSH Login to 192.168.1.244 failed. The most common causes for this type of failure are invalid credentials or the target does not permit remote login.

{

```
"ip": "192.168.1.244",
"host_info": {
  "ip": "192.168.1.244",
  "mac": "000c292f6c23",
  "id": "scan-1471692033-27",
  "start": "2016-08-20T11:20:33.71779289Z",
  "end": "2016-08-20T11:20:57.451885387Z",
  "status": "ssh: scan-1471692033-27 connect/login to 192.168.1.244 failed. Endpoint profile
failed. "
}
```

## Debug Web Page

To simplify troubleshooting, much of the information for the seed device and the discovered devices is collected in special web pages.

### Error! Hyperlink reference not valid.

These pages show device information for configured (seed devices) such as Sys Name, Sys Description, Object ID, and NAD configuration.

The screenshot shows a web interface with a navigation bar at the top. On the left, there's a sidebar with a button labeled '192.168.1.207'. The main content area is titled 'Device information' and contains a list of fields and their values for the device at 192.168.1.207. The fields include Sys Name, Sys Descr, Sys Location, Sys Object ID, Nad Init Required, Force Nad Init, Lldp supported, Cdp supported, Last Update time, and Trap Configured. Below this, there's a section for 'Nad Config' which contains a large JSON object representing the configuration details.

Configured Devices 1 Discovered Devices 2

These are the devices configured in Configuration --> Network --> Devices with SNMP read enabled

192.168.1.207

SwitchPort Info

**Device information**

Sys Name: ArubaS2500-24P

Sys Descr: ArubaOS (MODEL: ArubaS2500-24P-US), Version 7.1.3.2 (34362)

Sys Location:

Sys Object ID: {"exception":false,"valid":true,"BERLength":12,"syntax":6,"BERPayloadLength":12,"dynamic":false,"syntaxString":"OBJECT IDENTIFIER","value":[1,3,6,1,4,1,14823,1,1,28]}

Nad Init Required: false

Force Nad Init: false

Lldp supported: true

Cdp supported: false

Last Update time: 1471646476

Trap Configured: false

**Nad Config**

```
{
  "snmpReadConfigured":true,
  "dbonEventData":{
    "name":MAS,
    "ipAddress":192.168.1.207,
    "tagDefinitionMap":null,
    "cliConfigured":true,
    "radiusVerifySecret":true,
    "snmpWriteConfigured":false,
    "ipAddress":192.168.1.207,
    "verifyEnablePassword":true,
    "verifyPassword":true,
    "password":"aruba123",
    "enablePrompt":true,
    "passwordPrompt":true,
    "port":22,
    "enablePassword":true,
    "commandPrompt":true,
    "id":3004,
    "type":"SSH"
  },
  "defaultVlan":0,
  "forceRead":true,
  "snmpWriteConfig":null,
  "onConnectPorts":true,
  "port":161,
  "readArpInfo":true,
  "zoneId":0,
  "id":3004,
  "onConnectEnforcement":false,
  "snmpReadConfig":{
    "authKey":true,
    "snmpVersion":"V2C",
    "description":true,
    "community":"public",
    "authProtocol":null,
    "privKey":true,
    "securityLevel":null,
    "valid":true,
    "descr":true,
    "communityVerify":true,
    "authKeyVerify":true,
    "privPro":true
  },
  "values":{
    "tagNames":{
    }
  }
}
```

Selecting **Discovered Devices** shows the basic device information for discovered devices.

Configured Devices 1 Discovered Devices 2

Devices discovered during the network discovery

192.168.1.207  
192.168.1.209

### Device information

Switchport info

**Sys Name:** HP-3800-48G-PoEP-4SFP+

**Sys Descr:** HP J9574A 3800-48G-PoE+-4SFP+ Switch, revision KA.16.01.0007, ROM KA.15.10 (/ws/swbuildm/rel\_richmond\_qaoff/code/build/tam/swbuildm\_rel\_richmond\_qaoff\_rel\_richmond) (Formerly ProCurve)

**Sys Location:**

**LLDP supported:** true

**CDP supported:** true

**Last change time:** 0

**IP interfaces**

IP Address	Interface
192.168.2.1	192.168.1.209

**Switchport**

Port	Name	Device Type	Uplink port	No of MACs
1	1	Unknown	false	0
2	2	Unknown	false	0
3	3	Unknown	false	0
4	4	Unknown	false	0
5	5	Switch	true	25
6	6	Unknown	false	0
7	7	Unknown	false	0

Selecting **Switch Port Info** shows port level detail.

Configured Devices 1 Discovered Devices 2

Devices discovered during the network discovery

192.168.1.207  
192.168.1.209

### Port index

0 - 1
1 - 2
2 - 3
3 - 4
4 - 5
5 - 6
6 - 7
7 - 8
8 - 9
9 - 10
10 - 11
11 - 12
12 - 13
13 - 14
14 - 15
15 - 16
16 - 17
17 - 18

**Port Name:** gigabitethernet0/0/0

**Port Descr:** GE0/0/0

**Port Type:** ETHERNET\_PORT

**Device Type:** Switch

**If Type:** 6

**Port Active:** true

**Trunk Port:** false

**Last update time[Ms]:** 1471646451852

**MAC Address set**

308d993336a40
---------------

## Additional Resources

Detailed information on ClearPass Profiling can be found in the ClearPass Profiling Tech Note and the ClearPass Profiling Quick Start Guide available on the support site.

Support Site:

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/7961/Default.aspx>



a Hewlett Packard  
Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089

1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)

[www.arubanetworks.com](http://www.arubanetworks.com)