

ClearPass profiling

Wat zit er op jouw netwerk?

Herman Robers, Aruba CSE Security
11 april 2019

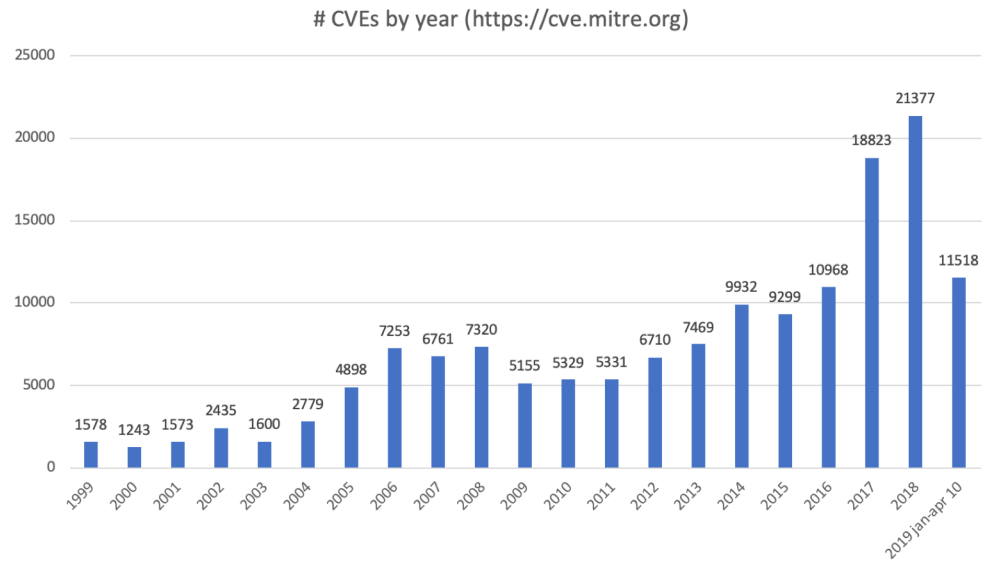
Agenda

- ClearPass recap
- Visibility methods
- Tuning ClearPass for visibility
- Summary
- Q&A



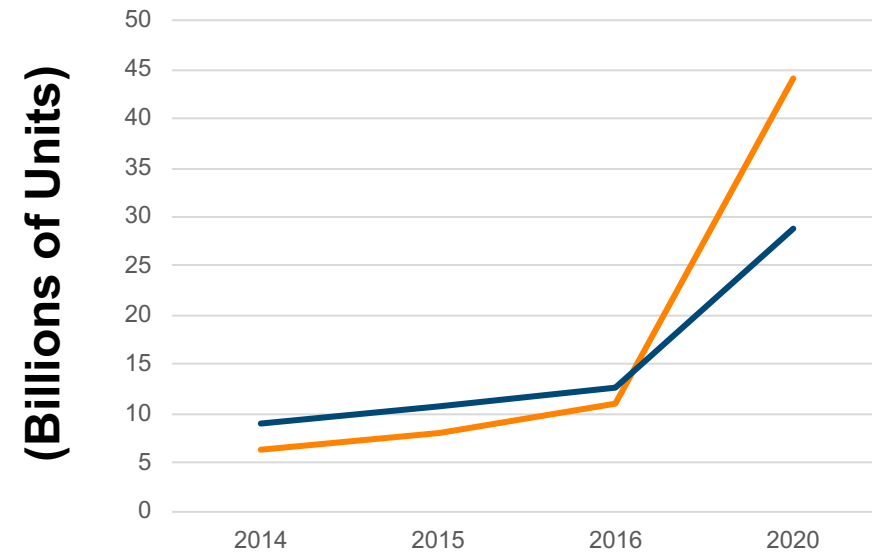
Security Challenges – IoT & Vulnerabilities

Vulnerabilities Identified per year



Source : MITRE CVE

Internet of Things Units Installed Base by Category



Source : Gartner 2016

Control – REMOVING UNCERTAINTY

- Enterprises define who can access
 - Files
 - Applications
- ClearPass extends that capability to network access



Defines **WHO** and **WHAT DEVICES** can connect to:

Which
DEVICES

Which
DATA

Which
INFRASTRUCTURE

Which
APPLICATIONS

ClearPass Solution



VISIBILITY

- Know what's connected on your wired & wireless multivendor environment
- See who is authenticated by role



CONTROL

- Reduce risk and workload through Automation – All devices Authenticated or Authorized – NO UNKNOWN DEVICES



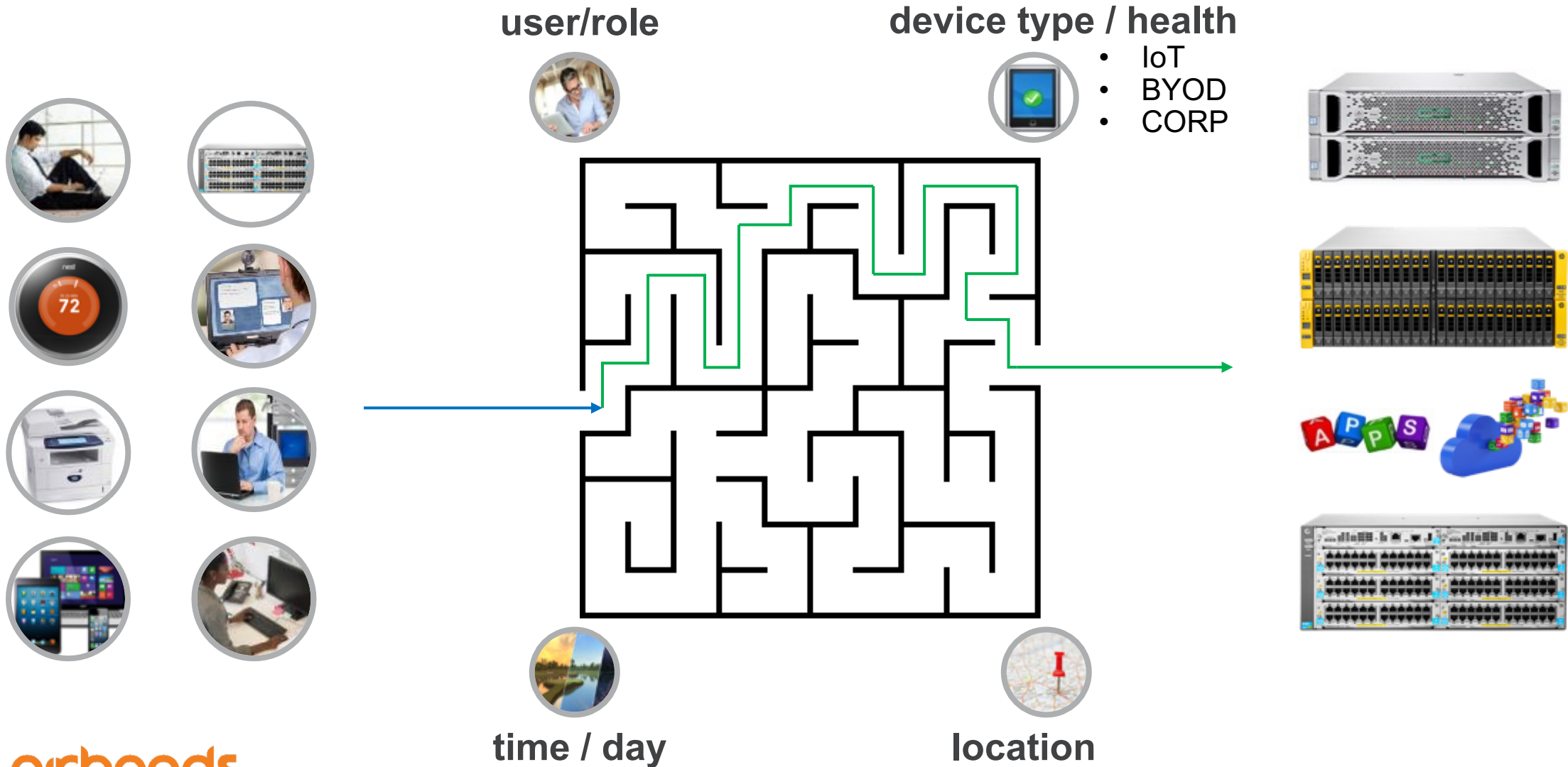
RESPONSE

- Change rules for users and devices based on behavior
- Adaptive response brokering with best of breed security solutions

Visibility – Profile Everything



Control – AUTOMATED AUTHENTICATION & AUTHORIZATION



Security Challenges – Separate Systems

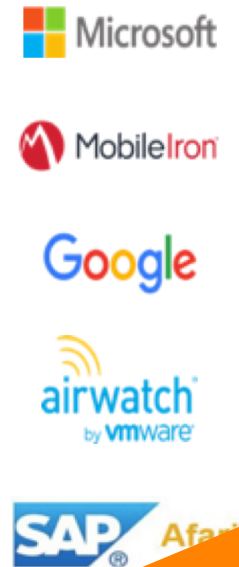
Security



SIEM



Device Management



MFA

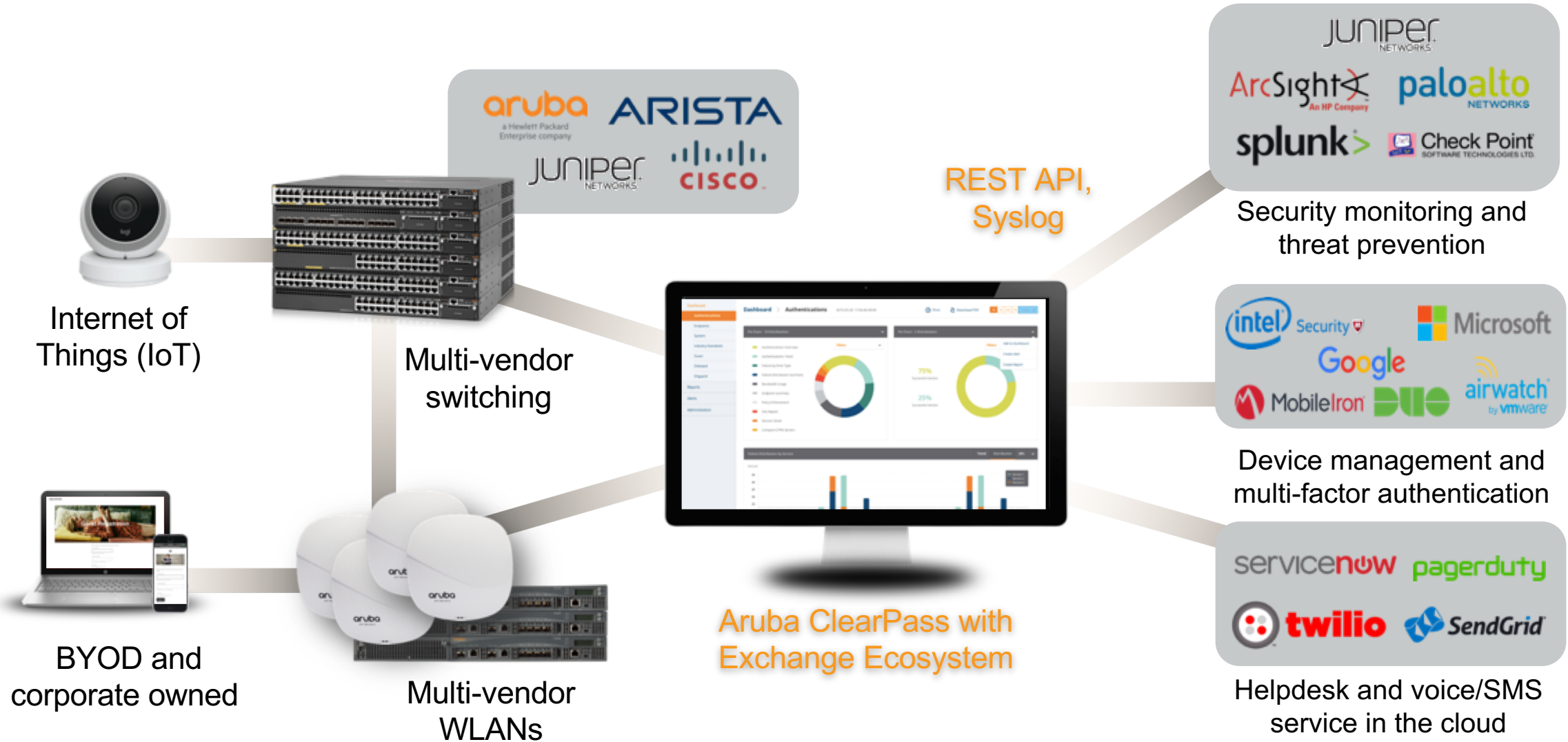


Services



**TOO MANY SECURITY TOOLS
SECURITY TOOLS NEED
TO WORK TOGETHER**

ClearPass Exchange: End to End Control









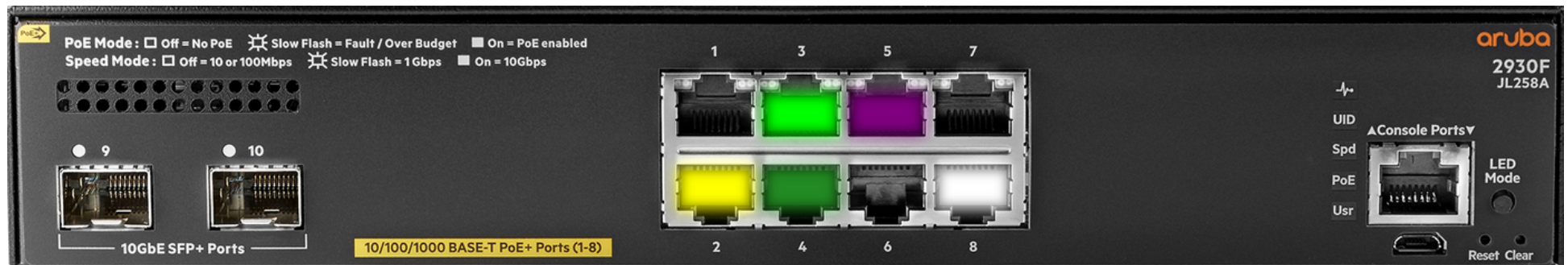
Controlling Network Access

#	Request Timestamp ▾	Source	NAS Port	Host MAC Addr	Username	Service	Login Status	Enforcement Profiles
1.	2019/01/17 08:57:16	RADIUS	1	b827ebde000d	b827ebde000d	Derin_Wired MAC - AOSS	ACCEPT	Introspect-Login-Logout-Profile, IoT
2.	2019/01/17 08:38:15	RADIUS	1	b827ebde000d	b827ebde000d	Derin_Wired MAC - AOSS	ACCEPT	Email Security Response Team - Unknown Device Connected, Isolate
3.	2019/01/17 08:37:09	RADIUS	1	b827ebde000d	b827ebde000d	Derin_Wired MAC - AOSS	ACCEPT	Profile

adding some colour...

Port Color per Role Assigned

	Uplink		Infrastructure
	Block		IAP
	Unknown		Corp
	Profile		AppleTV
	IoT		WebCam
	GuestReg		Guest
	BYOD		VoIP



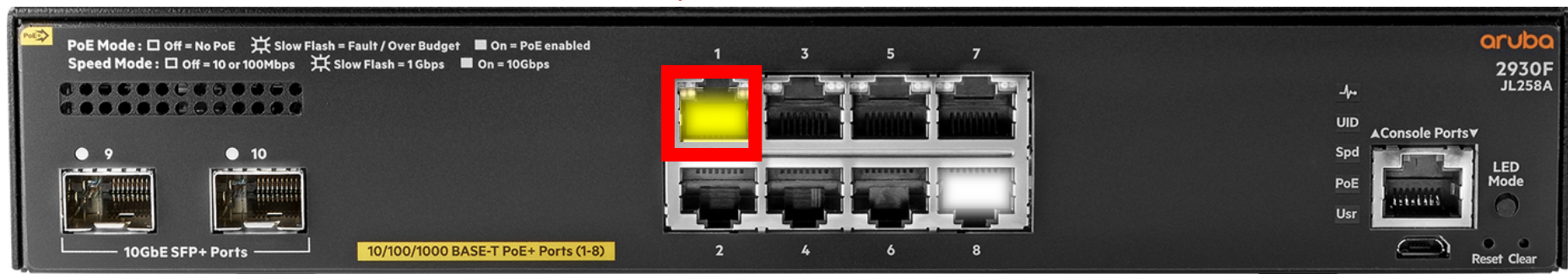
Step 1: Initial Device Connection

Summary	Input	Output	Alerts	Accounting
Login Status:	ACCEPT			
Session Identifier:	R000005a8-06-5c40af35			
Date and Time:	Jan 17, 2019 08:37:09 PST			
End-Host Identifier:	b8-27-eb-de-00-0d			
Username:	b827ebde000d			
Access Device IP/Port:	10.228.80.49:1 (Derin 2930F / Hewlett-Packard-Enterprise)			
System Posture Status:	UNKNOWN (100)			
Policies Used -				
Service:	Derin_Wired MAC - AOSS			
Authentication Method:	MAC-AUTH			
Authentication Source:	None			
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Time Source]			
Roles:	1547743030 1st_Unknown, Not_Profiled, [User Authenticated]			
Enforcement Profiles:	Profile			

```
SWITCH# show port-access clients 1
Downloaded user roles are preceded by *
Port Access Client Status
```

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
1	b827ebde000d	b827eb-de000d	10.228.85.6	*Profile-3139-1	MAC	3008

- Port Color per Role Assigned
- Uplink
 - Block
 - Unknown
 - Profile
 - IoT
 - GuestReg
 - BYOD
 - Infrastructure
 - IAP
 - Corp
 - AppleTV
 - WebCam
 - Guest
 - VoIP



Step 2: ClearPass Profiles Device

Endpoint	Attributes	Device Fingerprints	
MAC Address	b827ebde000d	IP Address	10.228.85.6
Description		Static IP	FALSE
Status	<input type="radio"/> Known client	Hostname	raspberrypi
	<input checked="" type="radio"/> Unknown client	Device Category	Computer
	<input type="radio"/> Disabled client	Device OS Family	Raspberry Pi
MAC Vendor	Raspberry Pi Foundation	Device Name	Raspberry Pi
Added by	Policy Manager	Added At	Jan 17, 2019 08:31:16 PST
Online Status	<input checked="" type="checkbox"/> Online	Last Profiled At	Jan 17, 2019 08:44:19 PST
Connection Type	Wired		
Switch IP	10.228.80.49		
Switch Port	1		

Device
category
profiled

Step 3: Device Category Change

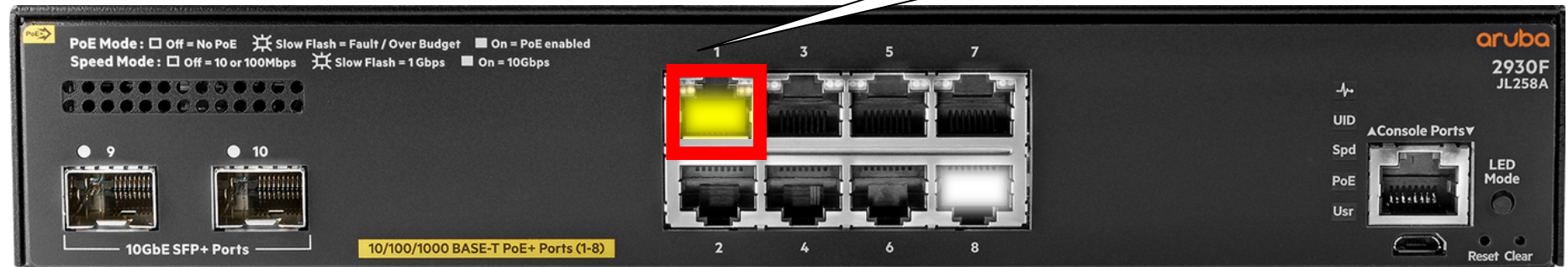
Summary	Input	Output	Accounting	Alerts	RADIUS CoA
CoA Action# 1					
Date and Time	Jan 17, 2019 08:37:32 PST				
Application Name	Policy Manager				
RADIUS CoA Action Type	CoA				
RADIUS CoA Action Name	[ArubaOS Switching - Bounce Switch Port]				
Status Code	1				
Status Message	Radius [ArubaOS Switching - Bounce Switch Port] successful for client b827ebde000d.				
RADIUS CoA Attributes	NAS-IP-Address = 10.228.80.49 User-Name = b827ebde000d HPE-Port-Bounce-Host = 12 Event-Timestamp = 1547743050 Calling-Station-Id = b8-27-eb-de-00-0d NAS-Port = 1				

Forces port bounce

Port disconnects for 12 seconds.
Device forgets IP

Port Color per Role Assigned

Uplink	Infrastructure
Block	IAP
Unknown	Corp
Profile	AppleTV
IoT	WebCam
GuestReg	Guest
BYOD	VoIP



Step 4: Now “Profiled” device connects

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R000005ab-06-5c40b3ec		
Date and Time:	Jan 17, 2019 08:57:16 PST		
End-Host Identifier:	b8-27-eb-de-00-0d (Computer / Raspberry Pi / Raspberry Pi)		
Username:	b827ebde000d		
Access Device IP/Port:	10.228.80.49:1 (Derin 2930F / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Derin_Wired MAC - AOSS		
	MAC-AUTH		
	Local:localhost		
	[Guest User Repository], [Endpoints Repository], [Time Source]		
Roles:	1547744237, Computer, Known, Profiled, Raspberry Pi, [User Authenticated], raspberrypi		
Enforcement Profiles:	Introspect-Login-Logout-Profile, IoT		

Inform other services

Inform other services

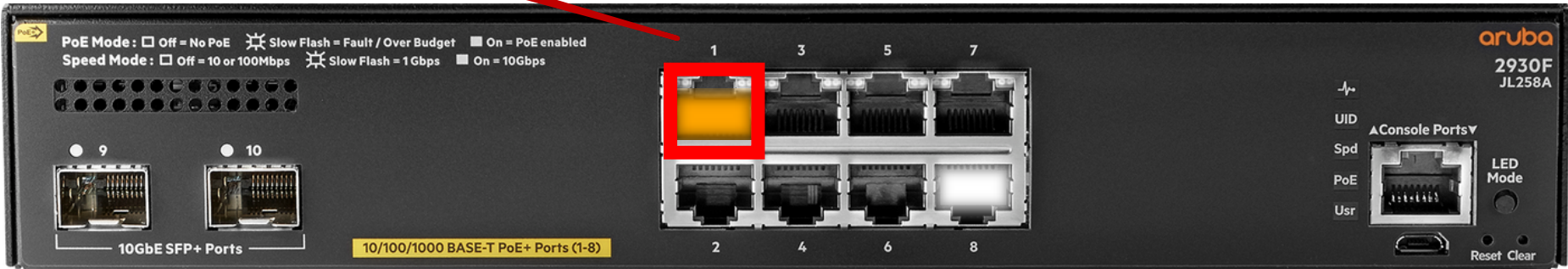
Different VLAN (could be tunnelled)

```
SWITCH# show port-access clients 1
Downloaded user roles are preceded by *
Port Access Client Status
```

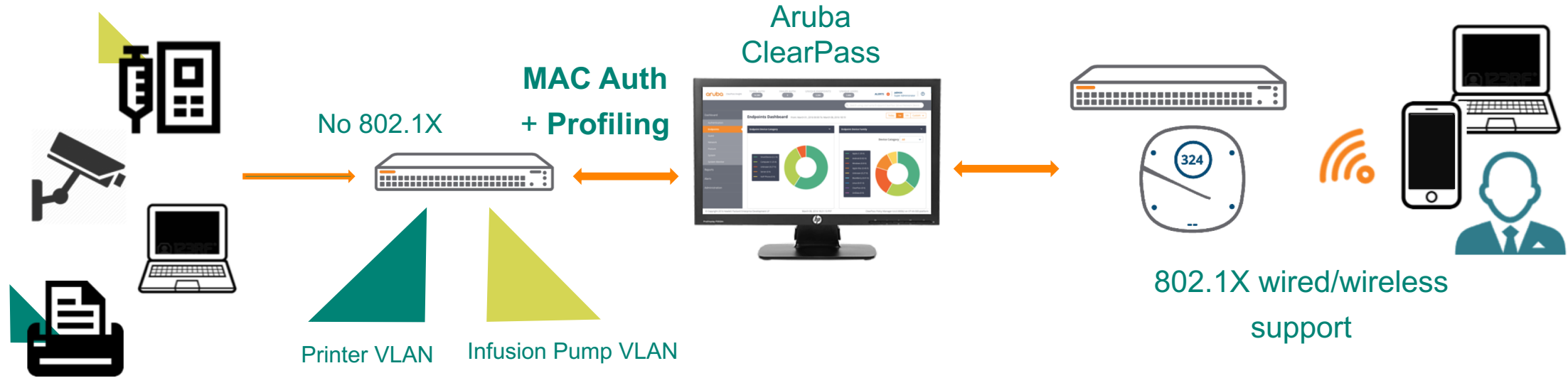
Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
1	b827ebde000d	b827eb-de000d	10.228.87.5	*IoT-3139-4	MAC	3012

Port Color per Role Assigned

	Uplink		Infrastructure
	Block		IAP
	Unknown		Corp
	Profile		AppleTV
	IoT		WebCam
	GuestReg		Guest
	BYOD		VoIP



Yes, we can do that on wireless as well, and multi-vendor

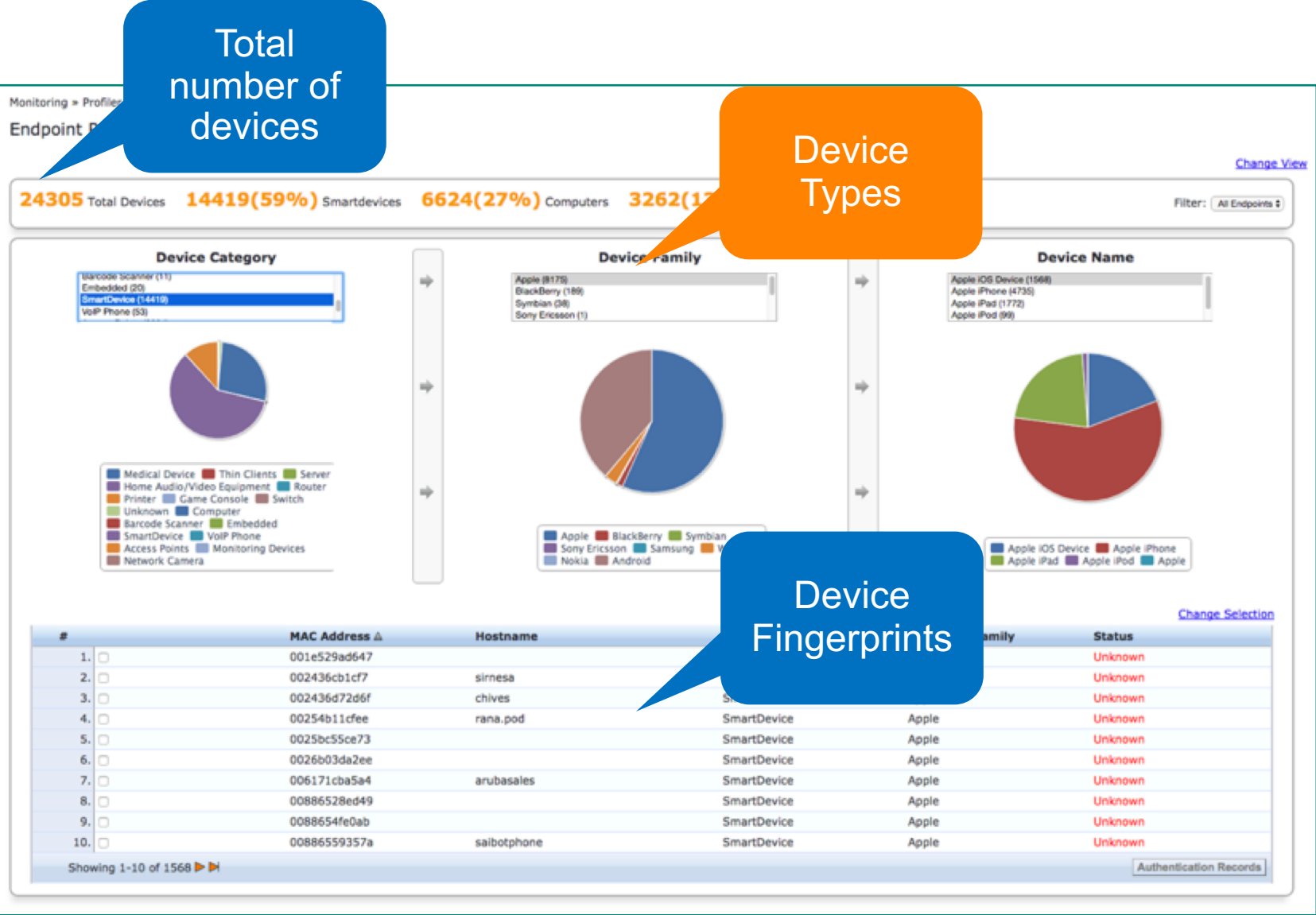


- Use 802.1X whenever possible
- Fallback to MAC authentication for non 802.1X capable devices
- Leverages ClearPass profiling for wired/wireless - IoT, laptops, mobile phones.

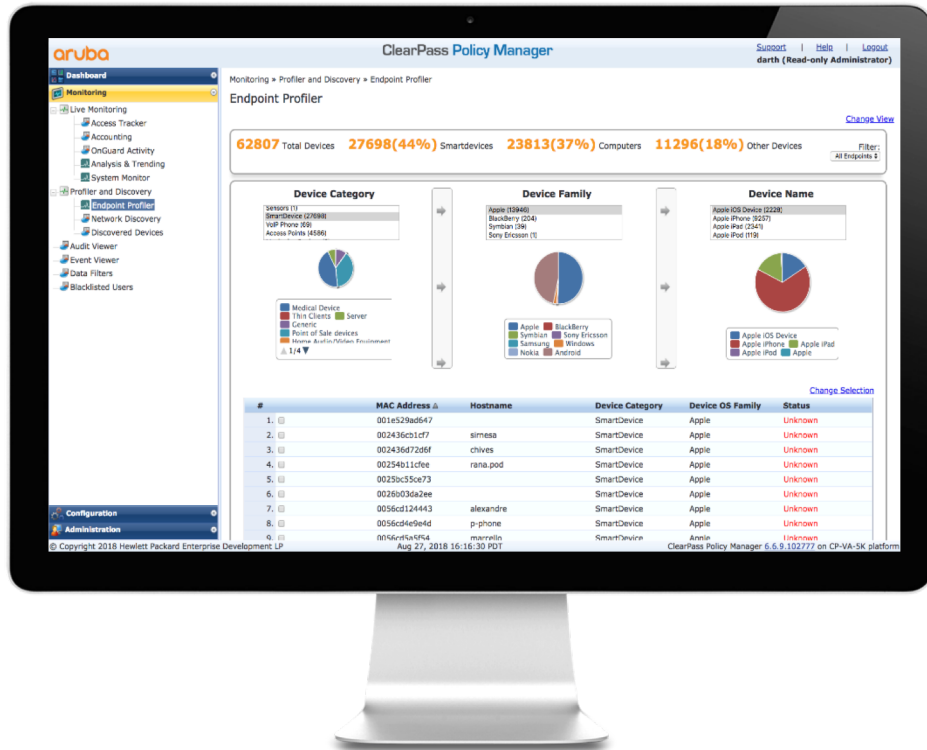
Profiling and Visibility

Methods and techniques

Visibility - What's on your network ?



Step 0: Device Visibility



Passive

- DHCP Fingerprinting
- TCP Fingerprinting
- HTTP User-Agent
- Aruba Device Fingerprint
- Cisco Device Sensor
- IPFIX/sFlow/Netflow

Active

- NMAP
- SNMP
- SSH
- WMI
- ARP
- CDP/LLDP Table
- OnGuard

Exchange

- MDM/EMM
- CMDB
- Endpoint/EDR
- Network Audit database

ML/AI

- IntroSpect
- ClearPass Device Insight*

Tuning ClearPass for visibility

Endpoints: What, Where and When?

- Understanding what is connecting to your network
- Taking advantage of existing ClearPass tools
 - Passive Scanning: DHCP profiling
 - Active Scanning using SNMP, SSH, WMI and NMAP
 - Network hierarchical scanning
 - Subnet scanning
- Using enhanced reports
 - Stakeholder focused overview report
 - Detailed technician report

ClearPass Deployment

- Install the Physical or Virtual appliance
 - Supports up to 4000 concurrent MAC addresses
- Configure the basic IP address credentials
- Login to GUI
 - Change default admin password
 - Install and activate Access licenses

Enable Insight

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

ClearPass Portal

Users and Privileges

Server Manager

Server Configuration

Log Configuration

Local Shared Folders

Licensing

External Servers

Certificates

Administration » Server Manager » Server Configuration

Server Configuration

Set Date & Time

Change Cluster Password

Manage Policy Manager Zones

NetEvents Targets

Clear Machine Authentication Cache

Virtual IP Settings

Make Subscriber

Cluster-Wide Parameters

Publisher Server: vis-cppm.hpearubademo.com [192.168.137.25]

#	Server Name	Management Port	Data Port	Zone	Insight	Cluster Sync	Last Sync Time
1.	vis-cppm.hpearubademo.com	192.168.137.25	-	default	Enabled	Enabled	-

Showing 1-1 of 1

Collect Logs

Backup

Restore

Cleanup

Shutdown

Reboot

System

Services Control

Service Parameters

System Monitoring

Network

FIPS

Hostname:

vis-cppm.hpearubademo.com

FQDN:

Policy Manager Zone:

default

Manage Policy

Enable Performance Monitoring Display:

☒ Enable this server for performance monitoring display

Insight Setting:

☒ Enable Insight

☒ Enable as Insight Master

Current Master:vis-cppm.hpearubademo.com(192.168.137.25)

Enable Ingress Events Processing:

☐ Enable Ingress Events processing on this server

Master Server in Zone:

Primary master

Span Port:

Data Port

☐ Enable TCP/ARP Fingerprinting

	IPv4	IPv6	Act
Management Port	IP Address	192.168.137.25	
	Subnet Mask	255.255.255.0	
	Default Gateway	192.168.137.254	
Data/External Port	IP Address		
	Subnet Mask		
	Default Gateway		
DNS Settings	Primary	8.8.8.8	
	Secondary		
	Tertiary		
	DNS Caching	Disabled	

Use only the Management port – keeps design simple

System

Services Control

Service Parameters

System Monitoring

Network

FIPS

Select Service:

Radius server

Parameter Name	Parameter Value	Default Value	Allowed V
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	
Thread Pool			
Maximum Number of Threads	40 threads	40	10-300
Number of Initial Threads	20 threads	20	5-300

Configure Insight

aruba ClearPass Insight

TOTAL AUTH 0 FAILED AUTH 0 UNIQUE ENDPOINTS 0 UNIQUE USERS 0

ALERTS 0 Menu

Search using Username/Endpoint/ClearPass Server/Network Device

Dashboard
Inventory
Reports
Alerts
Administration

Administration

Settings

File Transfer Settings

Host	Protocol	Port	Username	Password
<input type="text" value="Host"/>	<input checked="" type="radio"/> SCP	<input type="text" value="22"/>	<input type="text" value="Username"/>	<input type="text" value="Password"/>

Timeout

Database Settings

Database Retention	Report Retention	CSV Report Limit
<input type="text" value="90"/> Days	<input type="text" value="60"/> Days	<input type="text" value="50000"/> Rows

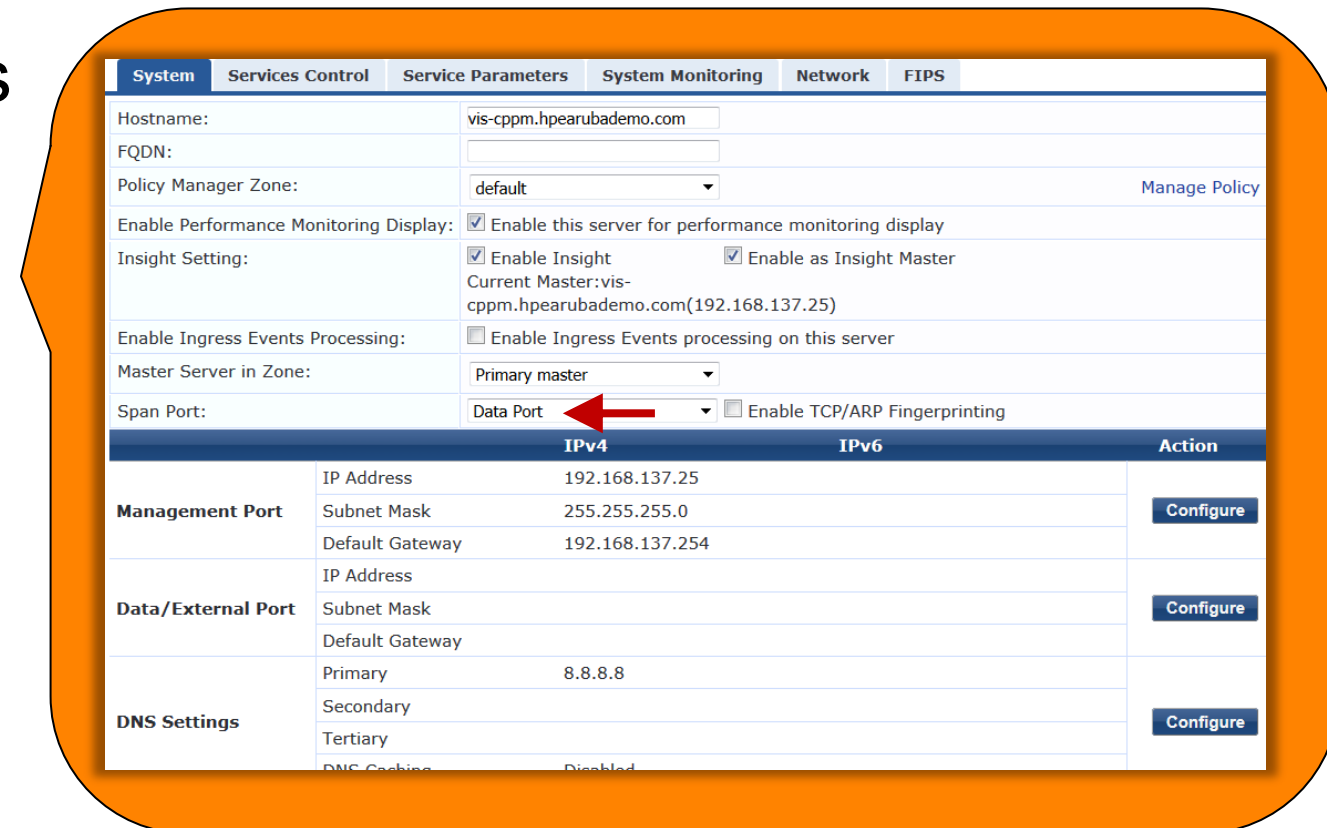
By default database retains information for 30 days

Better to extend to say 90 days – can go to 270 days! If disk space permitting


Configure Span port Profiling



- L3: DHCP relay to ClearPass
- L2: Port mirror traffic on to the ClearPass Data port
 - Configure ClearPass Data port as SPAN receiver

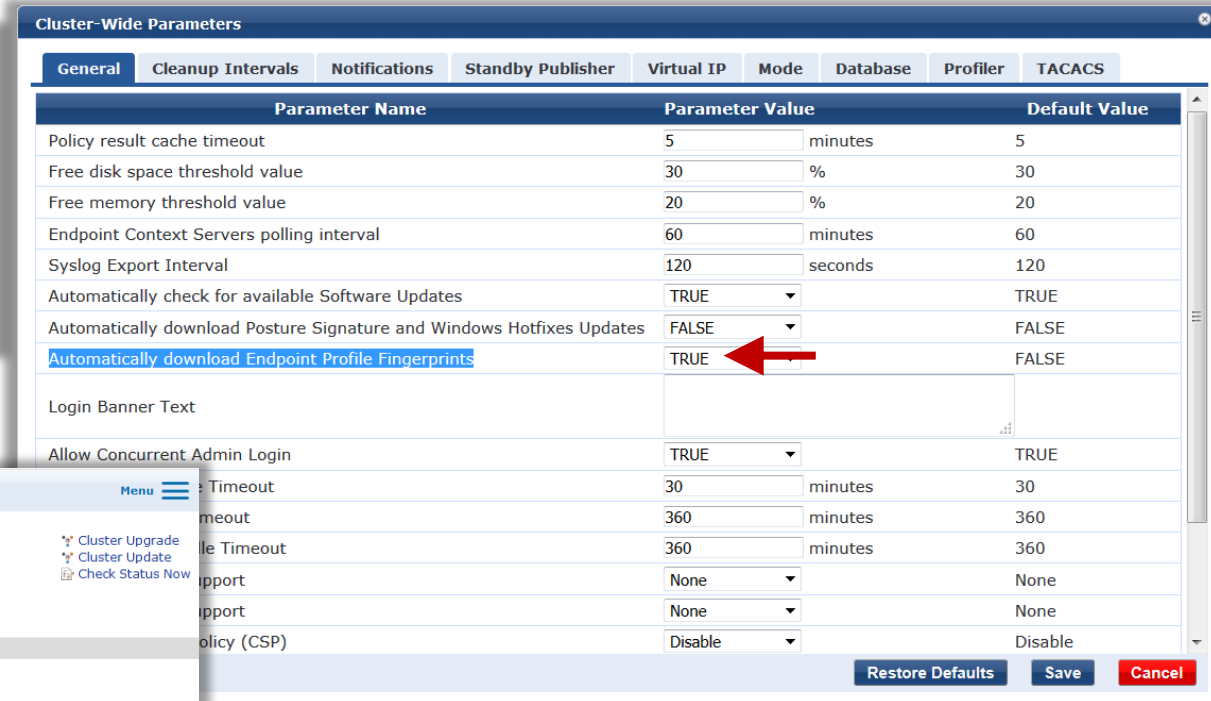


Configure Auto-Profile Fingerprints Update



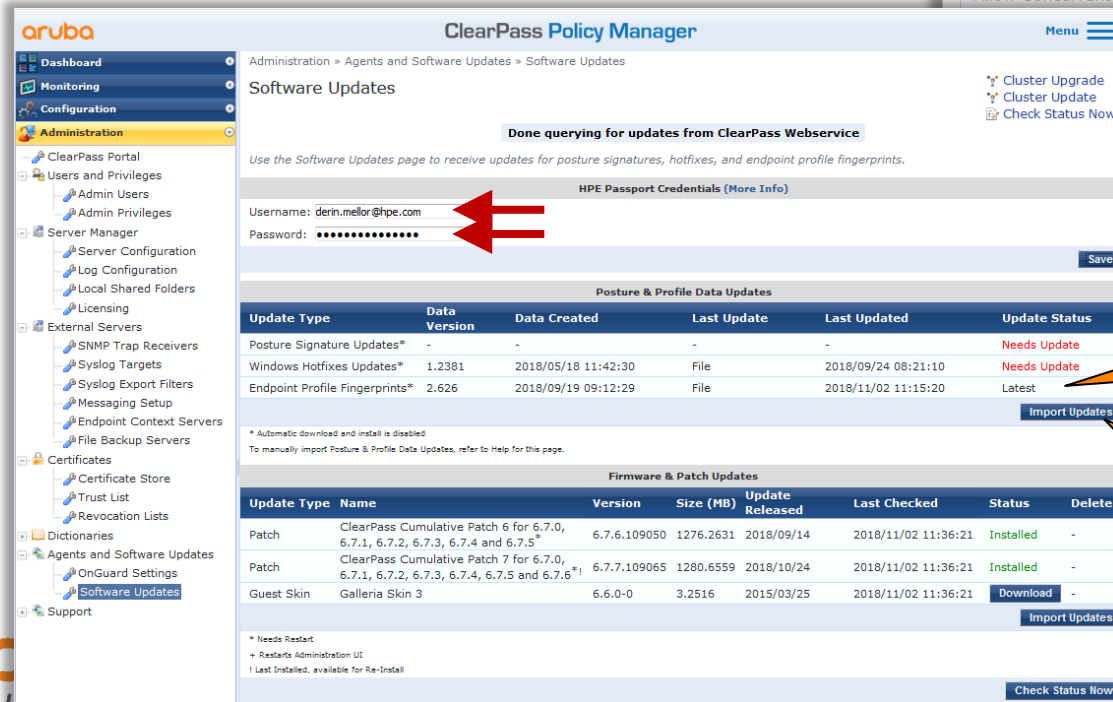
The screenshot shows the 'Server Configuration' page in the Aruba ClearPass Policy Manager. The left sidebar contains navigation links for Dashboard, Monitoring, Configuration, and Administration. The main content area shows the 'Server Configuration' section with a list of servers. A red arrow points to the 'Data Port' column header in the table.

#	Server Name	Management Port	Data Port	Zone	Insight	Cluster Sync	Last Sync Time
1.	vis-cppm.hpearubademo.com	192.168.137.25		default	Enabled	Enabled	-



The screenshot shows the 'Cluster-Wide Parameters' page in the Aruba ClearPass Policy Manager. The 'General' tab is selected, and the 'Automatically download Endpoint Profile Fingerprints' parameter is highlighted with a red arrow.

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
Endpoint Context Servers polling interval	60 minutes	60
Syslog Export Interval	120 seconds	120
Automatically check for available Software Updates	TRUE	TRUE
Automatically download Posture Signature and Windows Hotfixes Updates	FALSE	FALSE
Automatically download Endpoint Profile Fingerprints	TRUE	FALSE
Login Banner Text		
Allow Concurrent Admin Login	TRUE	TRUE



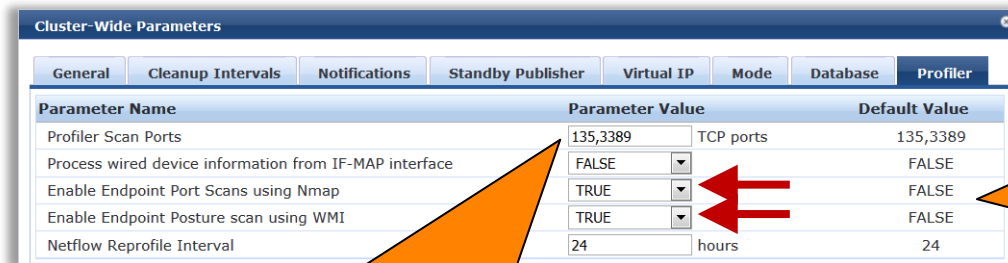
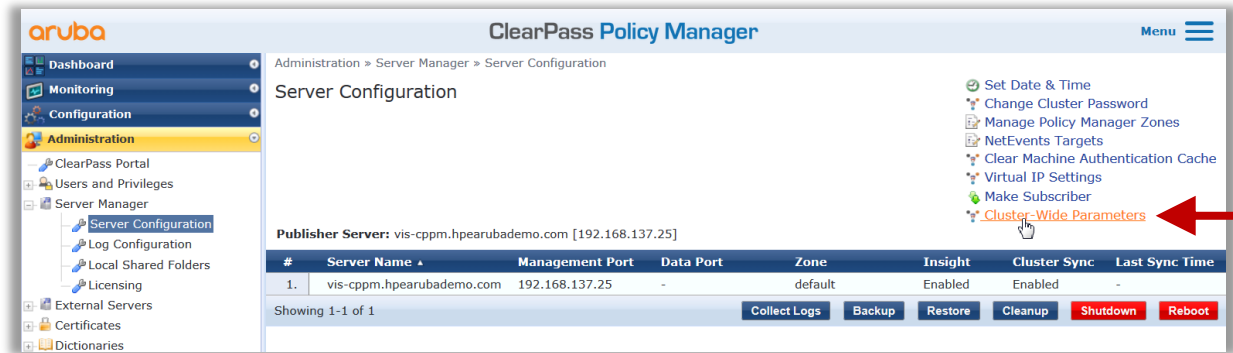
The screenshot shows the 'Software Updates' page in the Aruba ClearPass Policy Manager. The 'HPE Passport Credentials' section is highlighted with a red arrow. Below it, the 'Posture & Profile Data Updates' table shows the status of various updates.

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	-	-	-	-	Needs Update
Windows Hotfixes Updates*	1.2381	2018/05/18 11:42:30	File	2018/09/24 08:21:10	Needs Update
Endpoint Profile Fingerprints*	2.626	2018/09/19 09:12:29	File	2018/11/02 11:15:20	Latest

Validate fingerprints have been updated

If ClearPass operating in offline mode can manually download updates and upload on to ClearPass

Enable Active Fingerprinting



Enable nmap and WMI active scanning

WARNING
Nmap scanning scans all 64K TCP ports on each device

One option: Initially do full scan. Gather ports of interest and other known common and malicious ports. Populate the "Profiler Scan Ports" (disable NMAP scan once done)

Define SNMP and WMI credentials

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar has a 'Configuration' menu with 'Profile and Network Scan' > 'Profile Settings' selected. The main area is titled 'Profile Settings' and has tabs for 'SNMP Configuration', 'SSH Configuration', and 'WMI Configuration'. The 'SNMP Configuration' tab is active. It shows a 'Specify SNMP' section with 'IP Subnets/IP Addresses' containing a list of IP ranges. Below this is an 'Entries' table with three rows: V2C, public; V2C, private; and V2C, aruba123. At the bottom, there are fields for 'SNMP Version' (set to 'SNMP v1 with community strings'), 'Description', and 'Community String', along with 'Reset', 'Save Entry', 'Save', and 'Cancel' buttons.

Version	Username	Description
1. <input type="radio"/> V2C	public	
2. <input type="radio"/> V2C	private	
3. <input type="radio"/> V2C	aruba123	

Define all the networks to be scanned

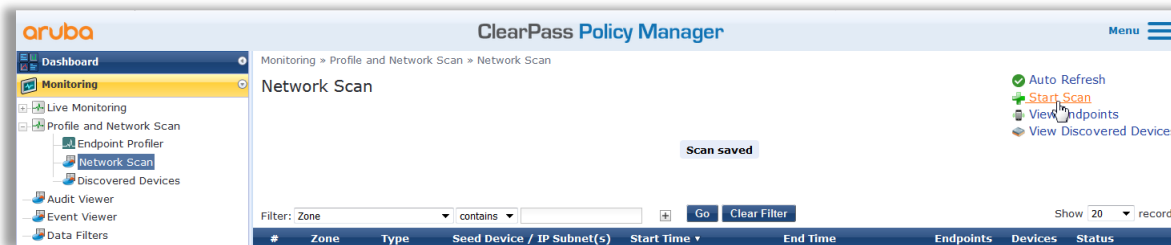
Define SNMP credentials

The screenshot shows the 'Configuration' window in the ClearPass Policy Manager. It has a section for 'IP Subnets/IP Addresses' with a text area containing '192.168.0.0/8, 172.16.0.0/12, 10.0.0.0/8'. Below this is an 'Entries' table with one row: hpearubademo.com/administrator. At the bottom, there are fields for 'Domain', 'Username', 'Password', 'Verify Password', and 'Description', along with 'Reset', 'Save Entry', 'Save', and 'Cancel' buttons.

Username	Description
1. <input type="radio"/> hpearubademo.com/administrator	

Define WMI credentials

Force Network Scan – Get a quick report



The 'Schedule Scan' dialog box contains the following fields and options:

- Scan Type:** Radio buttons for 'Network Scan' (selected) and 'Subnet Scan'.
- Zone:** A dropdown menu currently set to 'default'.
- Seed Devices (CSV):** A text input field containing '192.168.139.99,192.168.137.254'.
- Frequency of Scan:** A dropdown menu set to 'On Demand'.
- Start Time of Scan:** A text input field with '(optional)' next to it.
- Scan Depth:** A dropdown menu set to '3'.
- Probe ARP entries:** A checkbox labeled 'Probe all the ARP entries found to discover devices' which is checked.

At the bottom of the dialog is a 'WARNING' message: 'Performing network scans can be resource intensive and time consuming. For large networks, scans could take more than an hour and ideally should be done on a ClearPass node that is not servicing core authentications, or should be done outside of normal business hours.' Below the warning are 'Save' and 'Cancel' buttons.

If the network is large best to do the as a scheduled scan overnight

Specify as many known "seed" routers

Define number of router hops the discover will traverse

Make sure you read the ARP tables

On saving this will take typically 30s before the scan commences

Monitor Network Scan

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar has a 'Monitoring' menu with 'Network Scan' selected. The main panel is titled 'Network Scan' and includes a description: 'Network Scan uses a configured seed network device (typically a switch, router, or controller) to discover endpoints and network devices.' Below this is a filter bar with 'Zone' set to 'default' and a 'contains' dropdown. A table displays scan results with columns: #, Zone, Type, Seed Device / IP Subnet(s), Start Time, End Time, Endpoints, Devices, and Status. The first row shows a scan in progress with a status of 'Running' and a circular progress indicator.

#	Zone	Type	Seed Device / IP Subnet(s)	Start Time	End Time	Endpoints	Devices	Status
1.	default	Discovery	192.168.137.90 192.168.137.254	2019-02-12 09:15:09		8	2	Running

This indicates the status of the scan

The scan process will appear here

The screenshot shows the Aruba ClearPass Policy Manager interface with the 'Network Scan' page. The left sidebar shows the 'Monitoring' menu with 'Network Scan' selected. The main panel displays a table of completed scans. The table has columns: #, Zone, Type, Seed Device / IP Subnet(s), Start Time, End Time, Endpoints, Devices, and Status. Two rows are shown, both with a status of 'Completed' and a green checkmark icon. The 'Endpoints' and 'Devices' columns for the second row are highlighted with red boxes.

#	Zone	Type	Seed Device / IP Subnet(s)	Start Time	End Time	Endpoints	Devices	Status
1.	default	Discovery	192.168.137.90	2018-01-24 16:15:07	2018-01-24 16:18:44	7	2	Completed
2.	default	Discovery	192.168.137.90 192.168.137.99	2018-02-22 08:35:55	2018-02-22 08:44:13	12	2	Completed

Once scan complete has an indication of the Endpoint and NAS found


Discovered NAS - 1


aruba ClearPass Policy Manager

Monitoring » Profile and Network Scan » Discovered Devices

Discovered Devices

This page provides detailed information about a discovered network device, including a list of its neighbors in the network.

Vendor
ALL (6)
Aruba (2)
Hewlett-Packard-Enterprise (2)
IETF (2)

Aruba IETF
Hewlett-Packard-Enterprise

Status
ALL (6)
Imported (2)
New (4)

New Imported

Name	IP Address	Vendor	Status	Update Time
1. []	192.168.137.254	IETF	New	2019-03-11 15:0
2. []	192.168.137.90	IETF	New	2019-03-11 15:0
3. [] 20:4c:03:1f:fb:30	192.168.137.101	Aruba	Imported	2018-01-24 16:1
4. [x] Aruba-2930F-8G-PoEP-2SFPP	10.137.50.90	Hewlett-Packard-Enterprise	New	2018-02-22 08:5
5. [] HP-2920-24G-PoEP	10.137.10.90	Hewlett-Packard-Enterprise	Imported	2018-01-24 1
6. [] TeamX	192.168.137.99	Aruba	New	2018-02-27 08:44:6

Showing 1-6 of 6

Import Ignore

WARNING: Only devices with a name can be imported

Select and imported NAS as ClearPass NAD

Discovered NAS - 2

aruba ClearPass Policy Manager

Monitoring » Profile and Network Scan » Discovered Devices

Discovered Devices

Network Device Details

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Override Vendor: ☐

Enable RADIUS CoA: ☒ RADIUS CoA Port:

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

Aruba IETF Hewlett-Packard-Enterprise

New Imported

Filter: Name contains Go Clear Filter

Show 20 records

#	Name	IP Address	Vendor	Status	Update Time
1.	<input type="checkbox"/>	192.168.137.254	IETF	New	2019-03-11 15:04:48
2.	<input type="checkbox"/>	192.168.137.90	IETF	New	2019-03-11 15:04:48
3.	<input type="checkbox"/> 20:4c:03:1f:fb:30	192.168.137.101	Aruba	Imported	2018-01-24 16:18:27
4.	<input checked="" type="checkbox"/> Aruba-2930F-8G-PoEP-2SFPP	10.137.50.90	Hewlett-Packard-Enterprise	New	2018-02-22 08:44:07
5.	<input type="checkbox"/> HP-2920-24G-PoEP	10.137.10.90	Hewlett-Packard-Enterprise	Imported	2018-01-24 16:18:27
6.	<input type="checkbox"/> TeamX	192.168.137.99	Aruba	New	2018-02-22 08:44:07

Showing 1-6 of 6

As a minimum
define the
RADIUS secret

This is not used at
this stage but
good step to
control

Alternatively Manually Define NAD

aruba ClearPass Policy Manager

Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains [] Go Clear Filter

Show 20 records

#	Name	IP or Subnet Address	Description
1.	20_4c_03_1f_fb_30	192.168.137.101	Added by Network Discovery
2.	Cisco 3750 Switch	10.29.17.29	
3.	Cisco 3800 Switch	10.29.17.28	
4.	Cisco WLC	10.7.2.170	Cisco WLC located into the Test Plant
5.	Cisco WLC	10.2.2.2	
6.	Cisco WLC	172.16.0.109	

Edit Device Details

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: IAP

IP or Subnet Address: 192.168.137.100 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Aruba

Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799

Enable RadSec: ☐

Copy Save Cancel

If you have a raft of Network Devices to import use a CSV file – follow instructions defined here <https://ase.arubanetworks.com/solutions/id/95>

Manually Update NAD SNMP Details

aruba ClearPass Policy Manager

Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in ClearPass.

Filter: Name contains records

#	Name	IP or Subnet Address	Description
1.	20_4c_03_1f_fb_30	192.168.137.101	Added by discovery
2.	Cisco 3750 Switch	10.29.17.29	

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement

Allow SNMP Read: ☒ Enable Policy Manager to perform SNMP read operations

Policy Manager Zone: default

SNMP Read Setting: SNMP v2 with community strings

Community String: Verify:

Force Read: ☒ Always read information from this device

Read ARP Table Info: ☒ Read ARP table from this device

ClearPass will poll each defined NAD and pull back the ARP table

This is useful to do in conjunction with the Subnet Scan

Verify the SNMP Poll is Working

By default poll occurs every 60 minutes...

The screenshot shows the Aruba Event Viewer interface. On the left, a sidebar contains a menu with 'Event Viewer' highlighted by a red arrow. The main area displays a table of events. The first event is a 'ClearPass Validate Update Portal Credentials' error. A red arrow points to this event. Below the table, a 'System Event Details' modal is open, showing details for an SNMP event. The details include Source (SnmpService), Level (WARN), Category (ReadDeviceInfo), Action (Failed), and a description stating 'SNMP GET failed for device 10.29.17.29 with error=No response received'. An orange callout bubble at the bottom right states 'Clearly a problem with the SNMP poll'.

aruba

Monitoring » Event Viewer

Event Viewer

Select Server: cppm.hpearubademo.com (172.16.137.20)

Filter: Source contains [] Go Clear Filter Show 50 records

#	Source	Level	Category	Action	Timestamp
1.	ClearPass Validate Update Portal Credentials	ERROR	Validation Error	None	Sep 14, 2018 10:20:23 BST
2.	ClearPass Update Portal Credentials	ERROR	Validation Error	Failure	Sep 14, 2018 10:20:14 BST
3.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:17:43 BST
4.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:14:27 BST
5.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:13:19 BST
6.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:09:11 BST
7.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:09:03 BST
8.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:04:55 BST
9.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:04:47 BST
10.	Snmp	WARN	ReadDeviceInfo	Failed	Sep 14, 2018 10:00:31 BST

System Event Details

Source	SnmpService
Level	WARN
Category	ReadDeviceInfo
Action	Failed
Timestamp	Sep 14, 2018 10:13:19 BST
Description	SNMP GET failed for device 10.29.17.29 with error=No response received Reading sysObjectId failed for device=10.29.17.29 Reading switch initialization info failed for 10.29.17.29

Close

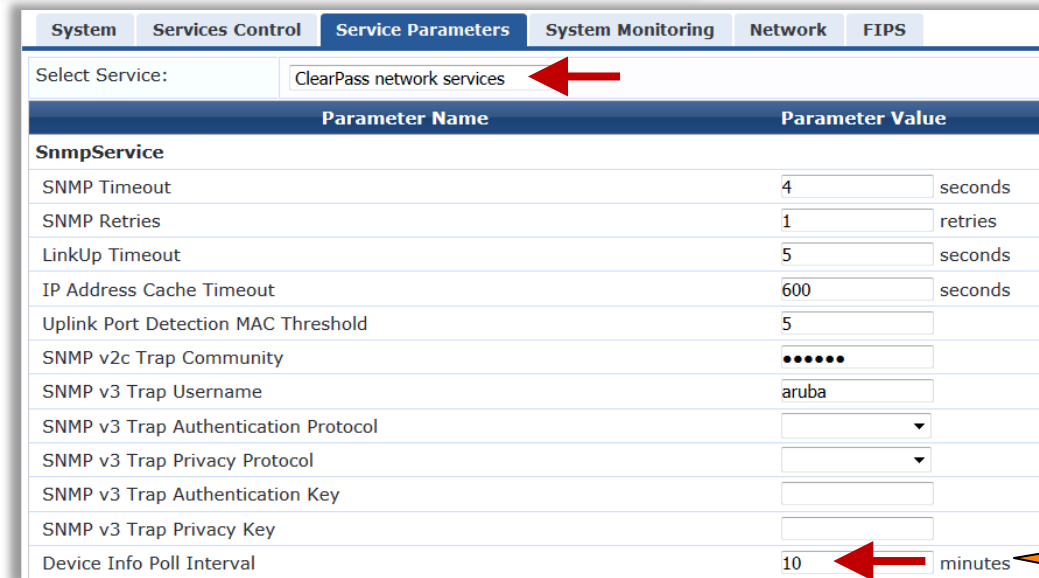
Clearly a problem with the SNMP poll

NAS Poll Rate



The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, ClearPass Portal, Users and Privileges, Server Manager, Log Configuration, Local Shared Folders, Licensing, External Servers, and Certificates. The main content area is titled 'Server Configuration' and shows the 'Publisher Server' configuration for 'vis-cppm.hpearubademo.com [192.168.137.25]'. A table lists the server details, and a list of actions is available on the right.

#	Server Name	Management Port	Data Port	Zone	Insight	Cluster Sync	Last Sync Time
1.	vis-cppm.hpearubademo.com	192.168.137.25	-	default	Enabled	Enabled	-

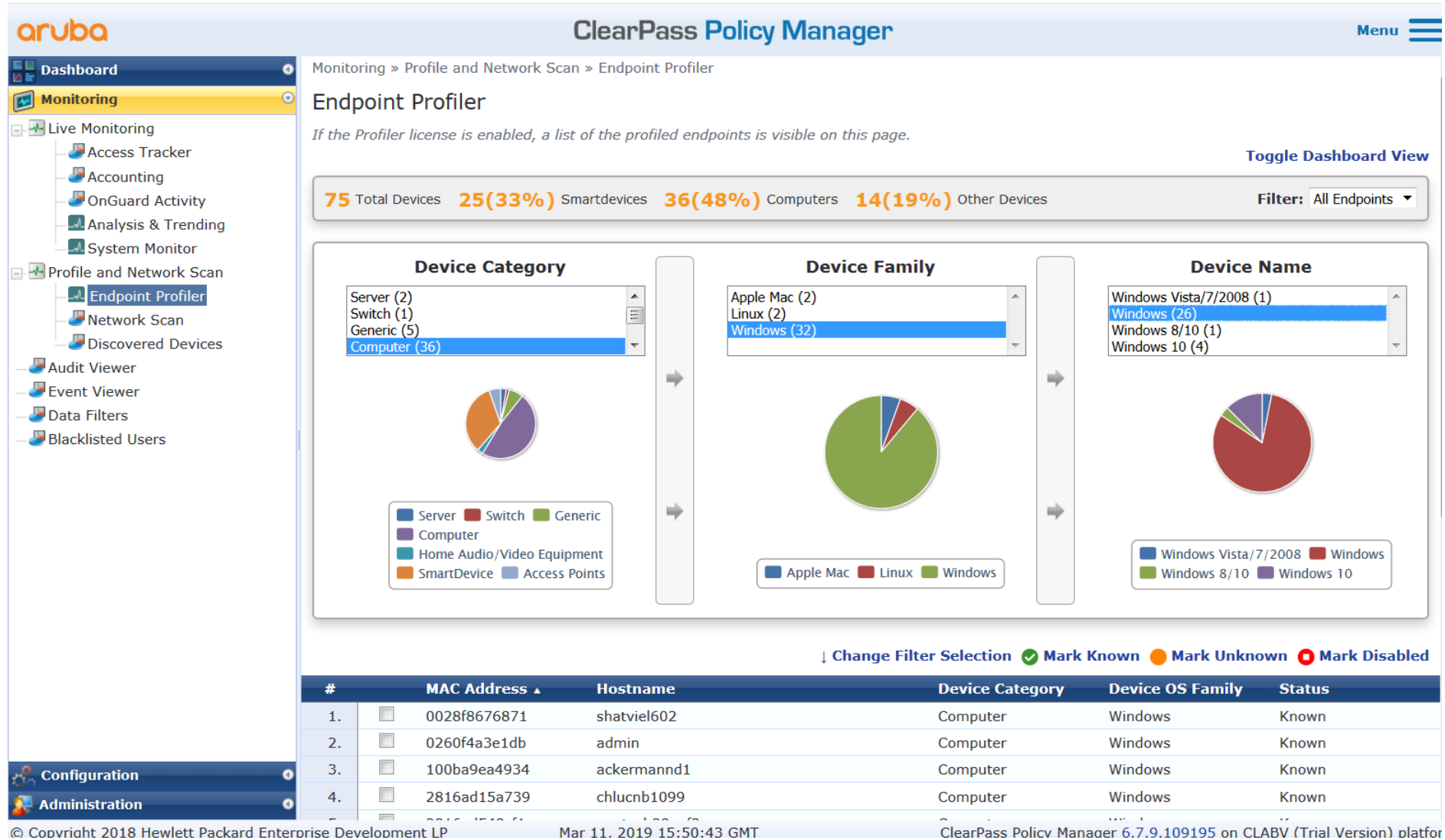


The screenshot shows the 'Service Parameters' tab in the Aruba ClearPass Policy Manager interface. The 'Select Service' dropdown is set to 'ClearPass network services'. The table below lists various parameters and their values.

Parameter Name	Parameter Value
SnmpService	
SNMP Timeout	4 seconds
SNMP Retries	1 retries
LinkUp Timeout	5 seconds
IP Address Cache Timeout	600 seconds
Uplink Port Detection MAC Threshold	5
SNMP v2c Trap Community	*****
SNMP v3 Trap Username	aruba
SNMP v3 Trap Authentication Protocol	
SNMP v3 Trap Privacy Protocol	
SNMP v3 Trap Authentication Key	
SNMP v3 Trap Privacy Key	
Device Info Poll Interval	10 minutes

Default is to poll switches/controllers /IAP/etc every 60 minutes

Quick Review of Discovered Endpoints



Update Network Scan to be Scheduled

aruba ClearPass Policy Manager Menu

Configuration » Profile and Network Scan » Network Scan

Network Scan + Start Scan

Configure Network Scans by adding the configurations (SNMP, SSH, or WMI) needed to query all the devices in the target network, as well as schedule a network scan or a subnet scan.

Filter: Type

#	Zone
1.	<input checked="" type="checkbox"/> default
2.	<input type="checkbox"/> default
3.	<input type="checkbox"/> default
4.	<input type="checkbox"/> default

Schedule Scan

Scan Type: ☒ Network Scan ☐ Subnet Scan

Zone: default

Seed Devices (CSV): 192.168.137.90,192.168.137.99,192.168.137.254

Frequency of Scan: Daily

Start Time of Scan: 00:00

Scan Depth: 3

Probe ARP entries: ☒ Probe all the ARP entries found to discover devices

WARNING: Performing network scans can be resource intensive and time consuming. For large networks, scans could take more than an hour and ideally should be done on a ClearPass node that is not servicing core authentications, or should be done outside of normal business hours.

Save Cancel

Show 20 records

Schedule	Status
Probe ARP enabled. On Demand	✓

Defined all the seed routers

Hourly, Daily, Weekly

Quiet time for scan

Create Scheduled Subnet Scan

aruba ClearPass Policy Manager

Configuration » Profile and Network Scan » Network Scan

Network Scan

Configure Network Scans by adding the configurations (SNMP, SSH, or WMI) needed to query all the devices in the target network, as well as schedule a network scan or a subnet scan.

Filter: Type

Show 20 records

Schedule Scan

Scan Type: ☐ Network Scan ☒ Subnet Scan

Zone: default

IP Subnet(s): 10.137.10.100/32

Frequency of Scan: Daily

Start Time of Scan: 22:30

Save Cancel

Defined a Subnet scan for interested networks

Scan is network intensive – run at quiet time

#	Zone	Schedule	Status
1.	default		✓
2.	default		✗
3.	default		✓
4.	default		✓
5.	default		✓
6.	default		✓
7.	Europe		✓
8.	Europe		✓

Look at Endpoint Details

aruba

Configuration » Identity » Endpoints

Endpoints

This page automatically lists all authenticated endpoints. An endpoint device is an internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).

Filter: MAC Address contains [] Go Clear Filter

Show 20 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	000c29325d18		Server	VMWare	Known	Yes
2.	000c298df655		Generic	Generic	Known	Yes
3.	000c29b4347a	cpm.hpearubademo.com	Server	ClearPass	Unknown	Yes
4.	000c29b43484		Generic	Generic	Unknown	Yes
5.	001a1e084bc6	Team1 IAP	Access Points	Aruba	Known	Yes
6.	0028f8676871	shatviel602	Computer	Windows	Known	Yes
7.	008701944e3b	galaxy-j5-2016	SmartDevice	Android	Known	Yes
8.	0260f4a3e1db	admin	Computer	Windows	Known	Yes
9.	04d6aa5e6cfb	galaxy-note8	SmartDevice	Android	Known	Yes
10.	1002b5b9a091	waltersn1	Computer	Windows	Known	Yes

Endpoint Attributes Device Fingerprints

MAC Address: 008701944e3b IP Address: 192.168.137.118

Description: Static IP: FALSE

Hostname: galaxy-j5-2016

Status: ☒ Known client ☐ Unknown client ☐ Disabled client

Device Category: SmartDevice

Device OS Family: Android

Device Name: Samsung Android

MAC Vendor: Samsung Electronics Co.,Ltd

Added by: Policy Manager

Online Status: Not Available

Connection Type: Wireless

Access Point: TeamX

Network SSID: TeamX-Corp

Feb 15, 2018 09:45:52 GMT

7 BST

What the device has been profiled as

The fingerprint

Endpoint Fingerprint Details

DHCP Option60: android-dhcp-7.1.1

DHCP Options: 53,61,50,54,57,60,12,55

DHCP Option55: 1,3,6,15,26,28,51,58,59,43

Export Delete

airhe TECH T

#ArubaAirheads 51

Only Known Devices Should Connect

- Unknown devices are potential risk
 - Should these be connected?
 - What are they
- Pulling any existing asset database – MAC address based
 - Configure MDM
 - Import existing network audits/CMDB
 - Use <https://ase.arubanetworks.com/solutions/id/91>

Import Insight Enhanced Endpoint Audit Report

aruba ClearPass Insight

TOTAL AUTH 0 FAILED AUTH 0 UNIQUE ENDPOINTS 0 UNIQUE USERS 0

ALERTS 0 Menu

Search using Username/Endpoint/ClearPass Server/Network Device

Dashboard
Inventory
Reports
Configuration
Custom Reports
Alerts
Administration

Import Custom Report template

Select file to import

Browse... 20190122-32910-Enhancement.signed.tar Import

This custom report is embedded in the supplied deployment document

Custom Reports

#	REPORT TITLE
No data available in table	

20 per page

Page: Go < >

Two reports templates appear

Custom Reports		
#		REPORT TITLE
1	<input type="radio"/>	Updated Endpoints Report
2	<input type="radio"/>	Not Updated Endpoints Report

Hold it! Where can I get this template?

- Should be part of ClearPass at some point
- Till then, we need to find a proper distribution location still
- Please contact me and I can share it.

Create Endpoints Audit Report

aruba ClearPass Insight

TOTAL AUTH 0 FAILED AUTH 0 UNIQUE ENDPOINTS 0 UNIQUE USERS 0

ALERTS 0 Menu

Search using Username/Endpoint/ClearPass Server/Network Device

1 report(s) deleted successfully

Dashboard
Inventory
Reports
Configuration
Custom Reports
Alerts

Configured Reports

Import report Create New Report

Create New Report

What would you like to see in your new Report?

Report Name
Endpoint Audit Report

Description
Report all endpoints that have been updated in the scheduled period

Category
Custom
Not Updated Endpoints Report
Updated Endpoints Report

Notifications
Notify by Email
derin.mellor@hpe.com
Notify by SMS

Options
☒ Include raw data in output
This is an executive report which includes pre-defined CSV columns
☐ Enable remote copy
Configure the Remote Directory in the Administration section to specify the remote copy destination.

Repeat Scheduled Report
Weekly
Repeat On
Monday
Hour of the day
04

Save

#ArubaAirheads 55

Create Missing Endpoints Audit Report

The screenshot shows the Aruba ClearPass Insight interface. The top navigation bar includes the Aruba logo, 'ClearPass Insight', and status indicators for 'TOTAL AUTH' (0) and 'FAILURES' (0). A search bar is located on the right. The left sidebar contains a menu with 'Dashboard', 'Inventory', 'Reports', 'Configuration' (highlighted), 'Custom Reports', and 'Alerts'. A notification at the top left states '1 report(s) deleted successfully'.

The main content area is titled 'Configured Reports'. It features two buttons: 'Import report' and 'Create New Report', with a red arrow pointing to the latter. An orange callout box explains: 'This will report all the endpoints that have not been seen for over a month – assuming the Insight logging is set to >30 days'.


The 'Create New Report' modal is open, showing the following fields:

- Report Name:** 'Derin Missing Endpoints' (with a red arrow pointing to the text input).
- Description:** 'Reports all the endpoints that have not been seen in the last month' (with a red arrow pointing to the text input).
- Category:** 'Custom > Not Updated Endpoints Report' (with a red arrow pointing to the dropdown menu).
- Notifications:** Includes a checked 'Notify by Email' option with the email address 'derin.mellor@hpe.com' (with a red arrow pointing to the email input), and an unchecked 'Notify by SMS' option.
- Options:** Includes a checked 'Include raw data in output' option (with a red arrow pointing to the checkbox) and an unchecked 'Enable remote copy' option. A red note states: 'This is an executive report which includes pre-defined CSV columns' and 'Configure the Remote Directory in the Administration section to specify the remote copy destination.'


At the bottom of the modal, there are three dropdown menus: 'Repeat Scheduled Report' (set to 'Monthly'), 'Day of the month' (set to '12'), and 'Hour of the day' (set to '01'). A red arrow points to the 'Monthly' option. A 'Save' button is located at the bottom right, with an orange callout box pointing to it that says 'Click on to the Save button'.

The bottom left corner features the 'airheads TECH TALK LIVE' logo. The bottom right corner shows the page number '56'.


Insight Endpoint Reports

 ClearPass Insight

TOTAL AUTH 0 FAILED AUTH 0 UNIQUE ENDPOINTS 0 UNIQUE USERS 0

ALERTS 0 Menu 

Search using Username/Endpoint/ClearPass Server/Network Device

 Report Missing Endpoints saved successfully

Dashboard

Inventory

Reports

Configuration

















Custom Reports





Alerts




Administration

Configured Reports

Import report Create New Report

Configuration							
#		NAME	DESCRIPTION	TEMPLATE	ENABLE		
1		Endpoint Audit Report	Report all endpoints that have been updated in the scheduled period	Updated Endpoints Report	ENABLED 	     	
2		Missing Endpoints	Reports all the endpoints not seen in the scheduled period	Not Updated Endpoints Report	ENABLED 	     	

20  page  Error  In Progress  Completed

Page:   

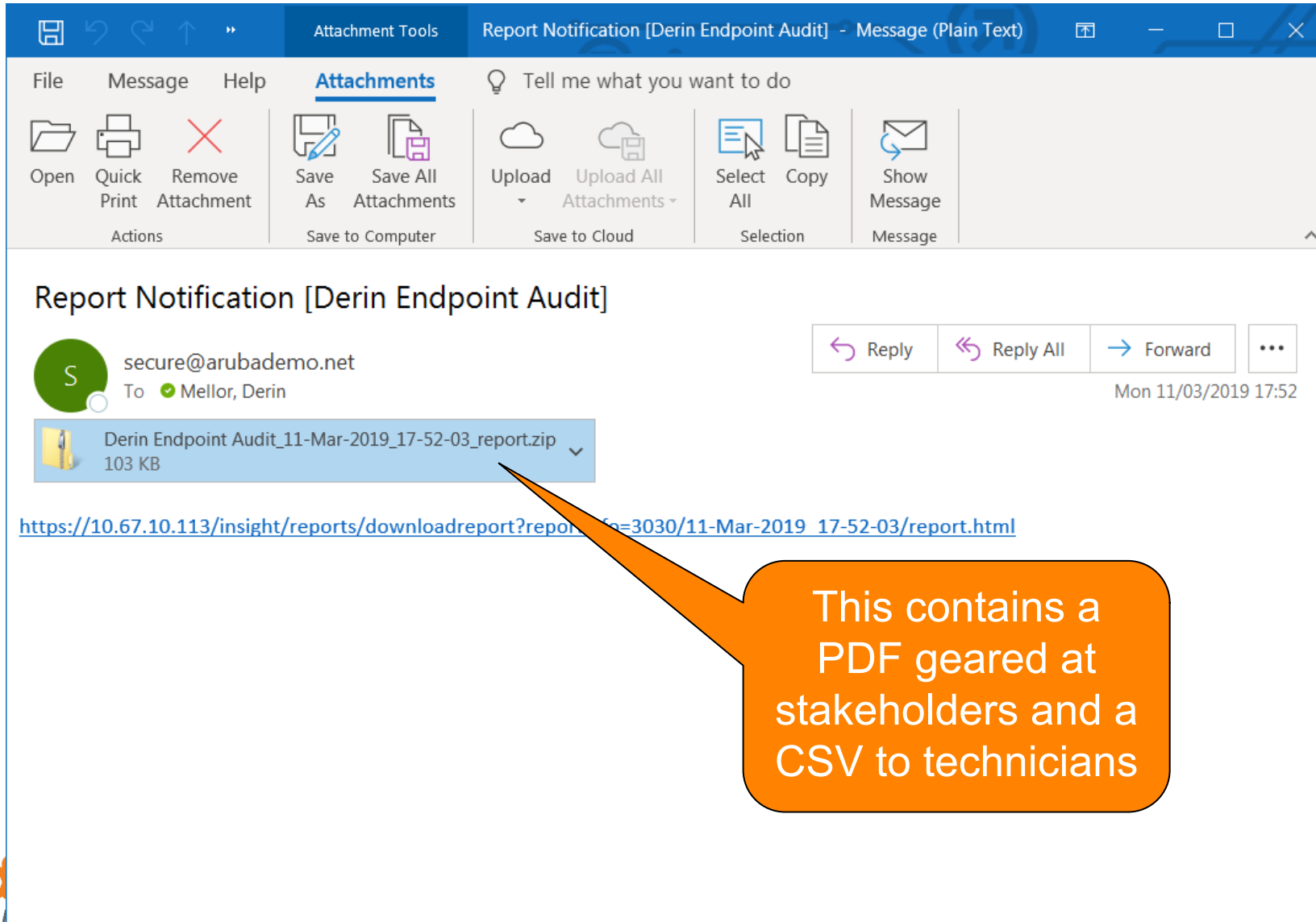
These reports are waiting for the schedule period

To manually run this report click this button

Wait for the scheduled report...



Endpoint Audit Report



The screenshot shows an email client window titled "Report Notification [Derin Endpoint Audit] - Message (Plain Text)". The ribbon includes "File", "Message", "Help", and "Attachments". The "Attachments" tab is active, showing icons for "Open", "Quick Print", "Remove Attachment", "Save As", "Save All Attachments", "Upload", "Upload All Attachments", "Select All", "Copy", and "Show Message". The email content shows a message from "secure@arubademo.net" to "Mellor, Derin" dated "Mon 11/03/2019 17:52". The attachment is "Derin Endpoint Audit_11-Mar-2019_17-52-03_report.zip" (103 KB). Below the attachment is a URL: https://10.67.10.113/insight/reports/downloadreport?reportId=3030/11-Mar-2019_17-52-03/report.html. An orange callout bubble points to the attachment with the text: "This contains a PDF geared at stakeholders and a CSV to technicians".

Report Notification [Derin Endpoint Audit]

secure@arubademo.net
To: Mellor, Derin

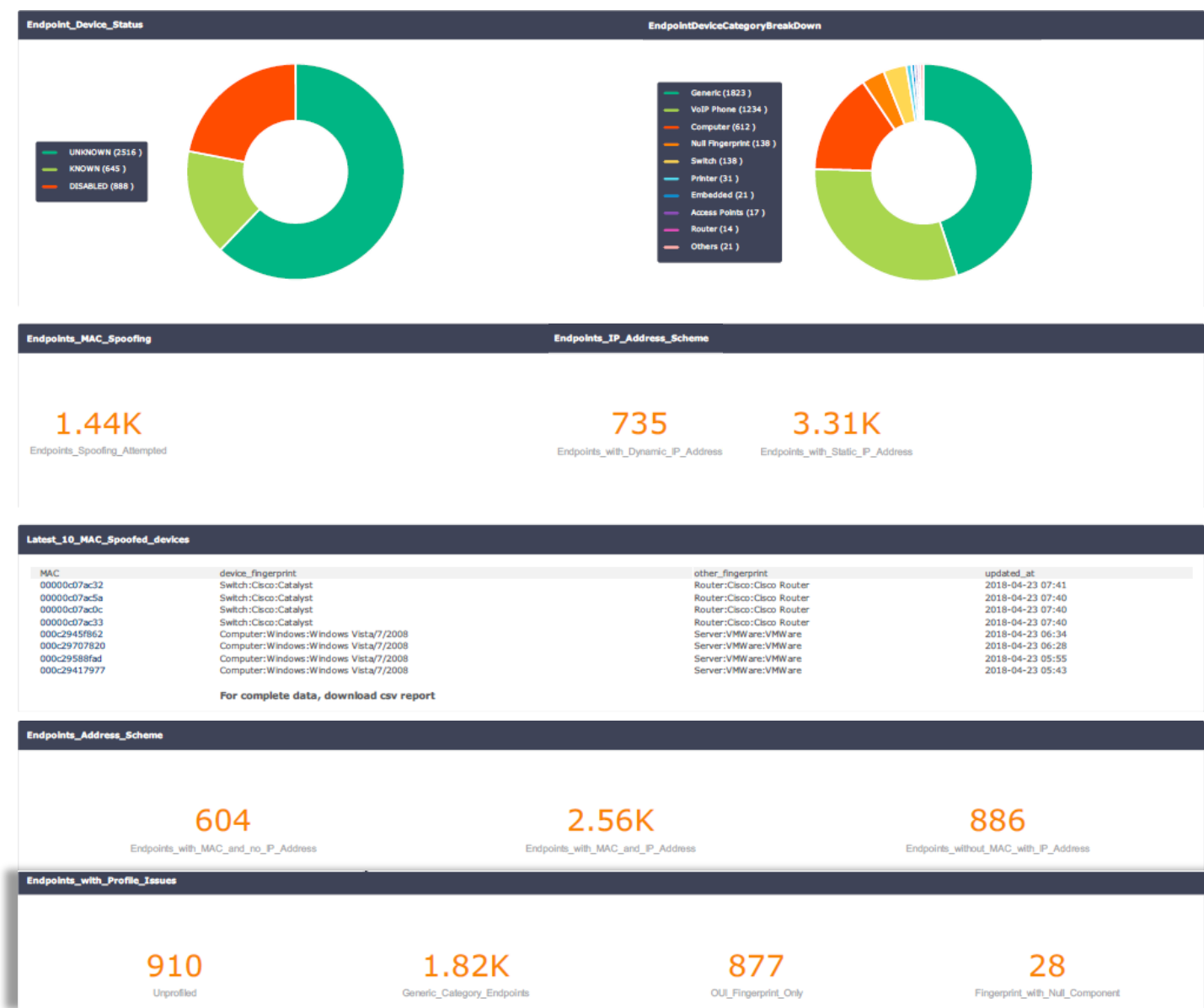
Mon 11/03/2019 17:52

Derin Endpoint Audit_11-Mar-2019_17-52-03_report.zip
103 KB

https://10.67.10.113/insight/reports/downloadreport?reportId=3030/11-Mar-2019_17-52-03/report.html

This contains a PDF geared at stakeholders and a CSV to technicians

PDF Stakeholder Report



Detailed CSV Endpoint Report

	status	macaddress	nas_ip	nas_name	nas_location	med	wired_port	ssid	ap	mac_vendor	ip	is_static	hostname	device_category	device_family	device_name	spoofed	fingerprint
6854	Unknown	000e101971fe'	10.218.196.134	JS0649_iAP	Camden	Wifi		Linbury	JS0649_	C-guys, Inc.	10.218.198.251	FALSE	wlp8a801058	Generic	C-guys	Unclassified Device	FALSE	{"dhcp": {"options":
6855	Unknown	000e10197220'	10.220.20.134	JS0007_iAP	Eltham	Wifi		Linbury	JS0007_	C-guys, Inc.	10.220.22.143	FALSE	wlp8a800858	Generic	C-guys	Unclassified Device	FALSE	{"dhcp": {"options":
6856	Unknown	000e10197268'	10.190.39.158	JS4484_iAP	Wandsworth E	Wifi		Linbury	JS4484_	C-guys, Inc.	10.190.39.209	FALSE	wlp8a800936	Generic	C-guys	Unclassified Device	FALSE	{"dhcp": {"options":
6857	Unknown	000e10197297'								C-guys, Inc.	10.228.174.229	FALSE	wlp8a801070	Generic	C-guys	Unclassified Device	FALSE	{"dhcp": {"options":
6858	Unknown	000e101972ae'	10.235.148.135	JS2258_WLC02_3200	Wakefield	Wifi		Linbury	JS2258_	C-guys, Inc.	10.235.150.147	FALSE	wlp8a801067	Generic	C-guys	Unclassified Device	FALSE	{"dhcp": {"options":
6859	Unknown	000e7f3c1ade'	10.236.128.12	JS_JS2037-0G-M-01-C296-2		Wired	FastEthernet0/3				10.236.128.79	TRUE					FALSE	{}
6860	Unknown	000e7fad16e0'	10.152.1.121	BC0001_B2_3750X_S01		Wired	GigabitEthernet3/0/2					TRUE					FALSE	{}
6861	Unknown	000e7faedeb8'	10.152.1.121	BC0001_B2_3750X_S01		Wired	GigabitEthernet3/0/2					TRUE					FALSE	{}
6862	Unknown	000e7fdf9ec3'	10.228.224.11	JS_JS0814-0G-M-01-C296-1		Wired	FastEthernet0/2				10.228.224.72	TRUE					FALSE	{}
6863	Unknown	000e7fe39f08'	10.242.96.11	JS_JS2057-0G-M-01-C296-1		Wired	FastEthernet0/11				10.242.96.79	TRUE					FALSE	{}
6864	Unknown	000ec6cd1262'	10.155.1.21	BC0004-Z02-CS3850-SW01		Wired	GigabitEthernet3/0/40			ASIX ELECTRON	10.155.28.228	FALSE	walsnt81004	Computer	Windows	Windows 8/10	FALSE	{"dhcp": {"options":

Validating Endpoints

- Unknown devices: status = Unknown
 - These devices need to be validated
- Disabled devices: status = Disabled
 - Why are these devices still connected to the network?
- IP only
 - Devices that have been found by subnet scan
 - No associated MAC address
 - ARP table scanning issue?
- Static IP
 - Is this a legitimate device with a static IP?
 - If not why is ClearPass not seeing the DHCP Request?
- No IP
 - Possibly an indication that ClearPass is not polling the correct ARP table

Validating Profiles

- Generic category
 - Identify the device type and create custom fingerprint for these devices
 - Feed this information (device type, category and fingerprint) back to Aruba TAC
- Unprofiled
 - DHCP Requests are not being relayed to ClearPass
 - Device has a static IP – ie no DHCP
 - Active scanning is not scanning that network
 - Firewall is blocking the active scans
 - Device is transient and was not connected during active scan
- OUI fingerprint only
 - Device has been scanned but reported no fingerprint – is this correct?
- NULL fingerprints component
 - Possible indication of SNMP/WMI/SSH credential issue
- Spoof detected

Importing Updated Endpoints

- Use the ASE Batch Import to convert this CSV into a suitable XML import file
 - <https://ase.arubanetworks.com/solutions/id/91>

ClearPass Benefits

– Real-time Visibility, Control and Responses

- NO GAPS
- NO AGENTS
- Multivendor Wired and Wireless Security Solution



– Fully Featured

- Built in Fingerprinting and Profiling
- Automated BYOD solution
- Built in Secure and Public Guest Solution
- Concurrent User Licensing
- Over 120 Security Vendor Partners



– Automates Secure Connectivity

- Reduces fragmentation
- Speeds up incident response



airheads

TECH TALK *LIVE*

Thank You