Table of Contents

ClearPass Profile 1
Setup 1
Device Profile 2
Collectors 2
- DHCP 3
- ClearPass Onboard 3
- HTTP User-Agent 3
- MAC OUI 5
- ActiveSync plugin 5
- CPPM OnGuard 8
- SNMP [Introduced in CPPM 5.2] 8
- Subnet Scanner [Introduced in CPPM 5.2] 9

Profiling 10
- Stage 1 10
- Stage 2 10

Post Profile Actions 11
Conflicts 12
Fingerprint Dictionaries 13
Profile UI 15
Profile APIs 18
- Post endpoint attributes for profiling 18
- Get endpoint by MAC or IP address 19

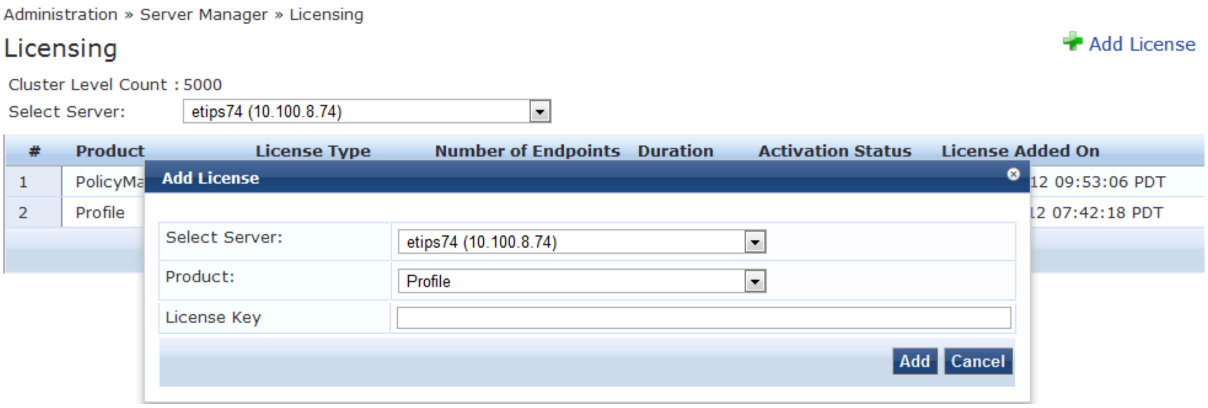
ClearPass Profile

Profile is a ClearPass module that automatically classifies endpoints using attributes obtained from ClearPass software components called Collectors. It can be used to implement BYOD flows where access has to be controlled based on the type of the device and the identity of the user. Setting up Profile in a network requires a minimal amount of configuration.

Setup

To classify devices using Profile, the following needs to be configured:

- **Add Profile license**. Navigate to: Administration » Server Manager » Licensing. Select "Profile" from the product dropdown menu



Administration » Server Manager » Licensing

Licensing

Cluster Level Count : 5000

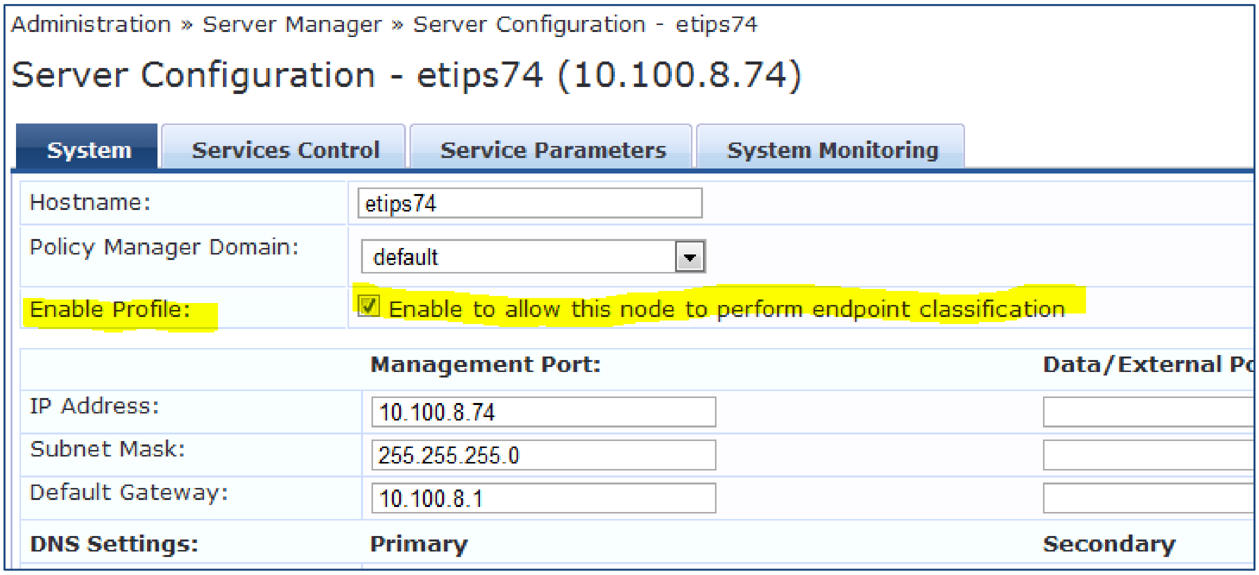
Select Server: etips74 (10.100.8.74)

#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On
1	PolicyMa					12 09:53:06 PDT
2	Profile					12 07:42:18 PDT

Add License

Select Server:	etips74 (10.100.8.74)
Product:	Profile
License Key	

- **Select one of the CPPM nodes in the same Zone as the profiler**. Navigate to Administration » Server Manager » Server Configuration. You should only select one Profile node per ClearPass Policy Manager (CPPM) Zone.



Administration » Server Manager » Server Configuration - etips74

Server Configuration - etips74 (10.100.8.74)

Hostname:	etips74	
Policy Manager Domain:	default	
Enable Profile:	☑ Enable to allow this node to perform endpoint classification	
	Management Port:	**Data/External Po**
IP Address:	10.100.8.74	
Subnet Mask:	255.255.255.0	
Default Gateway:	10.100.8.1	
DNS Settings:	**Primary**	**Secondary**

- **Configure collectors to send data to profiler.** Refer to Collectors section for more information.

Once devices are classified, you can use them in policies to control access within your network. You can use the *Authorization:[Endpoints Repository]* attributes in the CPPM Role Mapping Policy.

See section titled “Endpoint Profile Store as Authorization Source” for more information.

Device Profile

A device profile is a hierarchical model consisting of 3 elements - *DeviceCategory, DeviceFamily,* and *DeviceName* derived by Profile from endpoint attributes.

- *DeviceCategory* – This is the broadest classification of a device. It denotes the type of the device.
  Example: Computer, Smartdevice, Printer, Access Point, etc.

- *DeviceFamily* – This element classifies devices into a category; this is organized based on the type of OS or type of vendor.
  Example: Windows, Linux, Mac OS X are some of the families when category is Computer.
  Apple, Android are examples of DeviceFamily when category is SmartDevice.

- *DeviceName* - Devices in a family are further organized based on more granular details such as version.
  Example: Windows 7, Windows 2008 server are device names under Windows family.

This hierarchical model provides a structured view of all endpoints accessing the network.

Apart from these, Profile also collects and stores:

- IP Address
- Hostname
- MAC Vendor
- Timestamp when device was first discovered
- Timestamp when device was last seen

Collectors

Collectors are network elements that provide data to profile endpoints. The following collectors send endpoint attributes to Profile:

- DHCP
- ClearPass Onboard
- HTTP User-Agent
- MAC OUI – Acquired via various authentication mechanisms such as 802.1X, MAC authentication, etc.

- ActiveSync plugin
- CPPM OnGuard
- SNMP
- Subnet Scanner

- **DHCP**

DHCP attributes such as option55 (parameter request list), option60 (vendor class) and options list from DISCOVER and REQUEST packets can uniquely fingerprint most devices that use the DHCP mechanism to acquire an IP address on the network. Switches and controllers can be configured to forward DHCP packets such as DISCOVER, REQUEST and INFORM to CPPM. These DHCP packets are decoded by CPPM to arrive at the device category, family, and name. Apart from fingerprints, DHCP also provides hostname and IP address.

Configuring the Aruba Controller and Cisco Switch to Send DHCP Traffic to CPPM

```
interface <VLAN_NAME>
ip address <IP_ADDR> <NETMASK>
ip helper-address <DHCP SERVER IP>
ip helper-address <CPPM IP>
end
 -
```

Notice how multiple ‘ip helper-address’es can be configured to send DHCP packets to servers other than the DHCP server.

- **ClearPass Onboard**

ClearPass Onboard collects rich and authentic device information from all devices during the onboarding process. Onboard then posts this information to Profile via the Profile API. Since the information collected is definitive, Profile directly classifies these devices into their Category, Family and Name, without having to rely on any other fingerprinting information.

- **HTTP User-Agent**

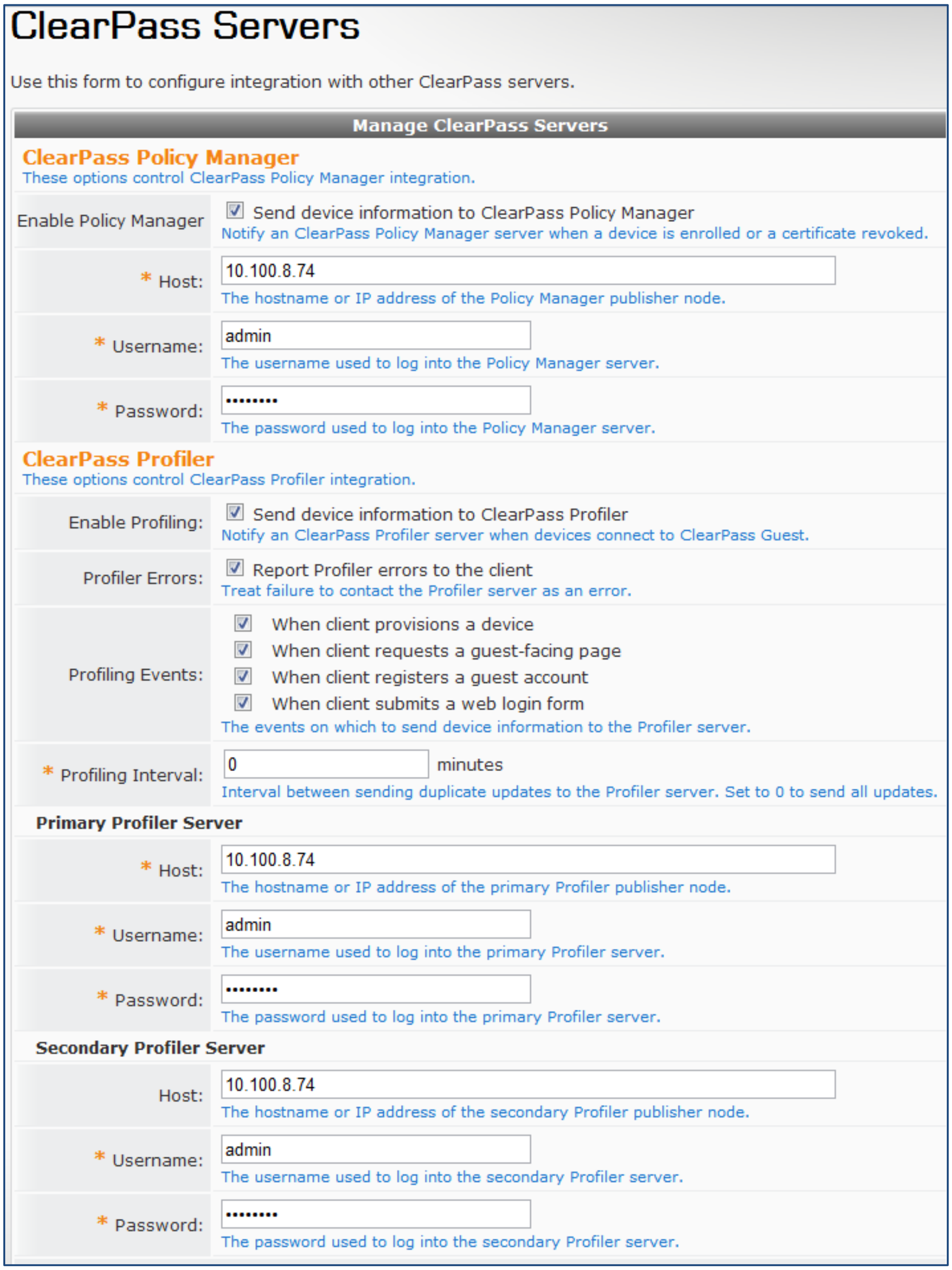
In some cases, DHCP fingerprint alone cannot fully classify a device. A common example is the Apple family of smart devices; DHCP fingerprints cannot distinguish between an Apple iPad and an iPhone. In these scenarios, User-Agent strings sent by browsers in the HTTP protocol are useful to further refine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

User-Agent strings are collected from:

- ClearPass Guest (Amigopod)
- ClearPass Onboard (Amigopod 3.9)
- Aruba controller through IF-MAP interface (future)

Configuration

Navigate to Administrator >> Network Setup >> ClearPass to configure ClearPass Onboard and ClearPass Guest to send HTTP User Agent string to Profile. The screenshot below shows how the CPPM publisher and Profile nodes are configured within Guest/Amigopod .



ClearPass Servers

Use this form to configure integration with other ClearPass servers.

Manage ClearPass Servers

ClearPass Policy Manager
These options control ClearPass Policy Manager integration.

Enable Policy Manager	☑ Send device information to ClearPass Policy Manager Notify an ClearPass Policy Manager server when a device is enrolled or a certificate revoked.
* Host:	10.100.8.74 The hostname or IP address of the Policy Manager publisher node.
* Username:	admin The username used to log into the Policy Manager server.
* Password:	•••••••• The password used to log into the Policy Manager server.

ClearPass Profiler
These options control ClearPass Profiler integration.

Enable Profiling:	☑ Send device information to ClearPass Profiler Notify an ClearPass Profiler server when devices connect to ClearPass Guest.
Profiler Errors:	☑ Report Profiler errors to the client Treat failure to contact the Profiler server as an error.
Profiling Events:	☑ When client provisions a device ☑ When client requests a guest-facing page ☑ When client registers a guest account ☑ When client submits a web login form The events on which to send device information to the Profiler server.
* Profiling Interval:	0 minutes Interval between sending duplicate updates to the Profiler server. Set to 0 to send all updates.

Primary Profiler Server

* Host:	10.100.8.74 The hostname or IP address of the primary Profiler publisher node.
* Username:	admin The username used to log into the primary Profiler server.
* Password:	•••••••• The password used to log into the primary Profiler server.

Secondary Profiler Server

Host:	10.100.8.74 The hostname or IP address of the secondary Profiler publisher node.
* Username:	admin The username used to log into the secondary Profiler server.
* Password:	•••••••• The password used to log into the secondary Profiler server.

- **MAC OUI**

Mac OUI can be useful in some cases to better classify endpoints. An example is Android devices, where DHCP fingerprints can only classify a device as a generic Android device, but it cannot provide more detail about vendor. Combining this information with MAC OUI, Profile can classify a device as HTC Android, Samsung Android, Motorola Android, etc. MAC OUI is also useful to profile devices such as printers which may be configured with static IP addresses.

- **ActiveSync plugin**

ActiveSync plugin is a Windows Service component (that is, it runs as a service on the Exchange server) provided by Aruba to be installed on Microsoft Exchange servers. When a device communicates with the corporate Exchange Server using the ActiveSync protocol, it provides attributes such as device type and user agent. These attributes are collected by the plugin software and are sent to CPPM Profile. Profile uses dictionaries to derive profiles from these attributes.

Configuration

Installation

1. The plugin is packaged as ArubaMSExchangePlugin.zip. This containes two files:
    a. setup.exe
    b. MSExchangePlugin.msi
2. Extract and copy both files on Microsoft Exchange Server 2010
3. Double click on "setup.exe" and install the Aruba MSExchange Plugin

Installation Folders

The plugin gets installed under "C:\Program Files\ArubaNetworks\" on 32-bit systems, and under "C:\Program Files (x86)\ArubaNetworks" on 64-bit systems. Folder structure is:

- $install_root\bin ==> Contains binaries of MSExchange Plugin
- $install_root\etc ==> Contains configuration files
- C:\ArubaNetworks\MSExchangePlugin\data ==> Contains ActiveSync plugin records which are periodically collected by the plugin
- C:\ArubaNetworks\MSExchangePlugin\var ==> Contains plugin log files

Configuration Files

1. IIS log reader configuration file:
   Location: $install_root\etc\iislogreader.conf

The content of the configuration file are pasted below:

```
[iis-log-config]
  logDir=C:/inetpub/logs/LogFiles/W3SVC1

  ####################################################
  # If advanced logging is enabled then make sure you
  # specify the path for advanced logging files
  # in the logDir variable
  ###################################################
  advancedLogging=0

  ####################################################
  # Read interval in seconds
  ####################################################
  readInterval=300

  ####################################################
  # Refresh interval for active sync records
  ####################################################
  refreshInterval=14400
```

2. ActiveSync log record configuration file:
   Location: $install_root\etc\logrecord.conf

The content of the configuration file are pasted below:

```
[log-record-config]
########################################################
# This is the data directory where the ActiveSync records
# are stored prior to sending it to Profile
########################################################
dataDir=C:/ArubaNetworks/MSExchangePlugin/var/data

[log-dispatcher-config]

########################################################
# This is the Profile URL and login credentials
########################################################
url=http://<profile-ipaddress>/async_netd/deviceprofiler/endpoints
username=any
password=any
```

3. MSExchange Plugin configuration file:
   Location: $install_root\etc\msexchange-plugin.conf

The content of the configuration file are pasted below:

```
    [domain-controller-info]

    ########################################################
    # AD domain controller name
    ########################################################
    serverName=WIN2008R2DEV-AD.dev.avendasys.com

    ########################################################
    # AD domain controller base dn
    ########################################################
    baseDn=dc=dev,dc=avendasys,dc=com

    ########################################################
    # AD domain authentication source name
    ########################################################
    authSourceName=

    ########################################################
    # AD domain bind dn
    ########################################################
    bindDn=cn=Administrator,cn=Users,dc=dev,dc=avendasys,dc=com

    ########################################################
    # AD domain bind password
    ########################################################
    bindPassword=password

    ########################################################
    # Filter configuration
    ########################################################
    userFilter=(&(objectClass=user)(sAMAccountName=%s))
    groupFilter=(&(objectClass=group)(member=%s))
    deviceFilter=(&(objectClass=top)(objectClass=msExchActiveSyncDevice))

    ########################################################
    # Attributes to fetch
    ########################################################

attributes=distinguishedName,msExchDeviceID,msExchDeviceModel,msExchDeviceTyp
e,msExchDeviceUserAgent
```

Note: Any configuration file changes above require the restart of Aruba MSExchange Plugin service.

- **CPPM OnGuard**

ClearPass OnGuard agents perform advanced endpoint posture assessment. It collects and sends OS details from endpoints during authentication. Profile uses os_type attribute from OnGuard to derive a profile. For example, a Device Name of Windows XP can be further classified as Windows XP Service Pack 3.

- **SNMP [Introduced in CPPM 5.2]**

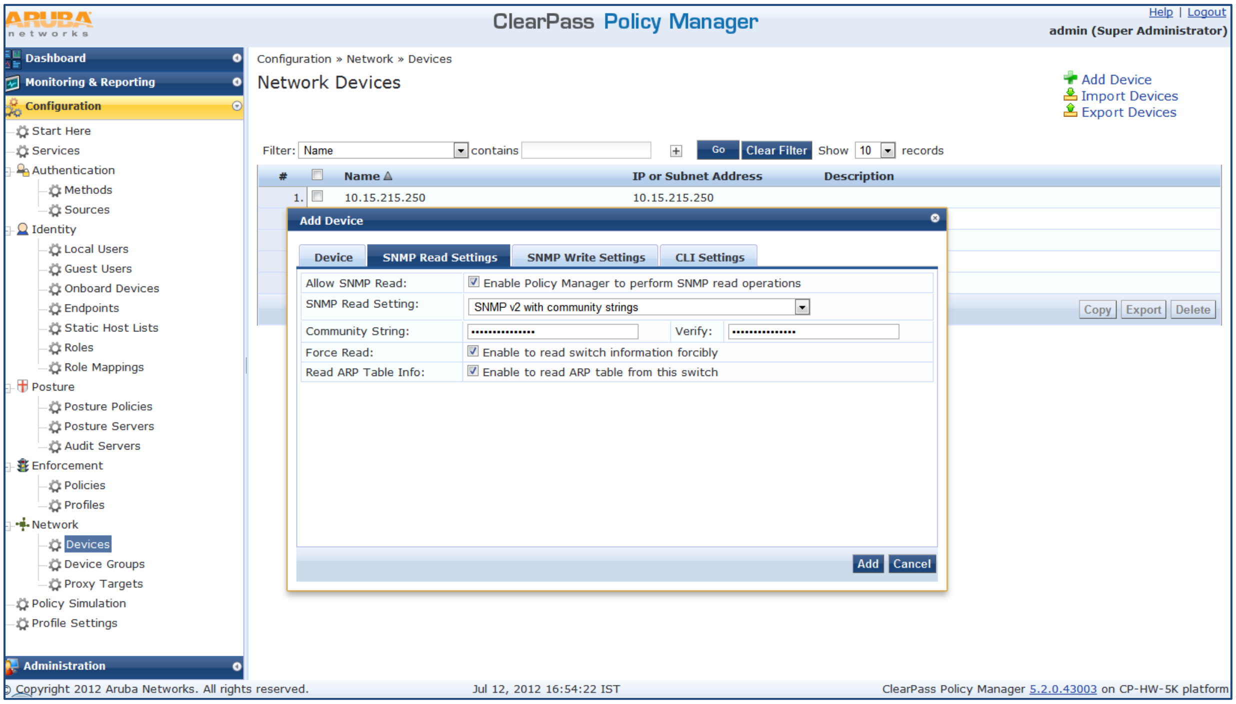
Endpoint information obtained by reading SNMP MIBs of network devices is used to discover and profile static IP devices in the network. The following information read via SNMP is used:

- **sysDescr** information from RFC1213 MIB is used to profile the device. This is used both for profiling switches/controllers/routers configured in CPPM, and for profiling printers and other static IP devices discovered through SNMP or subnet scans.
- **cdpCacheTable** information read from CDP (Cisco Discovery Protocol) capable devices is used to discover neighbour devices connected to switch/controller configured in CPPM
- **lldpRemTable** information read from LLDP (Link Layer Discovery Protocol) capable devices is used to discover and profile neighbour devices connected to switch/controller configured in CPPM
- **ARP table** read from network devices is used as a means to discover endpoints in the network.

Note that the SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with “public” community string.

Network Devices configured with SNMP Read enabled are polled periodically for updates based on the time interval configured in ***Administration -> Server Configuration -> Service Parameters -> ClearPass network services -> Device Info Poll Interval.***

Screenshot on following page.



#	Name	IP or Subnet Address	Description
1.	10.15.215.250	10.15.215.250	

Allow SNMP Read:	☑ Enable Policy Manager to perform SNMP read operations
SNMP Read Setting:	SNMP v2 with community strings
Community String:	•••••••••••••••• Verify: ••••••••••••••••
Force Read:	☑ Enable to read switch information forcibly
Read ARP Table Info:	☑ Enable to read ARP table from this switch

Copyright 2012 Aruba Networks. All rights reserved. Jul 12, 2012 16:54:22 IST ClearPass Policy Manager 5.2.0.43003 on CP-HW-5K platform

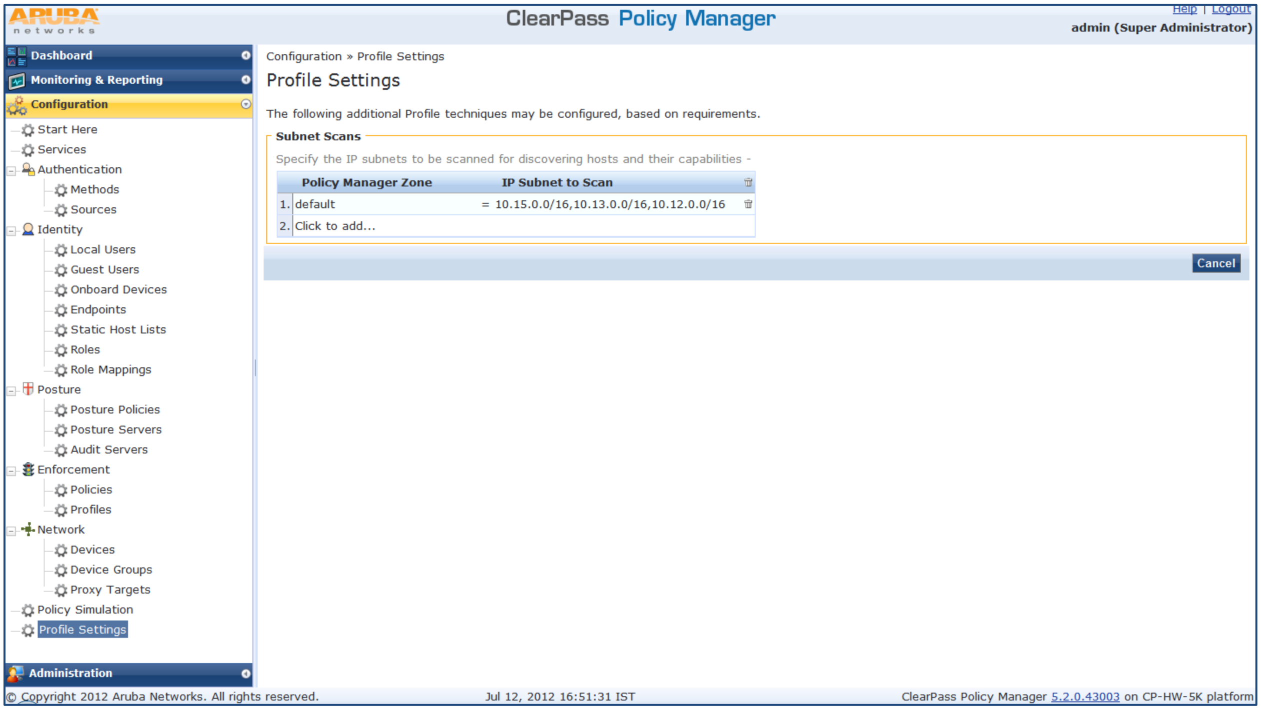
The following additional settings have been introduced for Profiling support:

1. **Read ARP Table Info** – Enable this setting if this is a L3 device and you want to use ARP table on this device as a way to discover endpoints in the network. Static IP endpoints discovered this way are further probed via SNMP to profile the device.
2. **Force Read** – Enable this to ensure all CPPM nodes in the cluster read SNMP information from this device irrespective of trap configuration on the device. This option is especially useful when demonstrating static IP based device profiling, since this does not require any trap configuration on the network device.

3. In large or geographically spread cluster deployments you do not want all CPPM nodes to probe all SNMP configured devices. The default behavior is for a CPPM node in the cluster to read network device information only for devices configured to send traps to that CPPM node.

- **Subnet Scanner [Introduced in CPPM 5.2]**

Network subnet scan is used to discover IP addresses of devices in the network. The devices discovered this way are further probed using SNMP to fingerprint and assign a Profile to the device.
Network subnets to scan and periodicity of scan is configured in Profile Settings screen. Subnets to scan are configured per CPPM Zone. This is particularly useful in deployments that are geographically distributed. In such deployments, it is recommended that you assign the CPPM nodes in a cluster to multiple "Zones" (from Administration -> Server Configuration -> Manage Policy Manager Zones) depending on the geographical area served by that node, and enable Profile on atleast one node per zone.



Configuration » Profile Settings

Profile Settings

The following additional Profile techniques may be configured, based on requirements.

Subnet Scans

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

	Policy Manager Zone		IP Subnet to Scan
1.	default	=	10.15.0.0/16,10.13.0.0/16,10.12.0.0/16
2.	Click to add...		

© Copyright 2012 Aruba Networks. All rights reserved. Jul 12, 2012 16:51:31 IST ClearPass Policy Manager 5.2.0.43003 on CP-HW-5K platform

Profiling

Profile uses a two-stage approach to classifying endpoints using input attributes.

- **Stage 1**

Stage 1 tries to derive device profiles using static dictionary lookups. Based on the attributes available, CPPM looks up DHCP, HTTP, ActiveSync and MAC OUI dictionaries, and derives multiple matching profiles. When there are multiple matches, priority of the source which provided the attribute is used to select the right profile. Listed below are sources in decreasing order of priority:

- Onguard/ActiveSync plugin
- HTTP User-Agent
- DHCP
- MAC OUI

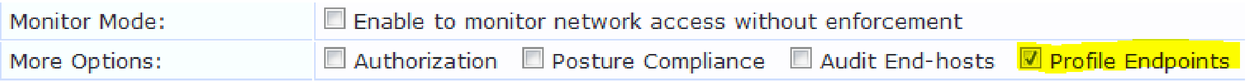
- **Stage 2**

CPPM comes pre-built with a set of rules that evaluates to a device profile. CPPM uses all input attributes and device profiles from Stage 1. The resulting rule evaluation may or may not result in a profile. Stage 2 is intended to refine the results of profiling.
Example:
With DHCP options, Stage 1 can identify that a device is Android. Stage 2 uses rules to combine this with MAC OUI to further classify an Android device as Samsung Android, HTC Android, etc.

Post Profile Actions

After profiling an endpoint, Profile can be configured to perform RADIUS Change of Authorization (CoA) on the NAD to which an endpoint is connected. Post profile rules are configured in the CPPM Service configuration wizard.

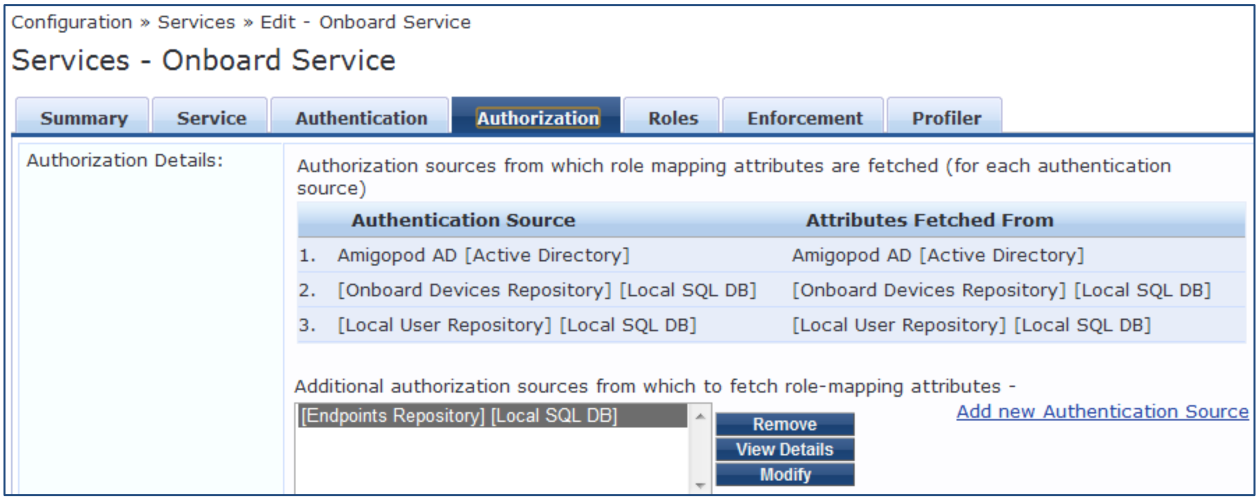
- Make sure you turn on “Profile Endpoints” from the Service tab:



Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts ☑ Profile Endpoints

- Configure [Endpoints Repository] as Authorization Source. Endpoint profile attributes derived by Profile are available through ‘[*Endpoint Repository]*’ authorization source. These attributes can be used in role-mapping or enforcement policies to control network access.

  Available attributes are:
  - *Authorization:[Endpoints Repository]:MAC Vendor*
  - *Authorization:[Endpoints Repository]:Category*
  - *Authorization:[Endpoints Repository]:OS Family*
  - *Authorization:[Endpoints Repository]:Name*



Configuration » Services » Edit - Onboard Service

Services - Onboard Service

Authorization Details:

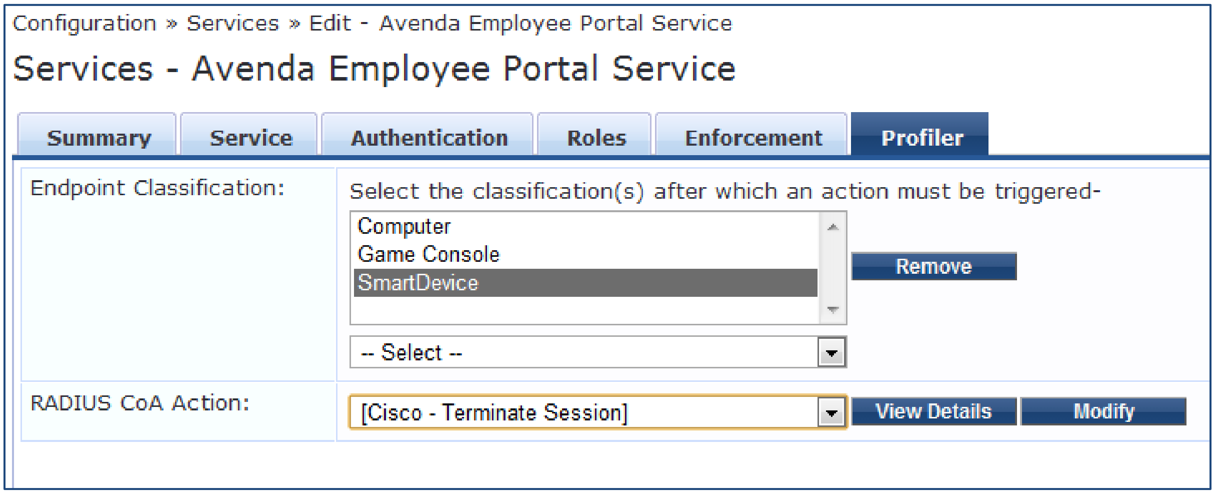
Authorization sources from which role mapping attributes are fetched (for each authentication source)

	Authentication Source	Attributes Fetched From
1.	Amigopod AD [Active Directory]	Amigopod AD [Active Directory]
2.	[Onboard Devices Repository] [Local SQL DB]	[Onboard Devices Repository] [Local SQL DB]
3.	[Local User Repository] [Local SQL DB]	[Local User Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Endpoints Repository] [Local SQL DB]

- You can select a set of categories and a CoA profile to be applied when the profile matches one of the selected categories. CoA is triggered using the selected CoA profile. ANY option from ‘*Endpoint Classification’* can be used to invoke CoA on a change of any one of the fields (category, family, and name).



Configuration » Services » Edit - Avenda Employee Portal Service

Services - Avenda Employee Portal Service

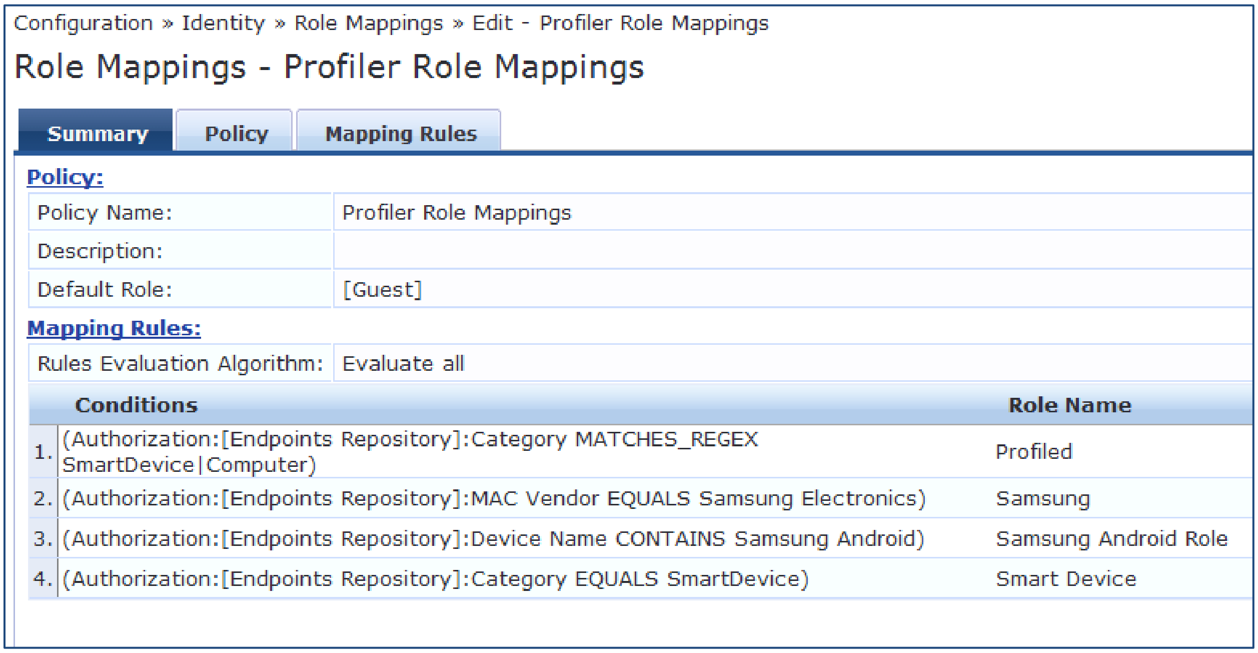
Endpoint Classification: Select the classification(s) after which an action must be triggered-

Computer
Game Console
SmartDevice

-- Select --

RADIUS CoA Action: [Cisco - Terminate Session]

- Use profiled endpoint attributes in Role Mapping Rules



Configuration » Identity » Role Mappings » Edit - Profiler Role Mappings

Role Mappings - Profiler Role Mappings

Policy:

Policy Name:	Profiler Role Mappings
Description:	
Default Role:	[Guest]

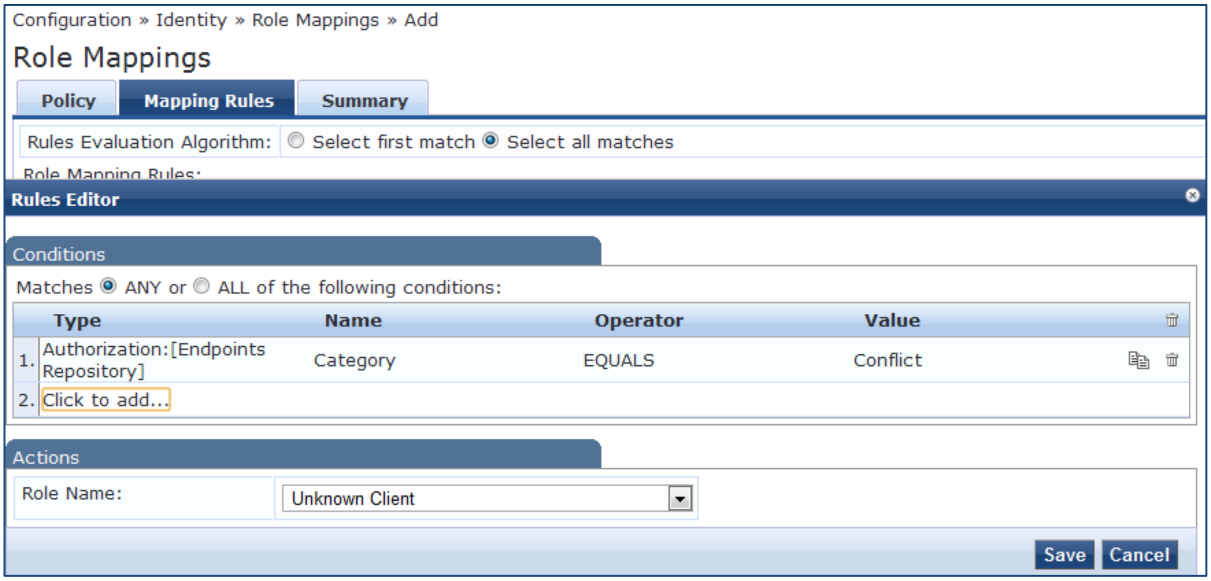
Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Role Name
1.	(Authorization:[Endpoints Repository]:Category MATCHES_REGEX SmartDevice|Computer)	Profiled
2.	(Authorization:[Endpoints Repository]:MAC Vendor EQUALS Samsung Electronics)	Samsung
3.	(Authorization:[Endpoints Repository]:Device Name CONTAINS Samsung Android)	Samsung Android Role
4.	(Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Smart Device

Conflicts

CPPM has the ability to profile devices from many inputs such as DHCP, MAC OUI, HTTP User Agent string, OnGuard, etc. Conflict happens when there is a difference in the information CPPM receives from these multiple sources. In the event that there is a conflict, the DeviceCategory attribute in [Endpoints Repository] authorization source is set as “Conflict”. You can use this as a condition in Role Mapping policy rule to tag a role for limited access.



Configuration » Identity » Role Mappings » Add

Role Mappings

Rules Evaluation Algorithm: ○ Select first match ● Select all matches

Role Mapping Rules:

Rules Editor

Conditions

Matches ● ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authorization:[Endpoints Repository]	Category	EQUALS	Conflict
2.	Click to add...			

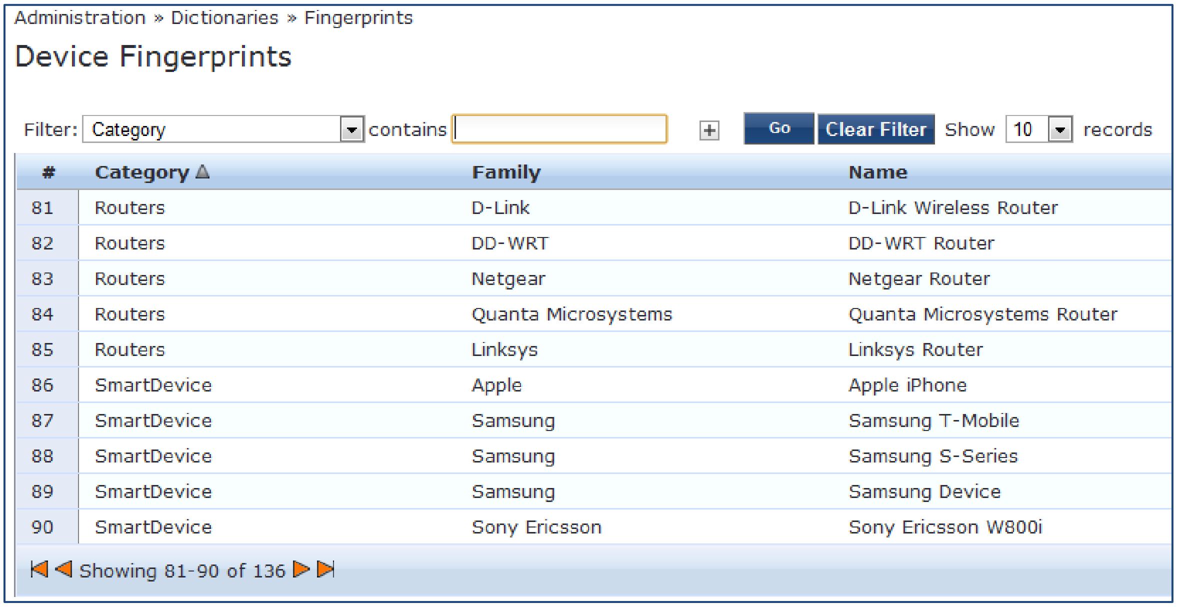
Actions

Role Name: Unknown Client

Fingerprint Dictionaries

CPPM uses a set of dictionaries and built-in rules to perform device fingerprinting. Listed below are the dictionaries used by CPPM.

- DHCP
- HTTP User-Agent
- ActiveSync attributes
- SNMP attributes
- MAC OUI

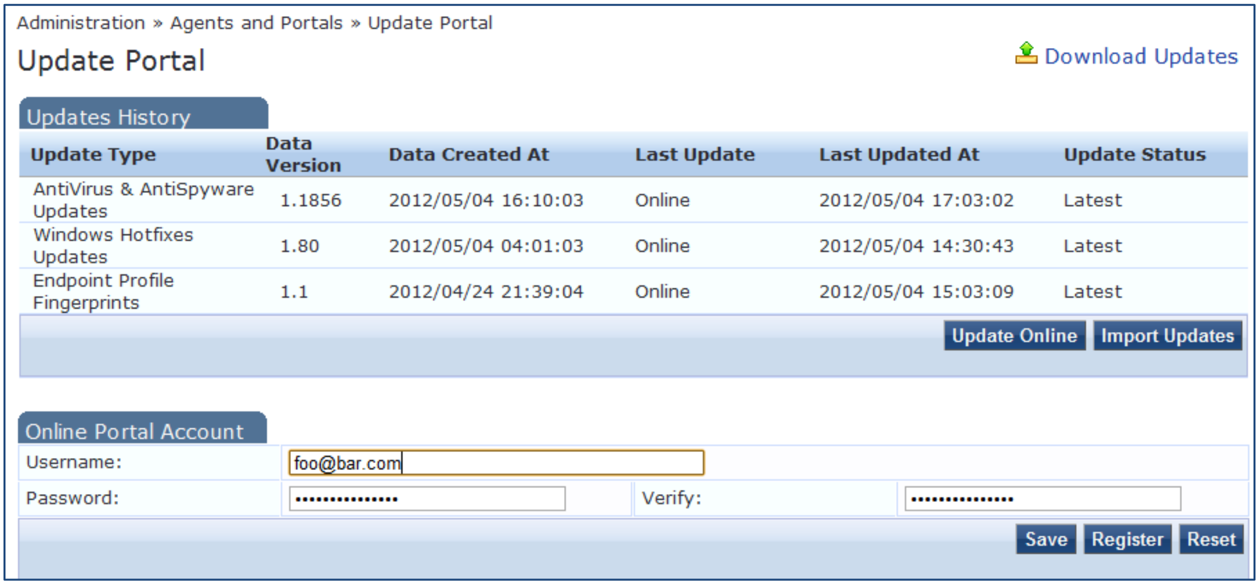


Device Fingerprints

#	Category ▲	Family	Name
81	Routers	D-Link	D-Link Wireless Router
82	Routers	DD-WRT	DD-WRT Router
83	Routers	Netgear	Netgear Router
84	Routers	Quanta Microsystems	Quanta Microsystems Router
85	Routers	Linksys	Linksys Router
86	SmartDevice	Apple	Apple iPhone
87	SmartDevice	Samsung	Samsung T-Mobile
88	SmartDevice	Samsung	Samsung S-Series
89	SmartDevice	Samsung	Samsung Device
90	SmartDevice	Sony Ericsson	Sony Ericsson W800i

Showing 81-90 of 136

As these dictionaries can change frequently, CPPM provides a way to automatically update fingerprints from an Aruba hosted portal. If external access cannot be provided to CPPM, the fingerprints file can be downloaded and imported through CPPM admin. The following screenshots show the configuration details for online and manual fingerprint updates.



Update Portal

Updates History

Update Type	Data Version	Data Created At	Last Update	Last Updated At	Update Status
AntiVirus & AntiSpyware Updates	1.1856	2012/05/04 16:10:03	Online	2012/05/04 17:03:02	Latest
Windows Hotfixes Updates	1.80	2012/05/04 04:01:03	Online	2012/05/04 14:30:43	Latest
Endpoint Profile Fingerprints	1.1	2012/04/24 21:39:04	Online	2012/05/04 15:03:09	Latest

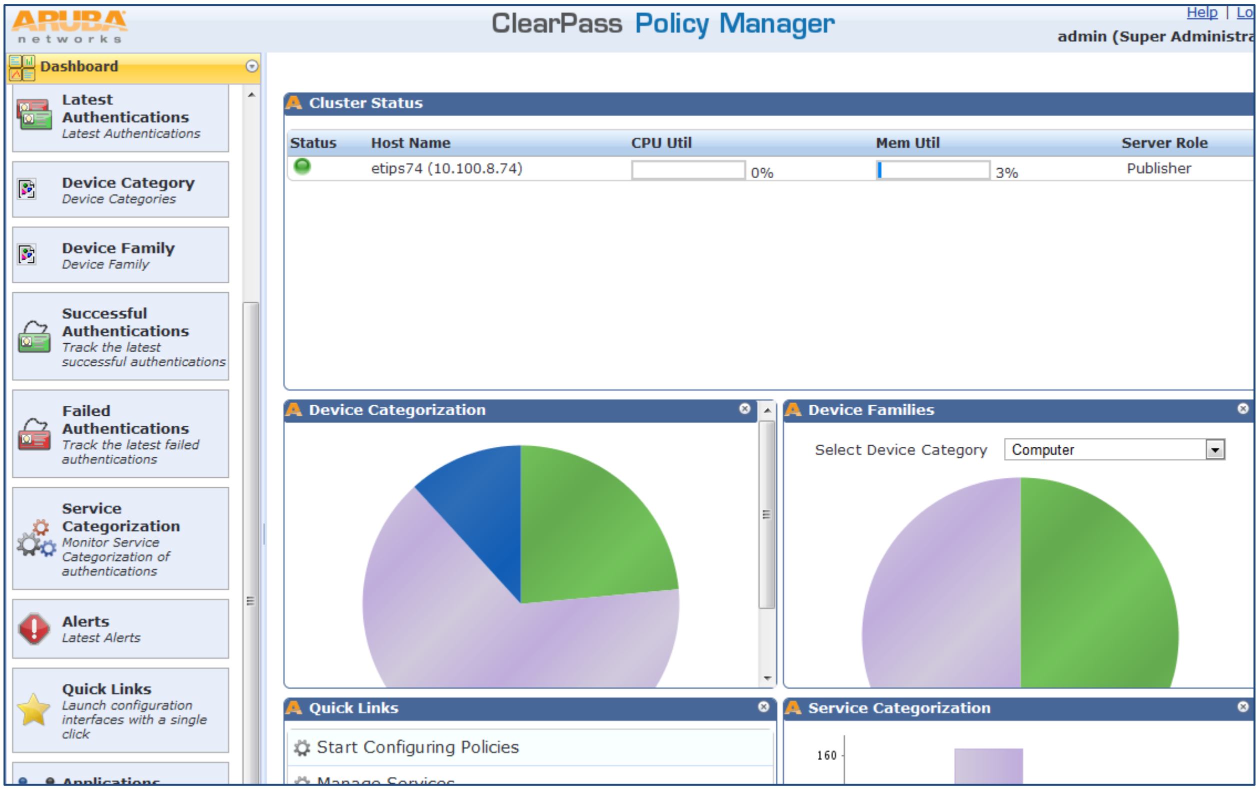
Online Portal Account

Username:	foo@bar.com		
Password:	•••••••••••••••	Verify:	•••••••••••••••

Profile UI

CPPM provides user interfaces to search and view profiled endpoints. It also provides basic statistics on the profiled endpoints.

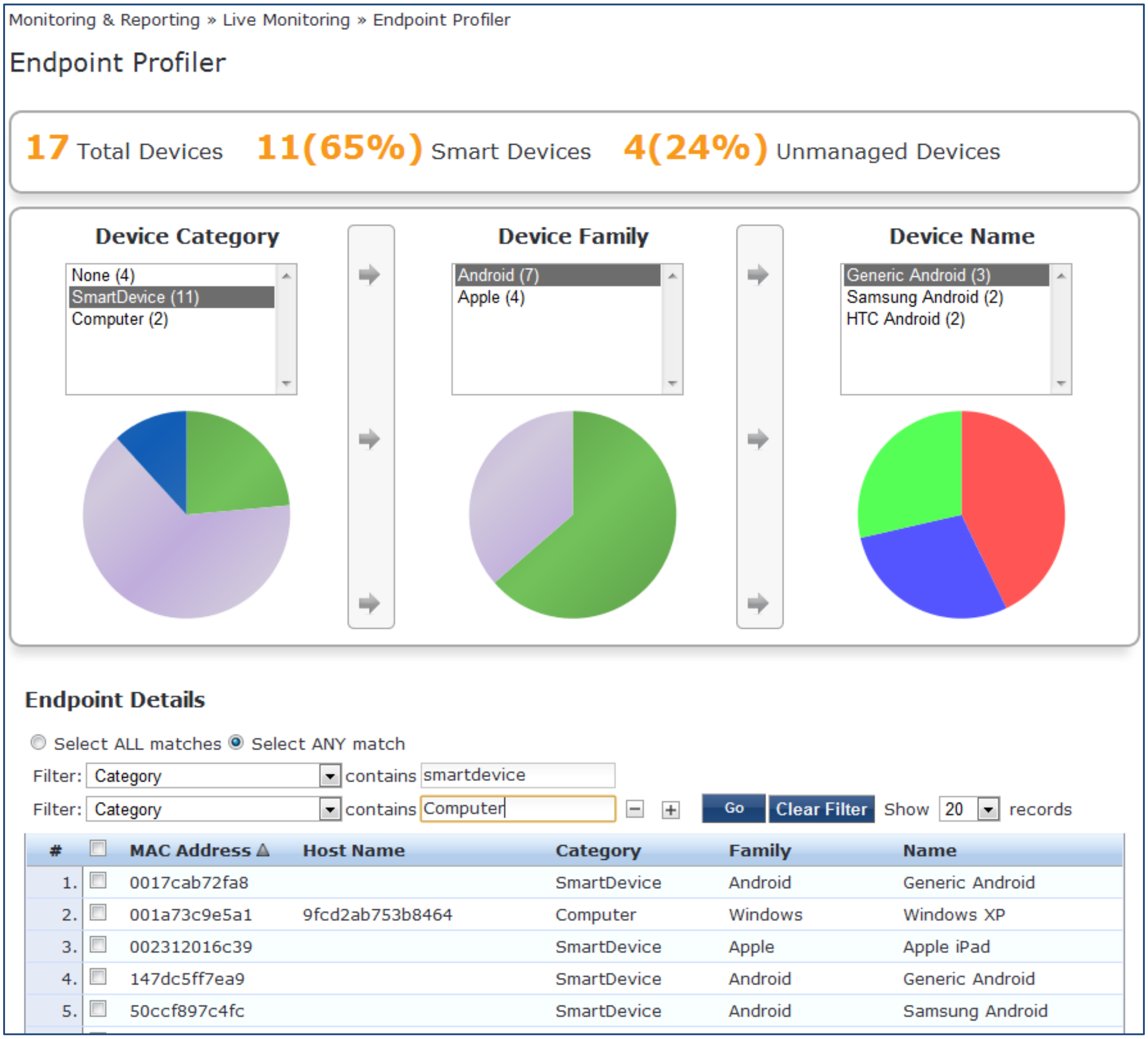
Dashboard widget showing basic distribution of device types



Status	Host Name	CPU Util	Mem Util	Server Role
●	etips74 (10.100.8.74)	0%	3%	Publisher

Select Device Category: Computer

Detailed device distribution and list of endpoints



Monitoring & Reporting » Live Monitoring » Endpoint Profiler

Endpoint Profiler

17 Total Devices 11(65%) Smart Devices 4(24%) Unmanaged Devices

Endpoint Details

○ Select ALL matches ● Select ANY match

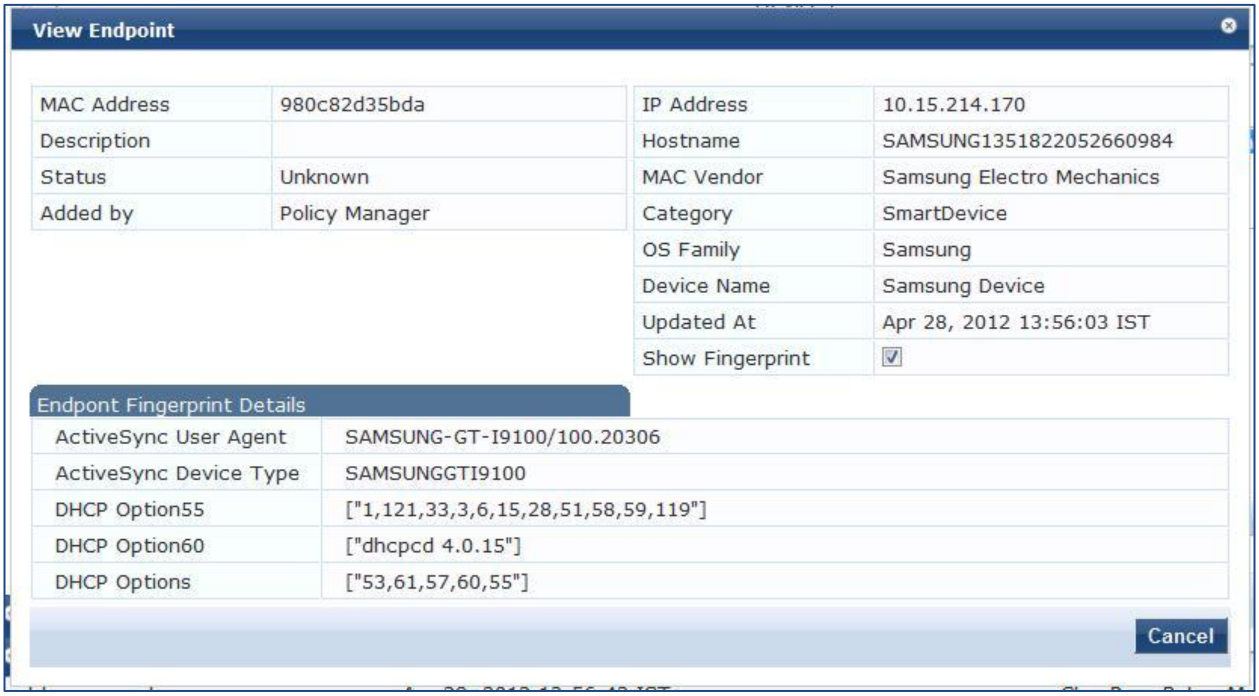
Filter: Category contains smartdevice

Filter: Category contains Computer

Show 20 records

#	□	MAC Address ▲	Host Name	Category	Family	Name
1.	□	0017cab72fa8		SmartDevice	Android	Generic Android
2.	□	001a73c9e5a1	9fcd2ab753b8464	Computer	Windows	Windows XP
3.	□	002312016c39		SmartDevice	Apple	Apple iPad
4.	□	147dc5ff7ea9		SmartDevice	Android	Generic Android
5.	□	50ccf897c4fc		SmartDevice	Android	Samsung Android

Profile details of an endpoint



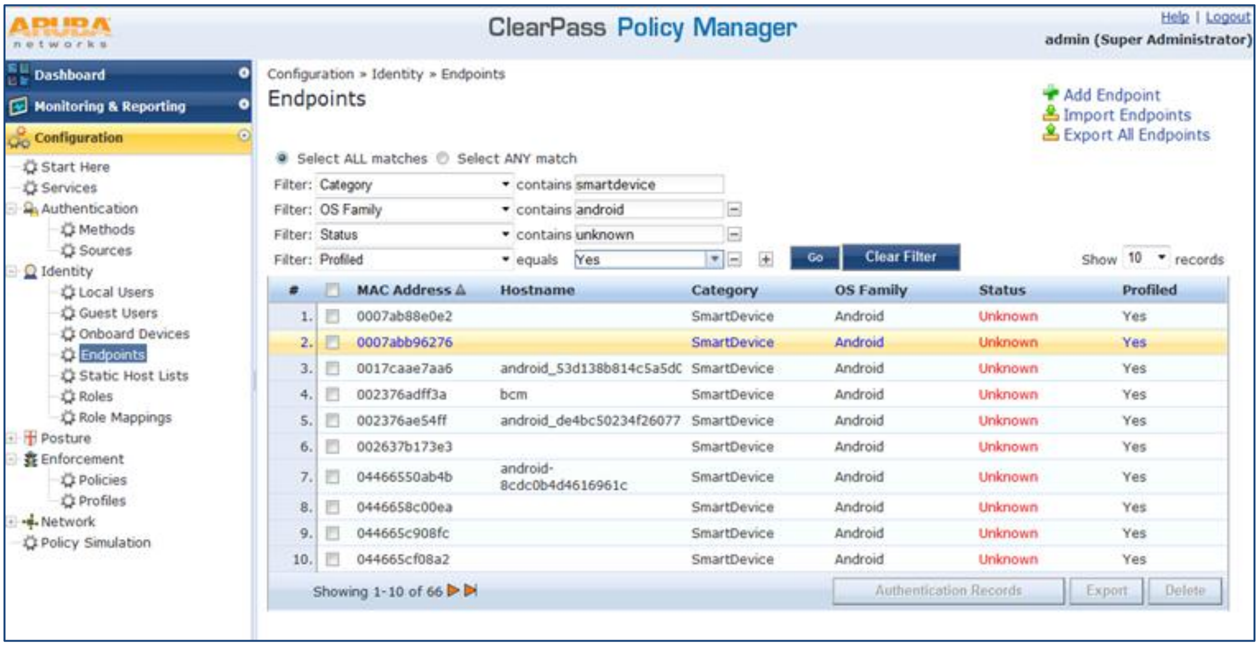
View Endpoint

MAC Address	980c82d35bda	IP Address	10.15.214.170
Description		Hostname	SAMSUNG1351822052660984
Status	Unknown	MAC Vendor	Samsung Electro Mechanics
Added by	Policy Manager	Category	SmartDevice
		OS Family	Samsung
		Device Name	Samsung Device
		Updated At	Apr 28, 2012 13:56:03 IST
		Show Fingerprint	☑

Endpont Fingerprint Details

ActiveSync User Agent	SAMSUNG-GT-I9100/100.20306
ActiveSync Device Type	SAMSUNGGTI9100
DHCP Option55	["1,121,33,3,6,15,28,51,58,59,119"]
DHCP Option60	["dhcpcd 4.0.15"]
DHCP Options	["53,61,57,60,55"]

Search endpoint profiles based on category/family/name, etc.



Endpoints

● Select ALL matches ○ Select ANY match

Filter: Category contains smartdevice
Filter: OS Family contains android
Filter: Status contains unknown
Filter: Profiled equals Yes

Show 10 records

#	□	MAC Address ▵	Hostname	Category	OS Family	Status	Profiled
1.	□	0007ab88e0e2		SmartDevice	Android	Unknown	Yes
2.	□	0007abb96276		SmartDevice	Android	Unknown	Yes
3.	□	0017caae7aa6	android_53d138b814c5a5dC	SmartDevice	Android	Unknown	Yes
4.	□	002376adff3a	bcm	SmartDevice	Android	Unknown	Yes
5.	□	002376ae54ff	android_de4bc50234f26077	SmartDevice	Android	Unknown	Yes
6.	□	002637b173e3		SmartDevice	Android	Unknown	Yes
7.	□	04466550ab4b	android-8cdc0b4d4616961c	SmartDevice	Android	Unknown	Yes
8.	□	0446658c00ea		SmartDevice	Android	Unknown	Yes
9.	□	044665c908fc		SmartDevice	Android	Unknown	Yes
10.	□	044665cf08a2		SmartDevice	Android	Unknown	Yes

Showing 1-10 of 66

Profile APIs

Profile exposes a set of REST APIs to receive endpoint attributes and to provide results of profiling. Basic HTTP authentication using CPPM admin user/passwords are required to for the APIs. Third-party products can easily integrate with ClearPass Profile by writing to these APIs.

- **Post endpoint attributes for profiling**

Attributes for a single or multiple endpoints can be POSTed to the following URL; this triggers profiling. MAC or IP address has to be present as the key. Other attributes are optional. If IP address is used as the key, Profile should have received MAC-IP binding from other sources such as DHCP.

- URL: https://{host}/async_netd/deviceprofiler/endpoints
- Method: POST
- Content-Type: application/json
- Input: Single or list of endpoint attributes

```
endpointinfo : {
  mac:
  ip:
  dhcp : {
     option55:
     option60:
     options:
  }
  hostname:
  http_user_agent
  active_sync : {
    device_type:
    user_agent:
  }
  host: {
    os_type:
  }
  snmp: {
    sys_descr:
    device_type:
    cdp_cache_platform:
  }
 }
```

Output:

- 200 OK on success
- 400 Bad Request - If input data is incorrect.
- 500 Internal Error - on service internal errors

- **Get endpoint by MAC or IP address**

- URL: https://device-profiler/async_netd/deviceprofiler/endpoints/{mac/ip}
- Method: GET

- Output:
- 200 OK - Success with json encoded endpoint details

```
{
  device_category : ,    => Computer, SmartDevice, Printer etc
  device_family: ,       => Android, Apple, Windows etc
  device_name: ,         => Samsung Android, Motorola Android, Apple
iPad etc
  added_at: ,            => as unix timestamp in seconds
  updated_at: ,          => as unix timestamp in seconds
}
```

- 404 Not Found - if endpoint with given MAC or IP address does not exist.
- 500 Internal Error - on service internal errors

Aruba Networks
1344 Crossman Avenue
Sunnyvale, CA 94089-1113
Phone: +1-408-227-4500
Fax: +1-408-227-4550