



# **Access Guardian and BYOD in AOS Release 8.1.1**

## **Configuration Guide through Use Cases**

Copyright © 2014 by Alcatel-Lucent

All rights reserved

Alcatel-Lucent, 26801 West Agoura Road, Calabasas, CA 91301, USA

+1(818) 880-3500

Neither this specification nor any of the information contained herein may be reproduced, or disclosed to or for the benefit of any other person or entity without consent of Alcatel-Lucent Enterprise

## Contents

1	Overview.....	4
2	Introduction .....	4
3	Access Guardian in AOS 8.1.1 .....	4
3.1	Access Guardian Benefits .....	5
3.2	Access Guardian Terminology .....	5
3.3	Access Guardian in AOS 8.1.1 vs Access Guardian in AOS 6.x.....	8
4	Access Guardian Use Cases.....	11
4.1	USE CASE 1: Classification only (no authentication) .....	11
4.2	USE CASE 2: Only Captive Portal authentication (no MAC/802.1x) .....	13
4.3	USE CASE 3: MAC authentication and/or Captive Portal.....	16
4.4	USE CASE 4a: Supplicant authentication only .....	18
4.5	USE CASE 4b: Supplicant/non-supplicant device authentication with Captive Portal 20	
4.6	USE CASE 5/6: Supplicant IP phone/non-supplicant, Network Policy TLV - tagged enabled on switch (single device on port).....	23
4.7	USE CASE 7: Multiple devices per UNP port. Supplicant IP phone connected to switch with non-supplicant laptop connected to IP phone (multiple devices per port) ...	25
4.8	USE CASE 8/9: 802.1x bypass MAC auth (with blacklist/or whitelist) .....	28
4.9	USE CASE 10: Post-authentication role assignment (QMR, Location- and Time-based Roles) 30	
4.9.1	QMR.....	30
4.9.2	Time policy .....	31
4.9.3	Location policy .....	32
5	Access Guardian BYOD with CPPM Integration .....	32
5.1	Use Case Summary .....	35
5.2	Pre-Requisite Switch Configuration.....	35
5.3	Pre-Requisite CPPM Configuration .....	37
5.3.1	Configure the AOS switches on CPPM for which CPPM is acting as the Policy Manager/RADIUS server .....	37
5.3.2	Update CPPM with latest Alcatel-Lucent Enterprise Dictionary .....	38
5.3.3	Configure CPPM to use an external AD server as an authentication source... 39	
5.3.4	Configure Static Host List for IP phones/printer devices .....	41
5.4	AOS switch and CPPM integration points.....	43

5.4.1	Edge-profile, access policy list and redirection URL handling .....	43
5.5	BYOD USE CASE 1: Guest access.....	44
5.5.1	Switch configuration .....	44
5.5.2	CPPM configuration .....	45
5.6	BYOD USE CASE 2: Unified authentication of IT-issued device .....	54
5.6.1	Switch configuration .....	54
5.6.2	CPPM configuration .....	55
5.7	BYOD USE CASE 3: Device onboarding with non-IT devices .....	62
5.7.1	Switch configuration .....	62
5.7.2	CPPM configuration .....	63
5.8	BYOD USE CASE 4: Guest Access/BYOD Access with Posture Check.....	76
5.8.1	Enabling BYOD USECASE 1 - Guest Access with Posture .....	76
5.8.2	Enabling BYOD USECASE 3 - Onboard with Posture .....	82
6	Glossary .....	91

# 1 Overview

This paper describes the functionality and configuration examples of the Access Guardian(AG) and Bring Your Own Device (BYOD) features available in the OmniSwitch 6860 product family and supported in the Alcatel-Lucent Operating System (AOS) Release 8.1.1. It walks through the Access Guardian functional behavior and configuration examples by means of different use cases.

## 2 Introduction

Access Guardian is a comprehensive set of network access control functions, which provide a dynamic, proactive network access control and security solution. Access Guardian has been a feature supported in the older version Alcatel-Lucent Enterprise switches such as the OmniSwitch 6850E running AOS 6.x.

The latest hardware platform, OmniSwitch 6860, which is a successor to OmniSwitch 6850E, is based on the next generation Linux software base - AOS 8.x. The implementation of Access Guardian in AOS 8.x software is different than the AG in AOS 6.x

Throughout the document Access Guardian will refer to the implementation in AOS 8.1.1 on OS6860 unless it specifically refers to Access Guardian or AG for AOS 6.x

## 3 Access Guardian in AOS 8.1.1

Alcatel-Lucent's Access Guardian refers to the following Alcatel-Lucent OmniSwitch security functions that work together to provide a dynamic, proactive network security solution.

**Universal Network Profile (UNP)** – UNP is enabled on switch ports to activate Access Guardian functionality that is used to authenticate and classify users into Edge profiles. Each profile is mapped to a VLAN ID to which the user is dynamically assigned.

**Authentication, Authorization, and Accounting (AAA)** – AAA provides the switch-based authentication and accounting configuration that defines the RADIUS-capable servers to use for each type of Access Guardian authentication (802.1X, MAC, and Captive Portal).

**Bring Your Own Device (BYOD)** – OmniSwitch/ClearPass Integration: The OmniSwitch leverages Access Guardian functionality along with the ClearPass Policy Manager (CPPM) to provide the overall BYOD solution. BYOD allows a wired guest, device, or authenticated user to connect to the network through an OmniSwitch edge device using the CPPM for unified authentication.

**Captive Portal** – Internal and external Captive Portal web-based authentication. The OmniSwitch

presents default or customized web pages to the user through an internal web server on the switch. A post-authentication and/or post-classification process validates user credentials and dynamically assigns a new role (policy list) to enforce user access to the network. External, guest Captive Portal authentication is provided through the Access Guardian interaction with the CPPM.

**Quarantine Manager and Remediation (QMR)** – QMR is a switch-based application that restricts the network access of known quarantined users and provides a remediation path to allow quarantined users to regain their network access.

### **3.1 Access Guardian Benefits**

- Flexible template-/profile-driven configuration
- Simplified and clean authentication/classification branches
- Multiple authentication mechanisms on a given port/LAG are supported: 802.1x, MAC-based, no authentication (classification rules are used to learn a user) and role-based policy list assignment for internal and external Captive Portal feature
- Flexible assignment of RADIUS server and associated properties per authentication method. This allows for different sets of ports to have different sets of authentication/accounting servers and associated RADIUS attribute properties.
- The Alcatel-Lucent AOS 8.1.1 software also provides a BYOD solution through close integration with Aruba's ClearPass Policy Manager (CPPM). Aruba CPPM provides the framework for device on-boarding (with CPPM Onboard module), guest registration and authentication (CPPM Guest Module), and device posture check (CPPM OnGuard Module).

### **3.2 Access Guardian Terminology**

**AAA Profile:** AAA profiles define a specific AAA configuration that can be applied at the port level (overrides the global AAA configuration) and are used to define the mapping of RADIUS servers needed for 802.1x, MAC authentication and accounting. An AAA profile is a grouping of all the properties required for authentication, authorization, accounting and can be applied on a per-port or per-LAG basis. It includes the following configuration parameters:

- The authentication server for 802.1x authentication and MAC authentication
- The accounting server for 802.1x authentication and MAC authentication
- The RADIUS attribute format configuration
- Authentication parameters like trust-radius, inactivity-logout interval, interim interval, etc.

**Captive Portal Profile:** A Captive Portal profile is associated with an edge-profile (defined below).

The Captive Portal profile includes the following configuration parameters:

- Captive Portal mode
- Captive Portal pass policy list, policy-list based on domain name
- Captive Portal aaa-profile
- Captive Portal success-url
- Captive Portal server ip address
- Captive Portal retry-count

**Access Guardian is designed to support three port types - edge, bridge and access. Initial 8.1.1 Release will support only “Edge” port type. This guide applies only to the features supported on edge-port. The port types are as defined below.**

**Edge port:** This is a UNP port type where NAC (802.1x/MAC authorization/classification/Captive Portal) and BYOD functions are supported. This is equivalent to features available under “aaa user-network-profile/802.1x” framework of AOS 6.x.

**Access port:** This is a UNP port type that supports the spb-profile features of AOS 7.x under the framework of Universal Network Profile. The support for “access port” is not available in Release 8.1.1. This will be supported in the following releases of AOS 8.x.

**Bridge port:** This is a UNP port type that supports the VLAN-profile feature of AOS 6.x/AOS 7.x under the framework of Universal Network Profile. The dynamic VLAN and profile creation features are supported on “bridge port”. The support for “bridge port” is not available in Release 8.1.1. This will be supported in the following releases of AOS 8.x.

**Edge-profile:** This is a grouping of all the properties that will be assigned to a user/device after the Network Access Control process. The edge-profile includes the following parameters:

- Default Quality of Service (QoS) policy list
- Captive Portal authentication enable/disable
- Captive Portal profile associated with this edge-profile
- Location policy list
- Time policy list
- Captive Portal pass
- Mobile-tag enable/disable
- Redirect enable/disable
- DPI enable/disable
- LLDP classification enable/disable

**Edge-template:** UNP edge-port templates define a specific port configuration to simplify and easily replicate the same configuration across multiple ports. The edge-template can be assigned to a single port or a link-aggregation. The edge-template includes the following configuration parameters:

- 802.1x authentication enable/disable
- Pass-alternate edge-profile
- 802.1x properties - tx-period, max-req, supp-timeout
- 802.1x authentication bypass enable/disable
- Action to take after 802.1x authentication bypass MAC-authentication - allow-eap on pass or fail or no-auth or none
- MAC authentication enable/disable
- Pass-alternate edge-profile
- Classification enable/disable

- 802.1x failure-policy
- Default edge-profile
- aaa-profile association with the edge-template
- BYOD redirect port bounce enable/disable

**Group-ID:** A configuration object of Access Guardian used to group together multiple edge-ports or edge link-aggregates into a single logical domain. Edge-templates can be assigned to group-ids.

**Learned Port Security:** This is a feature that limits the number of MACs learned on a port. This is a post-authentication check performed on the switch before a client MAC is learned or put in filtering mode.

**Mobile-tag:** This flag is enabled on an edge-profile. It indicates that the VLAN that the client is assigned after MAC has to be tagged on the port.

**Quarantine:** This is a role that a client can get into post authentication. The input to put a MAC into a Quarantined MAC group is configured manually on the individual switches or comes from the OmniVista Network Management System. The OmniVista is notified of a Quarantined MAC through a TRAP received from a switch in the network running network anomaly detection application or an intrusion detection system (IDS) running in the same subnet as the client. The IDS application can send the TRAP to the OmniVista and the OmniVista can configure all the switches in the logical group to put the MACs in the Quarantine Group. Access Guardian is responsible for moving the authenticated MAC from its current role to Quarantine Role.

**Redirect:** This term is used to mean there is an external server performing the BYOD function and is capable of sending RADIUS RFC 3576 Change of Authorization (COA) to the switch. A redirect server is configured on the system to point to Aruba's CPPM IP address

**UNP:** Universal Network Profile - In Release 8.1.1 only edge-profile is supported

### 3.3 Access Guardian in AOS 8.1.1 vs Access Guardian in AOS 6.x

Access Guardian in ASO 6.4.x and Access Guardian in AOS 8.1.1 implementations can be visually captured through the flow charts given below. They show the differences between the two implementations at the functional level.

Figure 1. Access Guardian in AOS 6.4.x Workflow

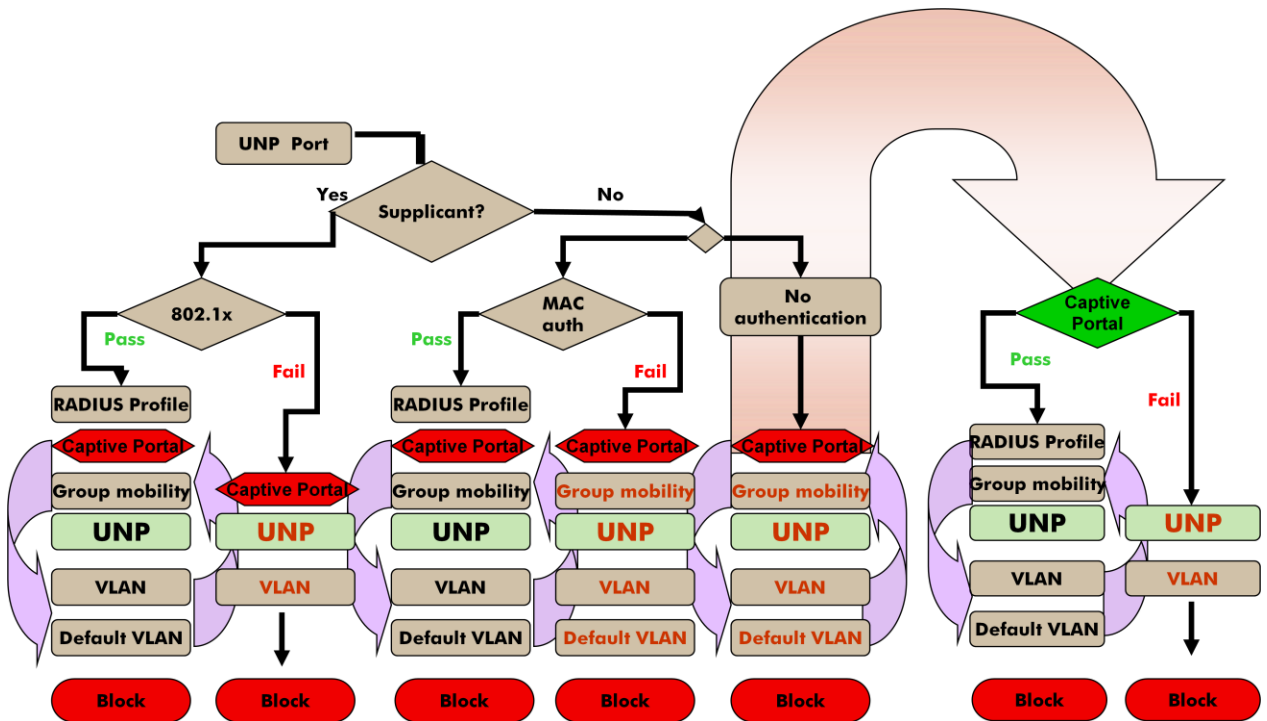
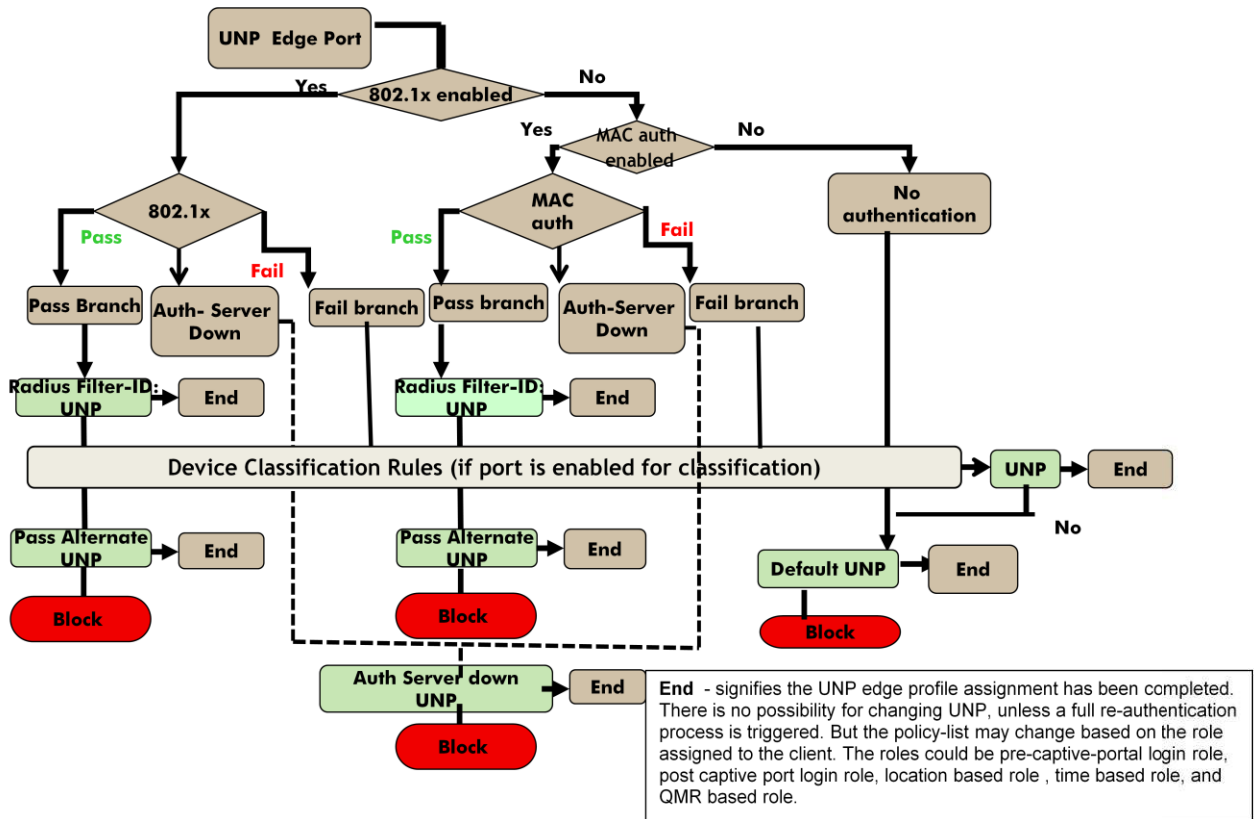




Figure 2. Access Guardian in AOS 8.1.1 Workflow



The functional differences between AG in AOS 6.4.x and AG in AOS 8.1.1 are described below.

1. Triggering of the authentication/classification

- a. In AOS 6.x, a port should first be identified as a mobile port and then 802.1x port to have the Access Guardian function enabled on the port. A port identified as mobile/802.1x port is automatically enabled for 802.1x authentication, MAC authentication and Group Mobility classification.
- b. In AOS 8.x, a port should first be identified as a UNP edge-port. A port identified as a UNP edge-port has to be explicitly enabled for 802.1x authentication, MAC authentication and/or classification. This provides the user with the control to choose the process to be enabled on the port - 802.1x or MAC authentication or both or classification only, etc.

2. Captive Portal authentication

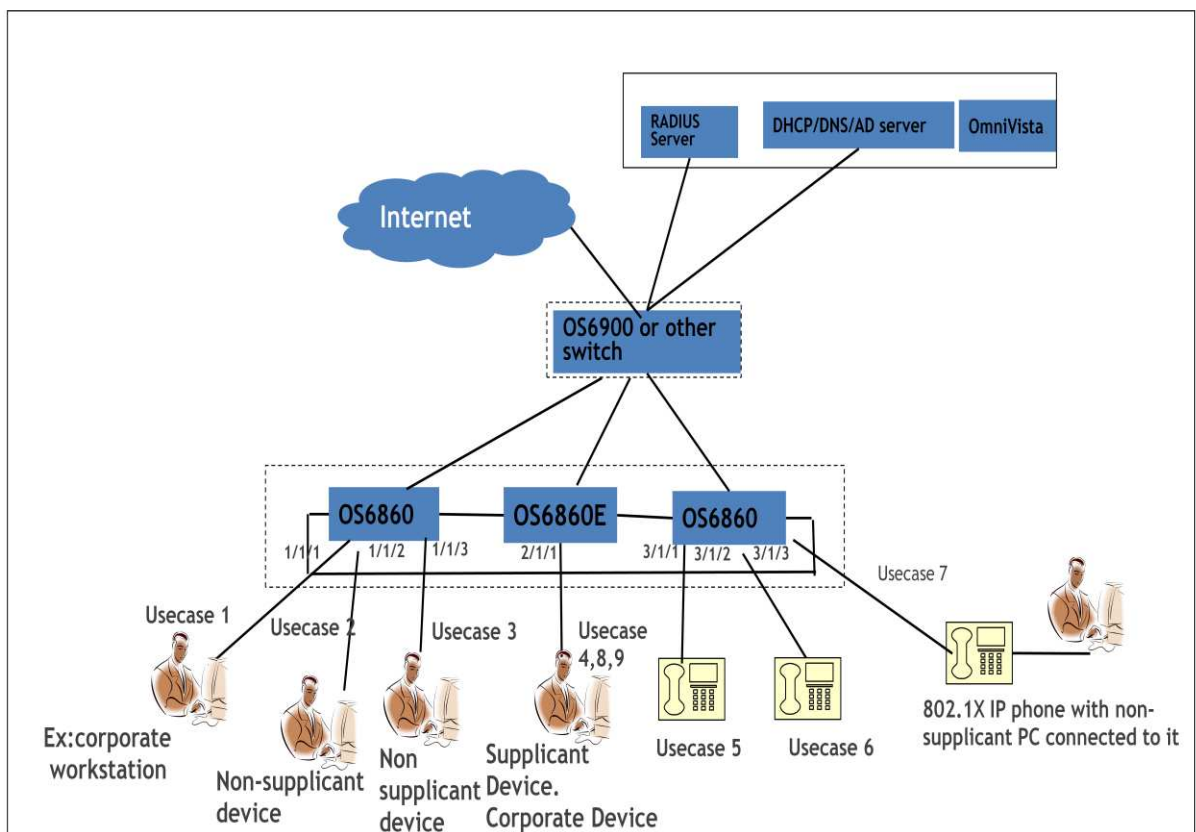
- a. In AOS 6.x implementation, the Captive Portal authentication is triggered from classification policies. The result of Captive Portal authentication is an “aaa User Network Profile” that may result in a new VLAN for the client. This requires the client to move from the temporary VLAN in which the Captive Portal was initiated to a new VLAN. This requires the DHCP address to be released and renewed.

- b. In AOS 8.x implementation, the Captive Portal authentication is triggered from a UNP edge-profile. Captive Portal enable/disable control is a property of the UNP edge-profile that is returned after the primary authentication and/or classification stage. The Captive Portal authentication does not result in a new UNP/VLAN. Instead the client remains in the same UNP/VLAN but can be associated with a post Captive Portal policy list that is different from the default policy list of the UNP profile. There is no VLAN change in 8.x, hence the client can immediately get access to the network after Captive Portal authentication since there is no need for additional DHCP release/renew process to get a new IP address.
3. Group Mobility and Device Classification
  - a. The terms Group Mobility used in AOS 6.x and Device Classification used in 8.x functionally refer to classification based on some classification rules. The client's traffic is matched against the classification rules to derive a User Network Profile". Group Mobility was an independent feature in AOS 6.x. This is not supported in AOS 8.x.
  - b. In 8.x, classification should be explicitly enabled on a port. It can be triggered when 802.1x/MAC authentication is not enabled and also when 802.1x/MAC authentication is enabled and if 802.1x or MAC authentication fails. AOS 8.x supports LLDP-based classification and policy assignment, DHCP fingerprinting-based classification and policy assignment (with BYOD appliance), DPI-based classification and policy assignment.
4. Profile assignment
  - a. In AOS 6.x, user network profile assigned in a branch can be changed on subsequent stages of the same branch. For example, Captive Portal processing happening after a primary authentication like 802.1x/MAC authentication and/or classification, can be changed post Captive Portal. This may result in a different policy list and new VLAN.
  - b. In AOS 8.x, UNP edge-profile assigned once in a branch cannot be changed in subsequent stages of the same branch. The only change possible is the role. A role is defined by a policy list. The client stays in the same UNP edge-profile and VLAN but the policy list changes based on different roles. The roles could be Captive Portal pre-login role, Captive Portal post-login role, location-based role, time-based role, QMR-based role, etc. In 6.x, UNP has one policy list associated with it, whereas in 8.x a UNP edge-profile has one base policy list that can be replaced as the user/devices changes roles based on Captive Portal authentication/location/time/lddp/DPI without changing the profile or VLAN.
5. VLAN to User Network Profile
  - a. In AOS 6.x, a VLAN was a property of the UNP.
  - b. In AOS 8.x, a VLAN is mapped to a UNP edge-profile separately. The same UNP edge-profile could potentially be mapped to different VLANs on different switches in the same network.

## 4 Access Guardian Use Cases

This section defines a set of typical use cases and the configurations of the switch in the context of each use case. The use cases in this section do not cover BYOD with CPPM. The use cases must be used as examples and should be modified to fit deployment requirements. For detailed configuration one must refer to the AOS 8.1.1 CLI Reference Guide since this document does not provide all the configuration options for this feature. The following network diagram will be used for the use case discussions.

Figure 3. Network diagram for use case scenarios



### 4.1 USE CASE 1: Classification only (no authentication)

This is the case of basic classification without an L2/L3 authentication method. AOS 8.1.1 supports different classification rules:

- Port, Group-id, MAC address, MAC address range, IP Address, IP Address range, MAC-OUI, LLDP - IPPhone, Authentication type
- Port+MAC+IP, Port+MAC, Port+IP, Group-id+MAC+IP, Group-id+MAC, Group-id+IP
- Extended classification rules, which are custom user-defined combinations

This example use case uses the MAC range classification rule to classify the devices into vlan 20.

The steps for configuration are as follows.

1. Create the required VLANs

```
vlan 10 admin-state disable name vlan10-block
```

```
vlan 20 admin-state enable name vlan20-corporate
```

2. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic on classification rule match.

3. Create the required UNP edge-profile

```
unp edge-profile corporate
```

4. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile corporate vlan 20
```

5. Create a default profile

```
unp edge-profile default-profile
```

6. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

7. Create MAC-based classification rules and associate a UNP edge-profile

```
unp classification-rule rule1 mac-address-range 08-00-27-00-98-0A 08-00-27-00-98-FF
```

```
edge-profile corporate
```

8. Identify the ports as edge-ports

```
unp port 1/1/1 port-type edge
```

9. Create an edge-template

```
unp edge-template classify-template
```

10. Enable classification on the template

```
unp edge-template classify-template classification enable
```

11. Create a default UNP for the edge-template

```
unp edge-template classify-template default-edge-profile default-profile
```

12. Assign the edge-template to edge ports you want to enable only classification

```
unp port 1/1/1 edge-template classify-template
```

**Note:**

The steps 9/10/11 listed above are based on template-based configuration. The same can be achieved directly at the port level using the following commands. It is encouraged to use a template so that it can be applied to a group of like ports. A set of ports that need the same template may be identified as a group using {**unp group-id 1 description “classify-only-ports”**} and then the template can be assigned to the group using {**unp edge-template classify-template group-id 1**}.

13. Set the default edge-profile on a port

```
unp port 1/1/1 default-edge-profile default-profile
```

14. Enabled classification on the port

```
unp port 1/1/1 classification enable
```

Traffic arriving on the port will trigger the following on the switch:

- Classification is automatically triggered
- If MAC address of client is in MAC range, then the UNP edge-profile “workstation”/vlan 20 is assigned
- If MAC address is not in range, a default edge-profile/vlan 10 is assigned
- MAC address should be learned in the assigned VLAN
- Port 1/1/1 is untagged member of the assigned VLAN

## ***4.2 USE CASE 2: Only Captive Portal authentication (no MAC/802.1x)***

This use case demonstrates the steps required to enable and configure Captive Portal authentication using the internal web server on the switch.

External Captive Portal functionality is provided only through the integration with ClearPass Policy Manager (see the BYOD use cases later in this document). There is no support for a generic external Captive Portal in AOS 8.1.1.

Different policy lists can be assigned to different users using the internal Captive Portal based authentication. Example: University with students, teachers, visitors, etc. going through Captive Portal authentication and getting different policy lists based on their role.

In AOS 8.x, Captive Portal authentication can be initiated only through an edge-profile. Hence an edge-profile must be assigned to the user through an L2 authentication (802.1x/MAC) or classification or through a default edge-profile. The edge-profile so assigned must have Captive Portal enabled. The result of Captive Portal authentication is assignment of Access Policy Lists. Different Access Policy Lists may be assigned to different users.

Captive Portal authentication cannot be used to change the UNP edge-profile or VLAN. It can only change the policy list assigned.

Network configuration for Captive Portal support is as follows:

1. Configure the DHCP server in the network to give out the IP addresses in the subnet of the VLAN associated with the edge-profile to be used
2. Configure the DNS with a DNS entry to map the Captive Portal Name to Captive Portal IP address that is configured on the OmniSwitch 6860 switches in the network

Switch configuration for Captive Portal support is as follows:

1. Configure a RADIUS server

```
aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile

```
aaa profile "ag-aaa-profile"
aaa profile ag-aaa-profile device-authentication captive-portal "alu-authserver"
aaa profile ag-aaa-profile accounting captive-portal "alu-authserver"
aaa profile ag-aaa-profile captive-portal session-timeout enable ←...very important to enable
session timeout
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block
vlan 30 admin-state enable name vlan-guest
```

4. Create the policy list for post Captive Portal authentication

```
policy condition cp-default-C1 source ip Any destination ip Any
policy action cp-default-A1
policy rule cp-default-R1 condition cp-default-C1 action cp-default-A1
policy list cp-default-list type unp
policy list cp-default-list rules cp-default-R1
qos apply
```

5. Create an edge-profile guest

```
unp edge-profile guest
```

6. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile guest vlan 30
```

7. Create a default profile

```
unp edge-profile default-profile
```

8. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

9. Create an edge-template

```
unp edge-template cp-only-template
```

10. Set the default profile for the edge-template to “guest” so that the clients can get into vlan 30 first using default edge-profile. Then the policy list can be updated based on Captive Portal authentication.

```
unp edge-template cp-only-template default-edge-profile guest
```

11. Assign the edge-template to a port

```
unp port 1/1/2 edge-template cp-only-template
```

12. Create Captive Portal profile

```
captive-portal-profile cp-profile
```

```
captive-portal-profile cp-profile aaa-profile ag-aaa-profile
```

13. Add Captive Portal authentication pass policy list, the success url. Captive Portal IP address by default is set to 10.123.0.1

```
captive-portal-profile cp-profile mode internal /*NOTE: this is the only mode supported in 8.1.1*/
```

```
captive-portal-profile cp-profile authentication pass policy-list cp-default-list
```

```
captive-portal-profile cp-profile success-redirect-url http://test-cp.com/success.html
```

14. Enable edge-profile with Captive Portal and assign the Captive Portal profile

```
unp edge-profile guest captive-portal-authentication enable
```

```
unp edge-profile guest captive-portal-profile cp-profile
```

Traffic arriving on the port will trigger the following on the switch

- The port is not enabled for classification/authentication, so the default UNP edge-profile and associated VLAN is assigned.
- Since the default UNP edge-profile (associated with edge-template of the port) is enabled for Captive Portal authentication, Captive Portal authentication is triggered.
- This means the client is put in built-in Captive Portal pre-login role. This does the following:
  - Only allows DHCP, DNS, ARP, ICMP
  - Traps HTTP/HTTPS traffic to CPU
  - The traffic is redirected to the internal Captive Portal server. The Captive Portal server name is resolved using DNS.
  - Client is presented with internal Captive Portal login page
  - User enters the credentials, which are authenticated against the configured RADIUS server

- Successful Captive Portal authentication should result in assignment of a policy list configured for Captive Portal authentication pass condition or policy list returned from RADIUS server.
- The client remains in edge-profile guest/vlan 30 and is presented with the configured success.html page.
- The Captive Portal fail policy should result in client remaining in the Captive Profile pre-login built-in role.

### 4.3 USE CASE 3: MAC authentication and/or Captive Portal

This use case can be used to support a port enabled for non-supPLICANT users. The port is enabled for MAC authentication followed by Captive Portal authentication.

The following scenarios can be handled:

- Guest users with non-supPLICANT devices
  - Will fail MAC authentication
  - MAC authentication fail can be assigned a default edge-profile that has Captive Portal enabled.
  - Captive Portal pass policy can set an access policy list different from the default policy list of the edge-profile.
  - Captive Portal fail policy can be set to filtering/block.
  - The UNP edge-profile/VLAN will not be changed after Captive Portal authentication.
- Corporate users with non-supPLICANT, corporate-issued devices (not likely)
  - Will pass MAC authentication
  - MAC authentication pass can be set to trigger Captive Portal authentication by assigning an edge-profile that is enabled for Captive Portal authentication or may terminate with a UNP edge-profile/VLAN.
  - Captive Portal is preferred to identify the user using the device.
  - The UNP edge-profile/VLAN will not be changed after Captive Portal authentication.
- Corporate user with non-supPLICANT, non-corporate-issued devices
  - Will fail MAC authentication
  - MAC authentication fail can be assigned a default edge-profile that has Captive Portal enabled.
  - Captive Portal pass policy can set an access policy list different from the default policy list of the edge-profile.
  - Captive Portal fail policy can be set to filtering/block.
  - The UNP edge-profile/VLAN cannot be changed after Captive Portal authentication.

The configuration steps are shown below.

#### 1. Configure a RADIUS server

```
aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2  
auth-port 1812 acct-port 1813
```



2. Create an “aaa” profile

**aaa profile “ag-aaa-profile”**

**aaa profile ag-aaa-profile device-authentication mac “alu-authserver”**

**aaa profile ag-aaa-profile accounting mac “alu-authserver”**

**aaa profile ag-aaa-profile device-authentication captive-portal “alu-authserver”**

**aaa profile ag-aaa-profile accounting captive-portal “alu-authserver”**

3. Create the required VLANs

**vlan 10 admin-state disable name vlan-block**

**vlan 20 admin-state enable name vlan-corporate**

**vlan 30 admin-state enable name vlan-guest**

4. Create the policy list

The default policy list is “allow all”. One should create a policy list if it needs to be different from the default.

5. Create the required UNP edge-profiles

**unp edge-profile corporate**

**unp edge-profile guest**

6. Map the edge-profile to appropriate VLANs

**unp vlan-mapping edge-profile corporate vlan 20**

**unp vlan-mapping edge-profile guest vlan 30**

7. Create a default profile

**unp edge-profile default-profile**

8. Map the default edge-profile to vlan 10

**unp vlan-mapping edge-profile default-profile vlan 10**

9. Create an edge-template

**unp edge-template auth-template**

10. Update the default profile for the edge-template to be guest, which has Captive Portal enabled

**unp edge-template auth-template default-edge-profile guest**

11. Enable MAC authentication on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return a UNP edge-profile on authentication pass.

**unp edge-template auth-template mac-authentication enable**

**unp edge-template auth-template mac-authentication pass-alternate edge-profile corporate**

12. Assign the edge-template to a port

**unp port 1/1/3 edge-template auth-template**

13. Create the Captive Portal profile

**captive-portal-profile cp-profile**

**captive-portal-profile cp-profile aaa-profile ag-aaa-profile**

14. Add Captive Portal authentication pass policy list

**captive-portal-profile cp-profile authentication pass policy-list cp-default-list**

15. Create an edge-profile with Captive Portal enabled and assign the Captive Portal profile to the edge-profile with Captive Portal enabled. Associate the default-edge-profile with the VLAN that you expect the client to be in.

**unp edge-profile guest captive-portal-authentication enable**

**unp edge-profile guest captive-portal-profile cp-profile**

Traffic arriving on the port will trigger the following on the switch

- MAC authentication first.
- On MAC authentication pass, the client is assigned to UNP corporate/vlan 20 or the UNP profile returned from RADIUS server.
- On MAC authentication fail, the client is assigned to the default edge-profile “guest”, which triggers the Captive Portal authentication successful. Captive Portal authentication should result in assignment of default access policy list or the access policy list returned by the authentication server
- The Captive Portal fail policy should result in client remaining in the Captive Portal pre-login built-in role.
- This means that in AOS 8.x the client does not move into a new UNP edge-profile/VLAN on Captive Portal pass.

#### ***4.4 USE CASE 4a: Supplicant authentication only***

This use case covers only supplicant corporate devices trying to get access to the network on a port.

This port is not open to any other device.

The configuration steps are as follows:

1. Configure a RADIUS server

**aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2**

**auth-port 1812 acct-port 1813**

2. Create an “aaa” profile

**aaa profile "ag-aaa-profile"**

**aaa profile ag-aaa-profile device-authentication 802.1x "alu-authserver"**

**aaa profile ag-aaa-profile accounting 802.1x "alu-authserver"**

3. Create the required VLANs

**vlan 10 admin-state disable name vlan-block**

**vlan 20 admin-state enable name vlan-corporate**

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic on classification rule match.

5. Create the required UNP edge-profiles

**unp edge-profile corporate**

6. Map the edge-profile to an appropriate VLAN

**unp vlan-mapping edge-profile corporate vlan 20**

7. Create a default profile

**unp edge-profile default-profile**

8. Map the default edge-profile to vlan 10

**unp vlan-mapping edge-profile default-profile vlan 10**

9. Create an edge-template

**unp edge-template onex-template**

10. Enable MAC authentication/802.1x on the edge-template. Pass alternate UNP edge-profile

may be configured if RADIUS server doesn't return a UNP edge-profile on authentication pass.

**unp edge-template onex-template 802.1x-authentication enable**

**unp edge-template onex-template 802.1x-authentication pass-alternate edge-profile corporate**

11. Assign the edge-template to a port

**unp port 2/1/1 edge-template onex-template**

Traffic arriving on the port will trigger the following on the switch:

- Supplicant device traffic will trigger 802.1 x authentications first.
- On 802.1x authentication pass, the client is assigned to UNP corporate/vlan 20 or the UNP profile returned from RADIUS server.

- On 802.1x authentication fail, if classification is not enabled, and if default edge-profile is not assigned, the MAC should be assigned to filtering/block
- For non-suppliant users, since MAC authentication/classification is not enabled, MAC authentication/classification is not triggered and if no default edge-profile is assigned to the port, the MAC should be assigned to filtering/block.
- This use case is to support ports in a network for suppliant corporate devices only.

#### ***4.5 USE CASE 4b: Suppliant/non-suppliant device authentication with Captive Portal***

This use case covers suppliant corporate devices and guess devices trying to get access to the network on the same port. The behavior in the different scenarios is as follows:

- Corporate suppliant device
  - Will pass 802.1x authentication
  - The client can be assigned a UNP corporate edge-profile/VLAN.
- Corporate user with non-suppliant non-corporate device
  - Will not trigger 802.1x authentication
  - Will fail MAC authentication
  - On MAC authentication fail, if classification is not enabled, default edge-profile associated with the port will be assigned and the default edge-profile can be enabled for Captive Portal authentication.
  - The Captive Portal pass policy may assign a new access policy list or the default access policy list of the default edge-profile.
  - The Captive Portal fail policy may result in block/filtering.
- Guest suppliant device
  - Will fail 802.1x authentication
  - If 802.1x failure-policy is not set, then if classification is not enabled, the default edge-profile associated with the port will be assigned and the default edge-profile should be enabled for Captive Portal authentication.
  - The Captive Portal pass policy may assign a new access policy list or the default access policy list of the default edge-profile.
  - The Captive Portal fail policy may result in block/filtering.
- Guest non-suppliant device
  - Will not trigger 802.1x authentication
  - If non-suppliant, MAC authentication will not be automatically triggered, MAC authentication must be explicitly enabled for the port.
  - On MAC authentication fail, if classification is not enabled, the default edge-profile associated with the port will be assigned and the default edge-profile should be enabled for Captive Portal authentication.
  - The Captive Portal pass policy may assign a new access policy list or the default access policy list of the default edge-profile.
  - The Captive Portal fail policy may result in block/filtering.

The configuration steps are as follows.

1. Configure a RADIUS server

```
aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile

```
aaa profile "ag-aaa-profile"
aaa profile ag-aaa-profile device-authentication 802.1x "alu-authserver"
aaa profile ag-aaa-profile accounting 802.1x "alu-authserver"
aaa profile ag-aaa-profile device-authentication mac "alu-authserver"
aaa profile ag-aaa-profile accounting mac "alu-authserver"
aaa profile ag-aaa-profile device-authentication captive-portal "alu-authserver"
aaa profile ag-aaa-profile accounting captive-portal "alu-authserver"
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block
vlan 20 admin-state enable name vlan-corporate
vlan 30 admin-state enable name vlan-guest
```

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic on classification rule match.

5. Create the required UNP edge-profiles

```
unp edge-profile corporate
unp edge-profile guest
```

6. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile corporate vlan 20
unp vlan-mapping edge-profile guest vlan 30
```

7. Create a default profile

```
unp edge-profile default-profile
```

8. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

9. Create an edge-template

**unp edge-template auth-template**

10. Update the default profile for the edge-template

**unp edge-template auth-template default-edge-profile guest**

11. Enable MAC authentication/802.1x on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return a UNP edge-profile on authentication pass.

**unp edge-template auth-template mac-authentication enable**

**unp edge-template auth-template 802.1x-authentication enable**

**unp edge-template auth-template mac-authentication pass-alternate edge-profile corporate**

**unp edge-template auth-template 802.1x-authentication pass-alternate edge-profile corporate**

12. Assign the edge-template to a port

**unp port 2/1/1 edge-template auth-template**

13. Create the Captive Portal profile

**captive-portal-profile cp-profile**

**captive-portal-profile cp-profile aaa-profile ag-aaa-profile**

14. Add Captive Portal authentication pass policy list

**captive-portal-profile cp-profile authentication pass policy-list cp-default-list**

15. Create an edge-profile with Captive Portal enabled and assign the Captive Portal profile to the edge-profile with Captive Portal enabled. Associate the default-edge-profile with the VLAN that you expect the client to be in.

**unp edge-profile guest captive-portal-authentication enable**

**unp edge-profile guest captive-portal-profile cp-profile**

Traffic arriving on the port will trigger the following on the switch:

- Supplicant device traffic will trigger 802.1 x authentications first.
- On 802.1x authentication pass, the client is assigned to UNP corporate/vlan 20 or the UNP profile returned from RADIUS server.
- On 802.1x authentication fail, if classification is not enabled, the default edge-profile associated with the port is assigned. The default edge-profile should be enabled for Captive Portal authentication.
- For non-supplicant users, if MAC-authentication is enabled, MAC authentication is triggered.
- If MAC authentication pass, the client is assigned to UNP corporate or the UNP edge-profile returned from RADIUS server.

- On MAC authentication fail, if classification is not enabled, the default edge-profile associated with the port is assigned. The default edge-profile should be enabled for Captive Portal authentication.
- The Captive Portal pass policy may assign a new access policy list or the default access policy list of the default edge-profile
- The Captive Portal fail policy should result in client remaining in the Captive Portal pre login built-in role.

#### **4.6 USE CASE 5/6: Supplicant IP phone/non-supplicant, Network Policy TLV - tagged enabled on switch (single device on port)**

This use case supports tagged traffic on a UNP edge-port. Usually tagged traffic is not honored on a UNP edge-port. The use case consists of 2 scenarios.

- An IP phone enabled for LLDP Network Policy TLV and the switch to which the IP phone is connected is configured to send a Network Policy TLV of tagged VLAN.
- An IP phone is statically configured to tag traffic with a specific VLAN.

The expected configuration:

- The VLAN associated with the profile the phone is expected to be assigned to must be tagged on the port after authentication, if any of the above scenarios is true.
- This is achieved in different ways in AOS 6.x and AOS 8.x. The configuration section below will illustrate this difference.

The traffic flow expected is as follows:

1. It is expected that EAP frames are the first frames sent by the IP phone on link-up. EAP frames are untagged.
2. In AOS 8.x:
  - a. If supplicant phone, 802.1x authentication is initiated. If non-supplicant phone, MAC authentication is initiated.
  - b. A RADIUS server must be configured to return the correct UNP edge-profile for voice device on authentication pass.
  - c. If the RADIUS server is not configured to return the UNP edge-profile, then the 802.1x/MAC authentication pass alternate edge-profile will be applied. The VLAN associated with pass-alternate UNP should have mobile-tag enabled.
  - d. If 802.1x fail should be set to block. MAC authentication fail must be enabled for LLDP IP phone classification.
3. The VLAN assigned after authentication/classification pass should be the same VLAN referred to in the scenarios above, i.e. the VLAN enabled for mobile-tag, the VLAN in the LLDP Network TLV advertisement and in the case of AOS 8.x, the VLAN associated with the edge-profile to be assigned to the IP phone.
4. This VLAN should be tagged on the port, so that the traffic to /from the IP phone can be tagged
5. LLDP frames are exchanged between phone and the switch. This will be untagged but will be accepted into the CPU since these are control frames.
6. Subsequent data traffic will be tagged with the right VLAN after LLDP exchange and this will be accepted since the VLAN is a tagged member of the port.

The configuration steps are as follows:

1. Configure a RADIUS server

```
aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2  
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile

```
aaa profile "ag-aaa-profile"  
aaa profile ag-aaa-profile device-authentication 802.1x "alu-authserver"  
aaa profile ag-aaa-profile accounting 802.1x "alu-authserver"  
aaa profile ag-aaa-profile device-authentication mac "alu-authserver"  
aaa profile ag-aaa-profile accounting mac "alu-authserver"  
aaa profile ag-aaa-profile device-authentication captive-portal "alu-authserver"  
aaa profile ag-aaa-profile accounting captive-portal "alu-authserver"
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block  
vlan 20 admin-state enable name vlan-corporate  
vlan 30 admin-state enable name vlan-guest  
vlan 40 admin-state enable name vlan-voice
```

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic on classification rule match.

5. Create the required UNP edge-profiles

```
unp edge-profile corporate  
unp edge-profile guest  
unp edge-profile corporate-voice
```

6. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile corporate vlan 20  
unp vlan-mapping edge-profile guest vlan 30  
unp vlan-mapping edge-profile corporate-voice vlan 40
```

7. Enable mobile-tag on the edge-profile

```
unp edge-profile corporate-voice mobile-tag enable
```

8. Create a default profile

```
unp edge-profile default-profile
```



9. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

10. Create an edge-template

```
unp edge-template voice-template
```

11. Update the default profile for the edge-template

```
unp edge-template voice-template default-edge-profile default-profile
```

12. Enable MAC authentication/802.1x on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return a UNP edge-profile on authentication pass.

```
unp edge-template voice-template 802.1x-authentication enable
```

```
unp edge-template voice-template mac-authentication enable
```

```
unp edge-template voice-template classification enable
```

```
unp edge-template voice-template 802.1x-authentication pass-alternate edge-profile corporate-voice
```

13. Assign the edge-template to a port

```
unp port 3/1/1-2 edge-template voice-template
```

14. Enable LLDP IP phone classification

```
unp classification lldp med-endpoint ip-phone edge-profile corporate-voice
```

15. Configure LLDP on port

```
lldp port 3/1/1-2 lldpdu TX-AND-RX
```

```
lldp network-policy 1 application voice vlan 40 l2-priority 6
```

```
lldp port 3/1/1-2 med network-policy 1
```

#### ***4.7 USE CASE 7: Multiple devices per UNP port. Supplicant IP phone connected to switch with non-supplicant laptop connected to IP phone (multiple devices per port)***

This use case addresses the scenario of multiple devices per UNP port. This use case consists of a supplicant IP phone with a laptop connected to it. The IP phone may be in one of the following two states:

- An IP phone enabled for LLDP Network Policy TLV and the switch to which the IP phone is connected is configured to send a Network Policy TLV of tagged VLAN.
- An IP phone is statically configured to tag traffic with a specific VLAN.

The expected configuration is the same as that for use cases 5/6:

- The VLAN associated with the profile the phone is expected to be assigned to must be tagged on the port after authentication, if any of the above scenarios is true.
- This is achieved in different ways in AOS 6.x and AOS 8.x. The configuration section below will illustrate these differences.

The expected traffic flow expected is as follows:

1. It is expected that EAP frames are the first frames sent by the IP phone on link-up. EAP frames are untagged.
2. In AOS 8.x:
  - a. The supplicant phone first sends EAP frames; 802.1x authentication is initiated.
  - b. The RADIUS server must be configured to return the correct UNP edge-profile for voice device on authentication pass.
  - c. If the RADIUS server is not configured to return the UNP edge-profile, then the 802.1x authentication pass alternate edge-profile will be applied. The VLAN associated with pass-alternate UNP should have mobile-tag enabled
  - d. If 802.1x fail should be set to block.
3. The VLAN assigned to the phone after authentication/classification pass should be enabled for mobile-tag (the VLAN in the LLDP Network TLV advertisement and in the case of AOS 8.x the VLAN associated with the edge-profile to be assigned to the IP phone).
4. This VLAN should be tagged on the port, so that the traffic to/from the IP phone can be tagged.
5. LLDP frames are exchanged between the phone and the switch. This will be untagged but will be accepted into the CPU since these are control frames.
6. Subsequent data traffic from the phone will be tagged with the right VLAN after LLDP exchange and this will be accepted since the VLAN is a tagged member of the port.
7. Subsequently, the non-supplicant laptop will send traffic to the same physical port through the phone.
8. Since the MAC is unknown MAC , MAC authentication is triggered
9. In AOS 8.x
  - a. On MAC authentication pass, client should be assigned a UNP returned from RADIUS or group mobility is enabled or default UNP is assigned
  - b. On MAC authentication fail, client undergoes classification if enabled or assigned the default edge-profile.

The configuration steps are follows:

1. Configure a RADIUS server

```
aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile

```
aaa profile "ag-aaa-profile"
aaa profile ag-aaa-profile device-authentication 802.1x "alu-authserver"
aaa profile ag-aaa-profile accounting 802.1x "alu-authserver"
```

```
aaa profile ag-aaa-profile device-authentication mac "alu-authserver"  
aaa profile ag-aaa-profile accounting mac "alu-authserver"  
aaa profile ag-aaa-profile device-authentication captive-portal "alu-authserver"  
aaa profile ag-aaa-profile accounting captive-portal "alu-authserver"
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block  
vlan 20 admin-state enable name vlan-corporate  
vlan 30 admin-state enable name vlan-guest  
vlan 40 admin-state enable name vlan-voice
```

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic on classification rule match.

5. Create the required UNP edge-profiles

```
unp edge-profile corporate  
unp edge-profile guest  
unp edge-profile corporate-voice
```

6. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile corporate vlan 20  
unp vlan-mapping edge-profile guest vlan 30  
unp vlan-mapping edge-profile corporate-voice vlan 40
```

7. Enable mobile-tag on the edge-profile

```
unp edge-profile corporate-voice mobile-tag enable
```

8. Create a default profile

```
unp edge-profile default-profile
```

9. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

10. Create an edge-template

```
unp edge-template voice-template
```

11. Update the default profile for the edge-template

**unp edge-template voice-template default-edge-profile default-profile**

12. Enable MAC authentication/802.1x on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return a UNP edge-profile on authentication pass.

**unp edge-template voice-template 802.1x-authentication enable**

**unp edge-template voice-template mac-authentication enable**

**unp edge-template voice-template classification enable**

**unp edge-template voice-template 802.1x-authentication pass-alternate edge-profile corporate-voice**

13. Assign the edge-template to a port

**unp port 3/1/1-2 edge-template voice-template**

14. Enable LLDP IP Phone classification

**unp classification lldp med-endpoint ip-phone edge-profile corporate-voice**

15. Configure LLDP on port

**lldp port 3/1/1-2 lldpdu TX-AND-RX**

**lldp network-policy 1 application voice vlan 40 l2-priority 6**

**lldp port 3/1/1-2 med network-policy 1**

#### **4.8 USE CASE 8/9: 802.1x bypass MAC auth (with blacklist/or whitelist)**

In some deployments it is always required to initiate MAC authentication before 802.1x authentication even if the switch receives an EAP frame from the client. The use case is to initiate 802.1x only if the device/client is valid. The 802.1x bypass feature allows this.

The deployments implement this in different ways. The MAC authentication may be used to authenticate against a server that has a list of either blacklist MACs or whitelist MACs.

- If blacklist MACs are in the authentication server, then MAC authentication pass means the client is not further authenticated using 802.1x, i.e. allow-eap only after MAC authentication fail.
- If whitelist MACs are in the authentication server, then MAC authentication pass means the client is valid and is required to go ahead with 802.1x authentication, i.e. allow-eap only after MAC authentication pass.
- The third case is to not perform 802.1 x authentications after MAC Authentication, i.e. allow-eap is none.
- The fourth case is to perform 802.1 x authentications only if MAC authentication was not done, i.e. allow-eap only on noauth.

This use case covers supplicant corporate devices/guest devices trying to get access to the network on the same port. There are differences between how AOS 6.x and AOS 8.x handle the various

scenarios.

The configuration steps are as follows:

1. Configure a RADIUS server

```
aaa radius-server "alu-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile

```
aaa profile "ag-aaa-profile"
aaa profile ag-aaa-profile device-authentication 802.1x "alu-authserver"
aaa profile ag-aaa-profile accounting 802.1x "alu-authserver"
aaa profile ag-aaa-profile device-authentication mac "alu-authserver"
aaa profile ag-aaa-profile accounting mac "alu-authserver"
aaa profile ag-aaa-profile device-authentication captive-portal "alu-authserver"
aaa profile ag-aaa-profile accounting captive-portal "alu-authserver"
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block
vlan 20 admin-state enable name vlan-corporate
vlan 30 admin-state enable name vlan-guest
```

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic on classification rule match.

5. Create the required UNP edge-profiles

```
unp edge-profile corporate
unp edge-profile guest
```

6. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile corporate vlan 20
unp vlan-mapping edge-profile guest vlan 30
```

7. Create a default profile

```
unp edge-profile default-profile
```

8. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

9. Create an edge-template

```
unp edge-template auth-template
```

10. Update the default profile for the edge-template

```
unp edge-template auth-template default-edge-profile guest
```

11. Enable MAC authentication/802.1x on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return a UNP edge-profile on authentication pass.

```
unp edge-template auth-template mac-authentication enable
```

```
unp edge-template auth-template 802.1x-authentication enable
```

```
unp edge-template auth-template 802.1x-authentication bypass enable
```

If MAC authentication is blacklist

```
unp edge-template auth-template mac-authentication allow-eap fail
```

If MAC authentication is whitelist

```
unp edge-template auth-template mac-authentication allow-eap pass
```

```
unp edge-template auth-template 802.1x-authentication pass-alternate edge-profile corporate
```

12. Assign the edge-template to a port

```
unp port 2/1/1 edge-template auth-template
```

## ***4.9 USE CASE 10: Post-authentication role assignment (QMR, Location- and Time-based Roles)***

This use case is applicable to post-authentication for all of the USE CASES 1 to 9 defined above. QMR is not a property of edge-profile. Location/Time-based policies are enabled per edge-profile. The post authentication edge-profile assigned to the client should be enabled for Location/Time-based policy classification.

### **4.9.1 QMR**

QMR can work on UNP edge-ports and non-UNP ports. This document only focuses on UNP edge-ports. A client MAC is determined to be in quarantine state when the OmniVista receives a TRAP indicating the MAC has to be quarantined, or the list may be manually configured on the OmniVista for every switch in the network. The TRAP can come from the OmniSwitch 6850 based on the network anomaly detection application or could come from an IDS running in the same subnet as the client. After the list of MACs is known, the OmniVista can add MAC to the Quarantine MAC group and push the configuration to the switches in the logical group or to all switches. Access Guardian should move the users with the MAC to a Quarantine role.

This feature has the following configurations:

1. Command to assign a new QMR policy list to replace the built-in QMR policy list. This is an optional command.

**unp restricted-role QMR policy-list <name>**

2. Create the Quarantine MAC Group. This is an optional command because the system has a default Quarantine MAC Group “Quarantined”.

**qos quarantine MAC-GROUP <name>**

3. Apply the QoS configuration for the MAC GROUP to take effect.

**qos apply**

4. Create the path to the remediation server. There is no default value.

**qmr quarantine path [www.remediate.com](http://www.remediate.com)**

5. The IP address/subnet of the remediation server should be added as part of the list of allowed IP addresses to which the client is allowed to communicate in Quarantined state.

**qmr quarantine allowed-name 10.242.254.105**

6. If there is no quarantine path to redirect to, then a quarantine page may be configured to inform the user of the Quarantine state.

**qmr quarantine page {enable | disable}**

## 4.9.2 Time policy

The time policy defines the validity period for which the client is assigned the determined role (policy list). For the time interval outside of the validity period the client is in “unauthorized” role. There is a built-in policy list associated with the unauthorized role. This policy list can be replaced by a user-defined policy list. Different validity periods may be created. One validity period policy can be assigned to each edge-profile as required and this is enforced post authentication.

1. Create different validity periods as required. Different validity periods can be defined and assigned to different UNP edge-profiles.

**unp policy validity-period employee-shift-time days Monday tuesday wednesday thursday friday  
timezone PST hours 6:00 TO 18:00**

**unp policy validity-period guest-time days Monday tuesday wednesday thursday friday saturday  
sunday timezone PST hours 9:00 TO 18:00**

2. Assign to different UNP

**unp edge-profile UNP-employee period-policy employee-shift-time**

**unp edge-profile UNP-guest period-policy guest-time**

3. Optionally define a new policy list for unauthorized role. The creation of the policy list is already described in previous use cases.

**unp restricted-role unauthorized policy-list custom-unauthorized**

### 4.9.3 Location policy

The location policy defines the validity period for which the client is assigned the determined role (policy list). For the time interval outside of the validity period the client is in “unauthorized” role. There is a built-in policy list associated with the unauthorized role. This policy list can be replaced by a user-defined policy list. Different validity periods may be created. One validity period-policy can be assigned to each edge-profile as required and this is enforced post authentication.

1. Create different location policies as required and assign to appropriate edge-profiles. Location policies can be created based on linkagg, port, system-location or system-name. The following example shows that UNP edge-profile that has the following location policy will allow access only if clients assigned to this edge-profile come in on the following ports. The clients in the edge-profile coming in on other ports will be assigned unauthorized role.

**unp policy validity-location employee-location port 1/1/1-24**

**unp edge-profile UNP-employee location-policy employee-location**

**unp policy validity-location guest-location port 1/1/15-24**

**unp edge-profile UNP-guest period-policy guest-location**

## 5 Access Guardian BYOD with CPPM Integration

The AOS Unified Access-BYOD solution with AG in AOS 8.1.1 consists of integration with the Aruba ClearPass Policy Manager (CPPM) v6.3.

The solution uses the RADIUS (RFC 3576) Change of Authorization (COA) to achieve this functionality. Integration with the CPPM and the use of the OmniVista Next Gen provides the following feature enhancements:

- Unified Access Policy Management solution for wired and wireless devices
- Standardized RADIUS COA between the switch and the CPPM
  - Provides the ability for the CPPM to force a change of UNP profile (in AOS 6.x) or UNP edge-profile and access-policy-list (in AOS 8.x)
  - Additionally this interface provides the ability for the CPPM to send a redirection URL to the switches so that the http/https traffic could be redirected to a guest registration/onboard portal or to a remediation portal for host integrity compliance
- Guest Access (Sponsored or Self Registration) - using the CPPM Guest module



- Onboarding of devices - using the CPPM Onboard module
- Posture check - using the CPPM OnGuard module
- Device Profiling - using the DHCP fingerprinting capability of CPPM

Figure 4. Functions of CPPM components

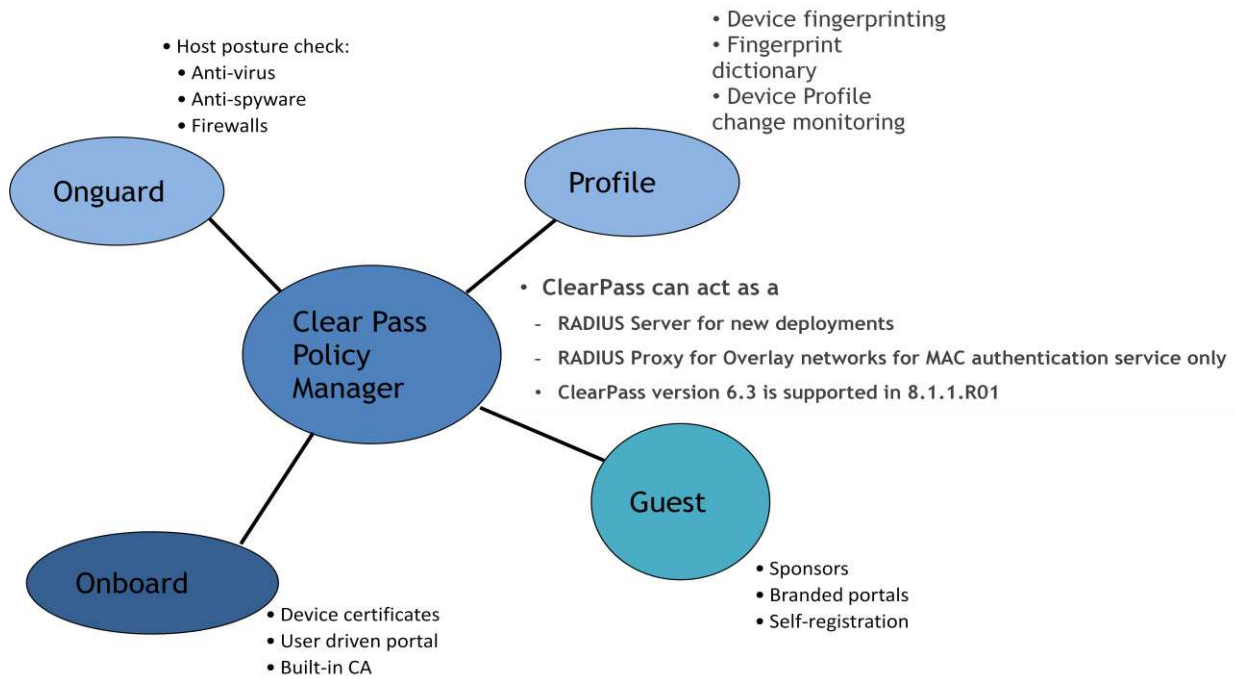
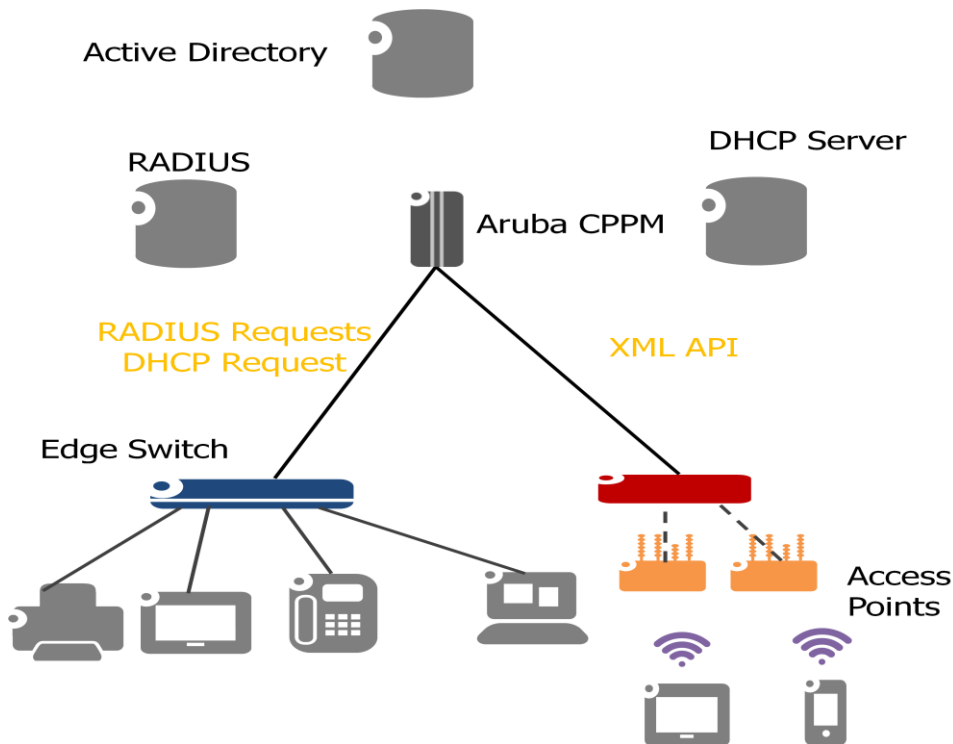


Figure 5. Components of the BYOD solution



The edge switch must be either OmniSwitch 6850E with AOS 6.4.6 or OmniSwitch 6450 with AOS 6.6.5 or OmniSwitch 6860/OmniSwitch 6860E with 8.1.1.

ClearPass Onboard automates 801.1x configuration and provisioning for BYOD and IT-managed devices - Windows, MAC OS X, iOS and Android wired, wireless and VPNs. This allows network administrators control over the consumer devices that are connected to an enterprise network.

## **5.1 Use Case Summary**

Consider a network with ports that can support employees with IT-issued devices, employees with BYOD devices, guests, specific vendors' IP phones and printers.

The employee user and IT-issued device credentials are in the external Active Directory Server. The IP phone information is created in a database of type Static Host List in the CPPM local database. The printer information is created in a database of type Static Host List in the CPPM local database. The guest accounts are created through self-registration or sponsored and will be created in the Guest User Repository using the guest module.

If Posture check is enabled for BYOD and guest devices, then the posture check has to be enabled post authentication of guest/BYOD users.

## **5.2 Pre-Requisite Switch Configuration**

The BYOD solution works in the framework of Access Guardian on the switch and requires the following configurations:

### **1. Specification of RADIUS server**

The RADIUS server must be configured as the CPPM.

```
aaa radius-server "cppm-authserver" host 10.242.254.102 key secret retransmit 3 timeout 2  
auth-port 1812 acct-port 1813
```

In AOS 8.x, different aaa profiles could be created to point to different RADIUS servers for each authentication method. This way a switch may operate with integration with CPPM on certain ports of the system and with a different set of RADIUS servers on others. Examples of assignment of the RADIUS servers to authentication methods are already shown in previous section.

### **2. Configuration of allowed list of IP addresses in addition to the CPPM server (optional)**

This is required if the clients have to be redirected to a remediation server that is not the CPPM server. Up to 5 allowed IP addresses can be configured.

```
unp redirect allowed-name remediation-server ip-address 10.242.254.103 ip-mask 255.255.255.0
```

### 3. Configuration to trigger port bounce or port timer on a port (port bounce is enabled by default on edge-port)

This feature is required to handle scenarios where a client is switched from one VLAN to another after COA. If port bounce is enabled, this means the port will be administratively put down. This is to trigger DHCP renewal and sometimes re-authentication. For cases where a port bounce is not an option, for example in case of multiple devices on a port, it is expected to configure a pause timer. This is the timer for which the client's MAC is put in filtering. This is to allow for the client's DHCP lease time to expire and retrigger DHCP request. This will allow the client to get an IP address in the new VLAN it has been assigned.

```
unp group-id port-bounce {enable | disable}
```

```
unp {port | linkagg} {chassis/slot/port1-portn | linkagg id} redirect port-bounce {enable | disable}
or
```

```
unp edge-template template-name redirect port-bounce {enable | disable}
```

```
unp redirect pause-timer < timer-val> /* Only global configuration is supported */
```

### 4. Configuration of enable redirect

The solution allows for the switch to redirect http/https traffic to the CPPM, which is the redirect server. The CPPM is responsible for hosting the pages for guest registration and device on-boarding. It may be required to redirect the client to a server other than the CPPM for remediation. This can be enabled with the following configurations. The CPPM is also responsible for sending the link to the redirection URL in the RADIUS COA message. The RADIUS COA is accepted only if there is a RADIUS context containing the profile information associated with the client in the switch. The profile associated with the client must be enabled for redirection.

In order for the switch to redirect client traffic, the switch must have a context for the user with an edge-profile enabled for redirect and the CPPM must return a URL.

```
unp edge-profile <profile-name> redirect {enable | disable}
```

It is also required that the RADIUS server/redirect server are configured to point to the CPPM as shown.

```
unp redirect-server 10.242.254.102
```

### 5. Support of new RADIUS Vendor Specific Attributes (VSAs)

Three new RADIUS VSAs have been introduced to support BYOD:

1. Alcatel-Access-Policy-List
  - VSA ID: 100

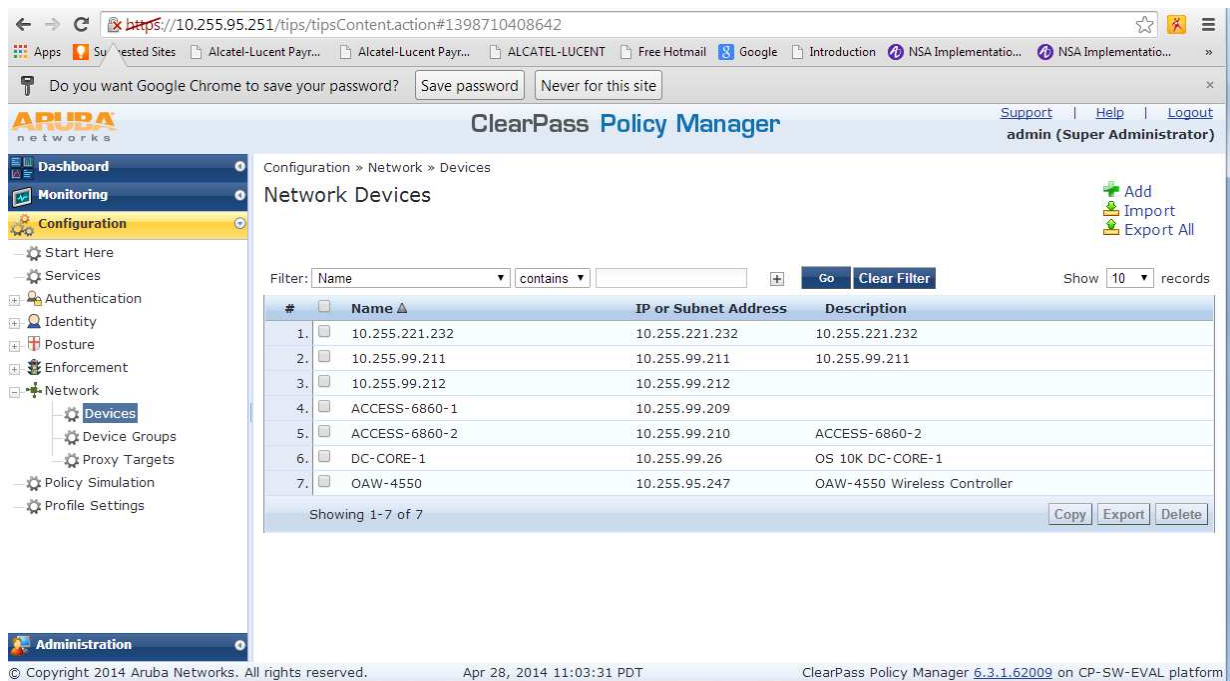
- **Description:** This attribute is used to return the Policy List from the CPPM. It can be used to send the Policy List from any RADIUS server capable of returning vendor-specific attributes.
2. **Alcatel-Redirection-URL**
    - **VSA ID:** 101
    - **Description:** This attribute is used to return the URL to which the switch is required to redirect all http/https traffic arriving from the client on a port. This must be sent along with the UNP edge-profile name returned in the RADIUS Filter-id attribute.
  3. **Alcatel-Redirection-Status (Not Used)**

### 5.3 Pre-Requisite CPPM Configuration

The CPPM may be directly configured by logging into the CPPM web interface or through the OmniVista Next Generation Network Management System. Listed below are the configurations that are directly done on the CPPM.

#### 5.3.1 Configure the AOS switches on CPPM for which CPPM is acting as the Policy Manager/RADIUS server

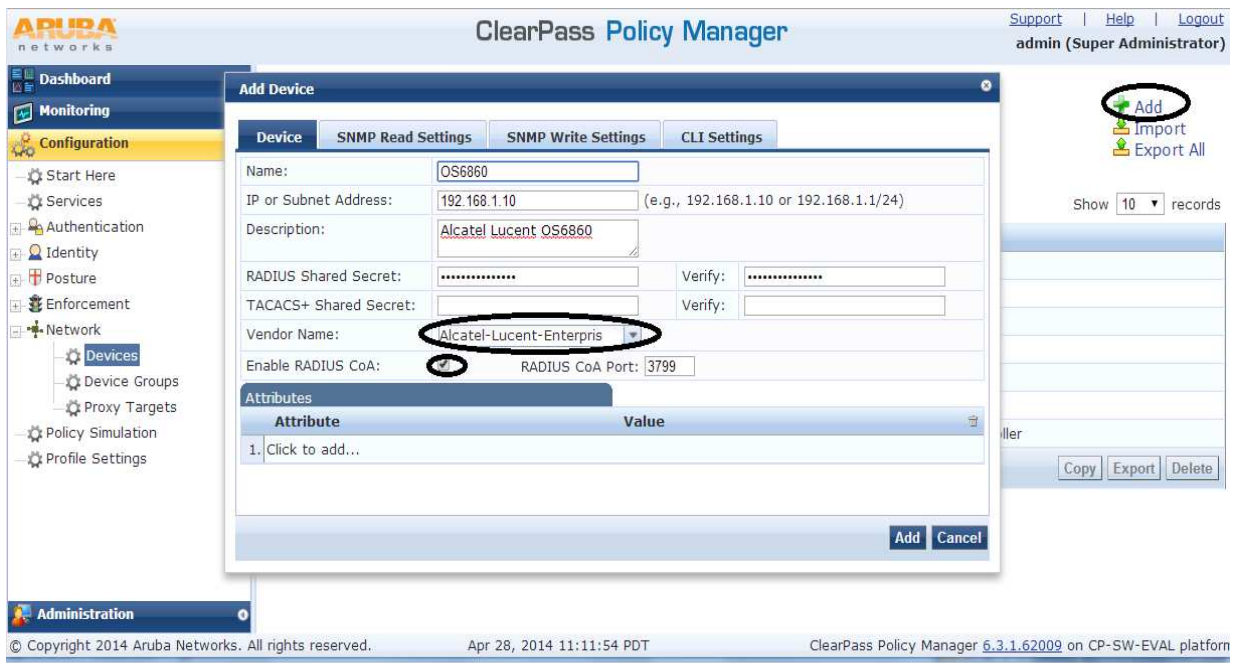
1. Configure the list of AOS Switches that the CPPM will interact with. Go to Configuration/Network/Devices tab on the left.



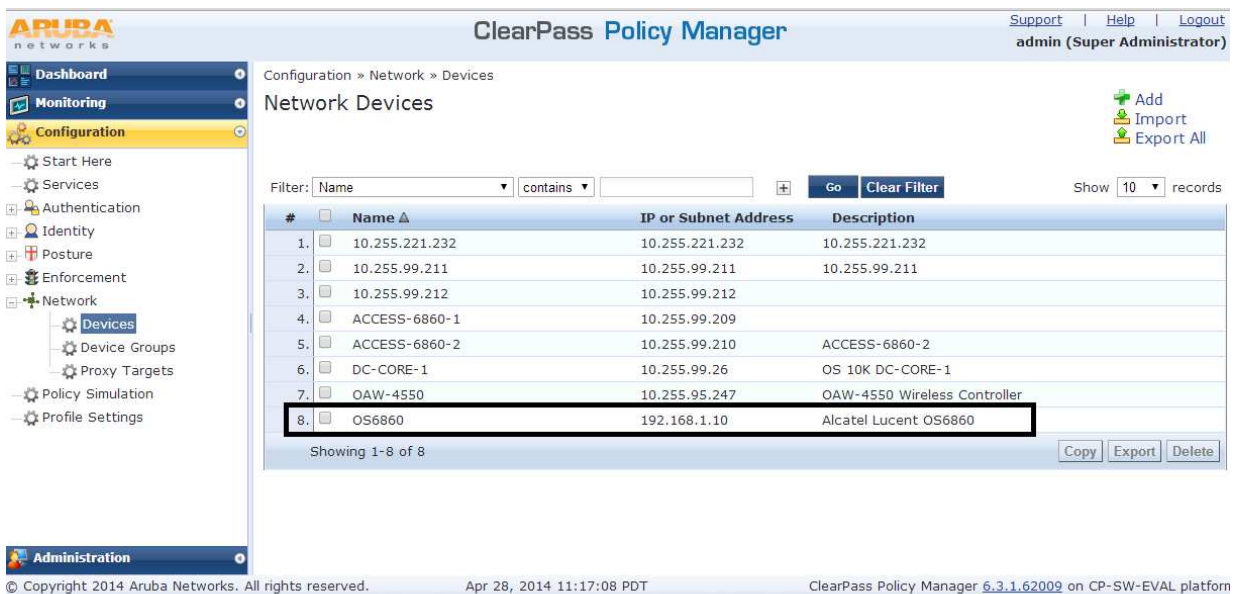
The screenshot shows the ClearPass Policy Manager web interface. The left sidebar is expanded to 'Configuration' > 'Network' > 'Devices'. The main content area shows a table of network devices. The table has columns for '#', 'Name', 'IP or Subnet Address', and 'Description'. There are 7 rows of data. Below the table, it says 'Showing 1-7 of 7'. At the bottom of the page, there is a footer with copyright information and version details.

#	Name	IP or Subnet Address	Description
1.	10.255.221.232	10.255.221.232	10.255.221.232
2.	10.255.99.211	10.255.99.211	10.255.99.211
3.	10.255.99.212	10.255.99.212	
4.	ACCESS-6860-1	10.255.99.209	
5.	ACCESS-6860-2	10.255.99.210	ACCESS-6860-2
6.	DC-CORE-1	10.255.99.26	OS 10K DC-CORE-1
7.	OAW-4550	10.255.95.247	OAW-4550 Wireless Controller

2. To add individual devices: Select Add and provide the name, IP address and description of the switch to manage. Make sure to select Alcatel-Lucent-Enterprise for Vendor name and check "Enable RADIUS CoA". All switches have to be added to this list and this process can be made easier by using OmniVista. OmniVista will automatically populate this in the CPPM when the CPPM is configured as the RADIUS server by the switches.



The device is added.

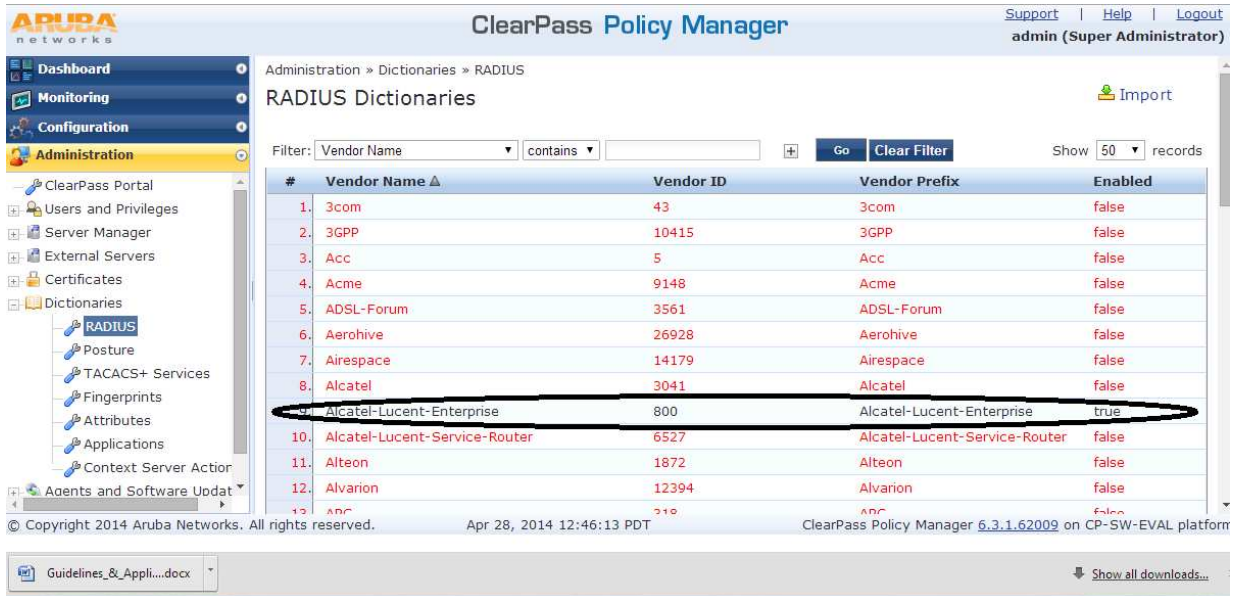


### 5.3.2 Update CPPM with latest Alcatel-Lucent Enterprise Dictionary

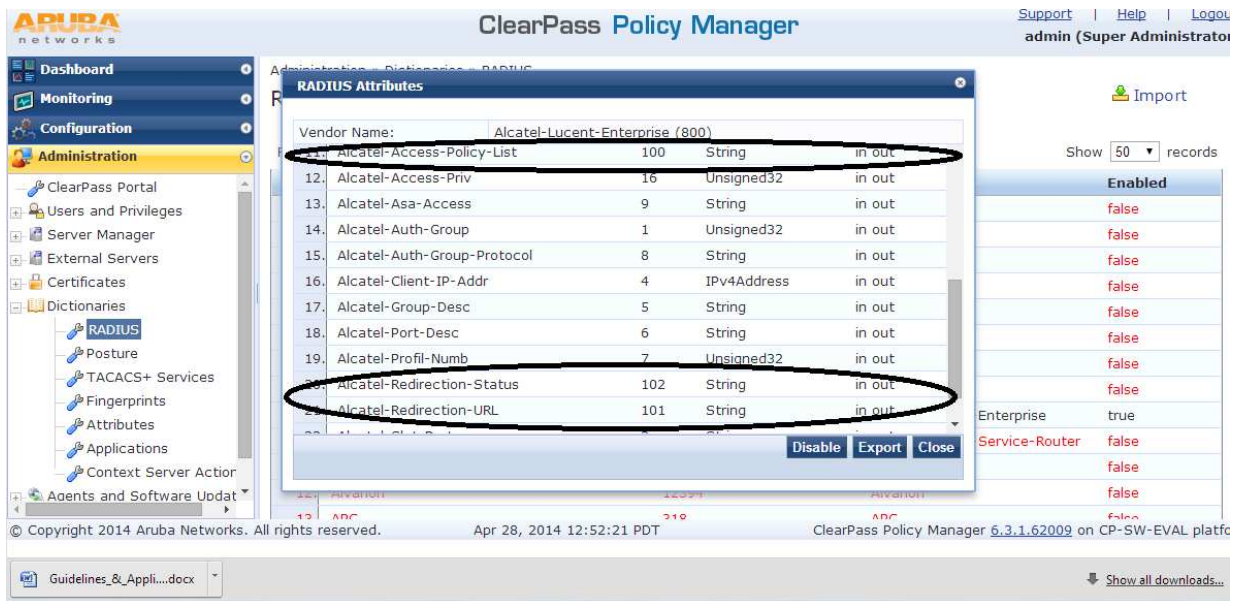
RADIUS Dictionary: The Access Guardian in AOS 8.1.1 has introduced three new Alcatel-Lucent vendor-specific attributes. Hence it is required to have the right dictionary files. The CPPM 6.3 should come preloaded with the new dictionary. Notice that the Vendor Name has changed from Xylan to Alcatel-Lucent Enterprise in the CPPM.

On the CPPM, go to Administration/Dictionaries/RADIUS to find the RADIUS dictionaries from

various vendors.



The three attributes are highlighted below. VSA ID 102 Alcatel-Redirection-Status is not used.



### 5.3.3 Configure CPPM to use an external AD server as an authentication source

1. Add external Active Directory Service if it will be used as one of the authentication sources against which the users are authenticated. Go to Configuration/Authentication/Sources. Select Add.

The screenshot shows the 'Authentication Sources' configuration page in ClearPass Policy Manager. The breadcrumb trail is 'Configuration » Authentication » Sources'. The page title is 'Authentication Sources'. In the top right corner, there are three buttons: 'Add', 'Import', and 'Export All'. The 'Add' button is circled in red. Below the buttons is a filter section with a dropdown for 'Name', a 'contains' operator, an input field, and 'Go' and 'Clear Filter' buttons. To the right of the filter is a 'Show 20 records' dropdown. The main content is a table with columns for '#', 'Name', 'Type', and 'Description'. The table lists 12 authentication sources, including various SQL DBs, Static Host Lists, and Active Directory services.

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	IXIA MACs	Static Host List	IXIA MACs
8.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
9.	MAC Authentication List	Static Host List	MAC Authentication List
10.	mac caching MAC-Guest-Check	Generic SQL DB	
11.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
12.	SQA Active Directory Service	Active Directory	SQA Active Directory Service

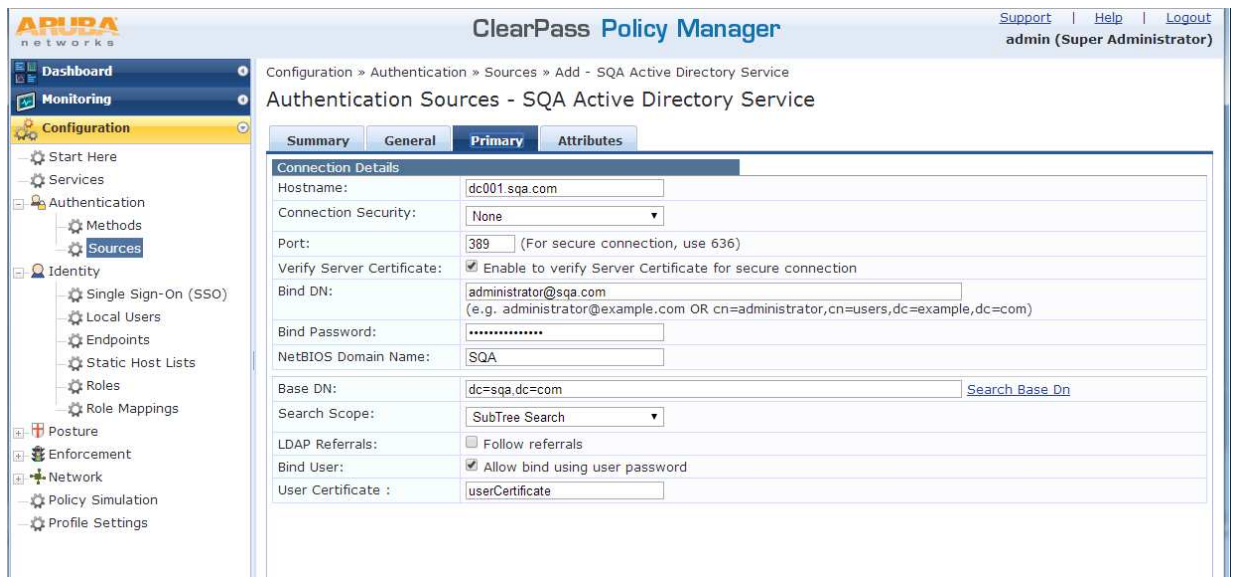
2. Update the general information for the Authentication source as shown below. The name/description could be the user's choice.

The screenshot shows the configuration page for the 'SQA Active Directory Service' in ClearPass Policy Manager. The breadcrumb trail is 'Configuration » Authentication » Sources » Add - SQA Active Directory Service'. The page title is 'Authentication Sources - SQA Active Directory Service'. There are four tabs: 'Summary', 'General', 'Primary', and 'Attributes'. The 'General' tab is selected. The form contains the following fields:

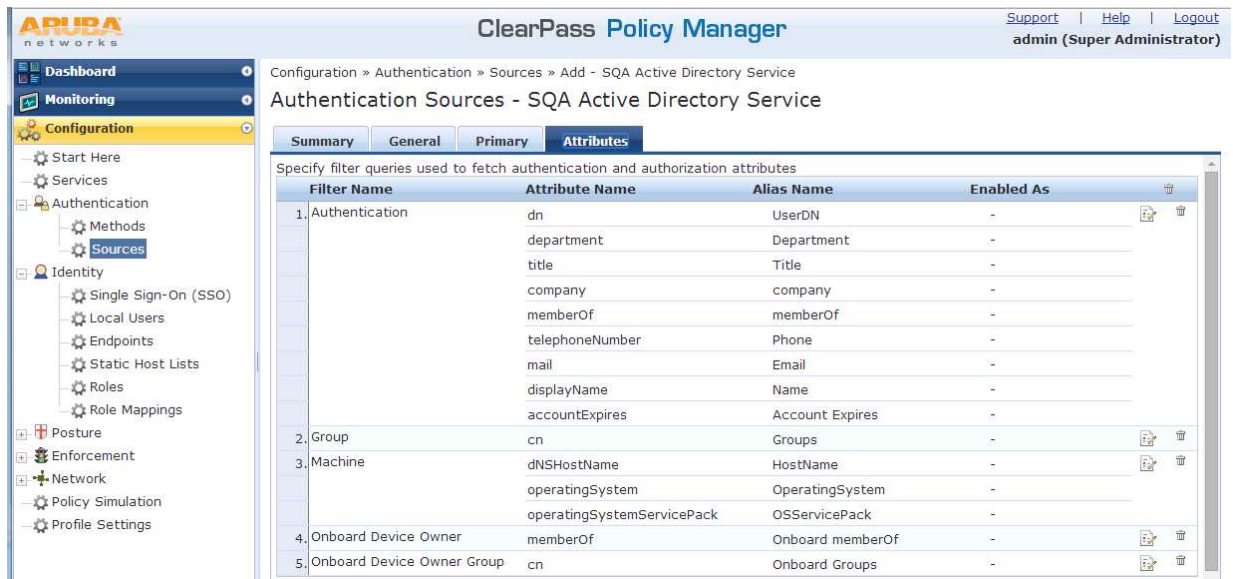
- Name: SQA Active Directory Service
- Description: SQA Active Directory Service
- Type: Active Directory
- Use for Authorization:  Enable to use this Authentication Source to also fetch role mapping attributes
- Authorization Sources: A dropdown menu with a 'Remove' button and a 'View Details' button.
- Server Timeout: 10 seconds
- Cache Timeout: 36000 seconds
- Backup Servers Priority: A list with 'Move Up', 'Move Down', 'Add Backup', and 'Remove' buttons.

3. Update additional information as according to the Active Directory configuration





- Retain the default for the attributes of the AD server that can be used for filtering information for the CPPM to use as shown below.

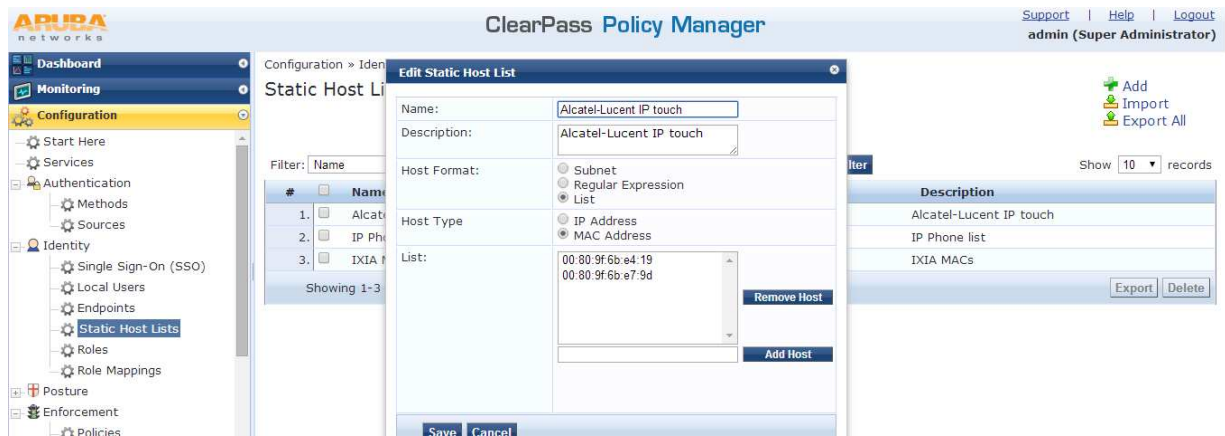


### 5.3.4 Configure Static Host List for IP phones/printer devices

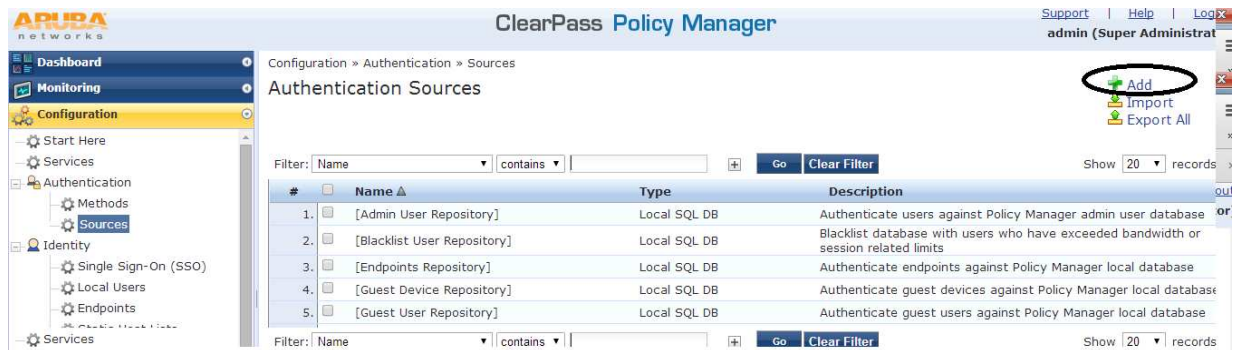
- Go to Configuration/Identify/Static Host List and Select Add. Create two lists: one for IP phone and another for printers, etc. The example shows only one list.



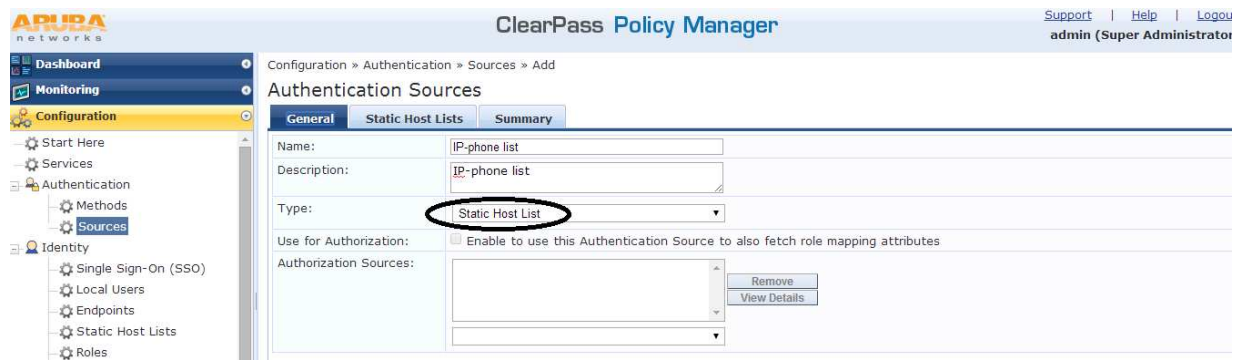
- Specify name, description and the list of MAC addresses of IP phones or a regular expression for range of IP addresses to match. Save and exit.



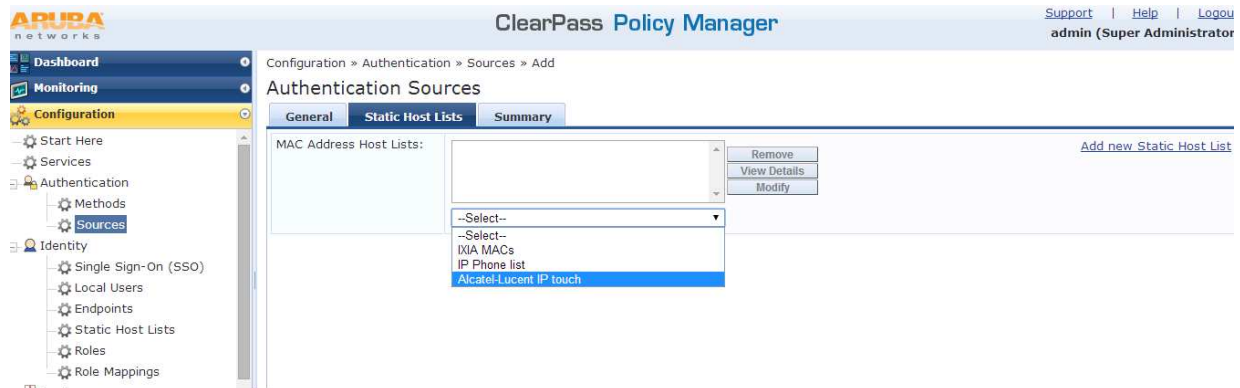
- Go to Configuration/Authentication/Sources and Click Add.



- Enter a name and description and select Type to be "Static Host List"



5. Select the IP phone list created



6. Create additional Authentication sources as required for the deployment.

## 5.4 AOS switch and CPPM integration points

### 5.4.1 Edge-profile, access policy list and redirection URL handling

1. The edge-profile and the access policy lists associated with the edge-profile are the property of the switch.
2. The edge-profile and the policy list may be configured in the OmniVista network management system and pushed to the AOS switches or the edge-profile, and the policy list may be configured directly on the AOS switches.
3. The CPPM can be configured to return three RADIUS attributes in a RADIUS response or a RADIUS COA response to the switch.

Following are the rules that apply to the policy list that is enforced on the AOS switch:

1. An edge-profile is not required to be associated with a policy list.
2. If the edge-profile is not associated a policy list then the default policy list is:
  - a. Allow-All for all the edge-profiles except for edge-profile of name UNP-restricted
  - b. UNP-restricted is a special edge-profile that has a Restricted built-in policy list
3. If the CPPM returns only an edge-profile:
  - a. The policy list associated with the edge-profile is applied if it is configured.
  - b. If there is no policy list configured, then a default "Allow-All" policy list is applied.
4. If the CPPM returns an edge-profile and a policy list in the RADIUS response:
  - a. The CPPM returned policy list is applied even if the edge-profile has a policy list associated with it.
5. If the CPPM returns an edge-profile and a Redirection URL in the RADIUS response:
  - a. The switch applies the built-in Restricted policy list that redirects all the http traffic to the redirection URL returned by the CPPM server.

6. A user may define a new restricted policy list, but this has to be configured on the switch and the policy list name must be returned in the RADIUS attribute returned from the CPPM.

## 5.5 BYOD USE CASE 1: Guest access

This is the use case for guest access to the network. The workflow for guest access is as follows:

1. Guest device sends traffic to the switch. The switch initiates MAC authentication to the CPPM.
2. CPPM MAC authentication service is configured to return a restricted UNP edge-profile role to the user. This role redirects all http/https traffic to the guest registration page.
3. This allows the user to self-register or use the sponsored user name/password.
4. Based on Captive Portal Service, the CPPM verifies that the user is authorized to access the network and returns an appropriate edge-profile via RADIUS COA message back to the switch.

### 5.5.1 Switch configuration

1. Configure a RADIUS server to point to the CPPM

```
aaa radius-server "cppm-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile - provides the authentication server to use for an authentication method and other RADIUS attribute format configurations

```
aaa profile "byod-aaa-profile"
aaa profile byod-aaa-profile device-authentication mac "cppm-authserver"
aaa profile byod-aaa-profile accounting mac "cppm-authserver"
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block
vlan 30 admin-state enable name vlan-guest
vlan 40 admin-state enable name vlan-voice
vlan 1000 admin-state enable name vlan-restricted
```

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic for full access post authentication. The restricted edge-profile "UNP-restricted" has a default built-in policy list that allows the user to be redirected to the redirect server that is configured as shown in the previous section.

A policy list may be defined for guest-role:

```
policy condition guest-condition source ip 10.255.30.0 mask 255.255.255.0 destination Any
policy action guest-action
policy rule guest-rule condition guest-condition action guest-action
policy list guest-role type unp
```

**policy list guest-role rules guest-rule**

5. Create the required UNP edge-profiles and associate to guest VLAN

**unp edge-profile UNP-guest**

**unp vlan-mapping edge-profile UNP-guest vlan 30**

**unp edge-profile UNP-guest qos-policy-list guest-role**

6. Create a default profile and associated to vlan 10

**unp edge-profile default-profile**

**unp vlan-mapping edge-profile default-profile vlan 10**

7. Create a restricted profile and associate to restricted vlan 1000

**unp edge-profile UNP-restricted**

**unp vlan-mapping edge-profile UNP-restricted vlan 1000**

8. Create a voice profile and associate to voice vlan 40

**unp edge-profile UNP-voice**

**unp vlan-mapping edge-profile UNP-voice vlan 40**

9. Create an edge-template, which sets the properties that can be applied to a set of edge-ports

**unp edge-template byod-template**

10. Enable MAC authentication on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return a UNP edge-profile on authentication pass.

**unp edge-template byod-template mac-authentication enable**

**unp edge-template byod-template mac-authentication pass-alternate edge-profile UNP-guest**

11. Assign the edge-template to a port

**unp port 2/1/1 edge-template byod-template**

## 5.5.2 CPPM configuration

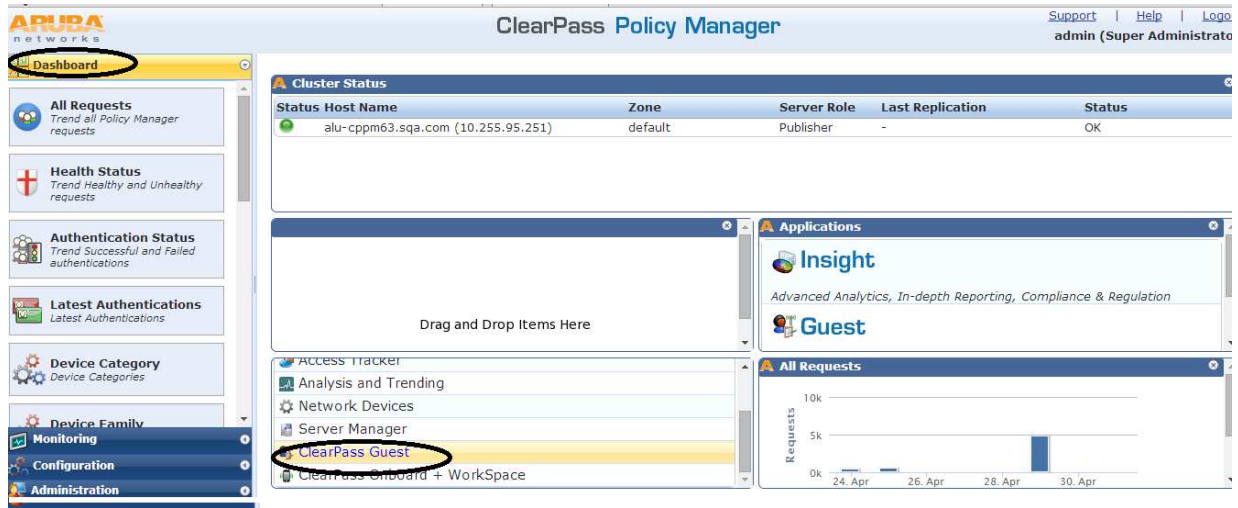
The CPPM configuration can be grouped into following three categories:

1. Configure the Captive Portal Page and Guest User Account.
2. Configure the required Enforcement Profiles and Policies.
3. Configure the MAC authentication service and the Captive Portal Web Authentication service.

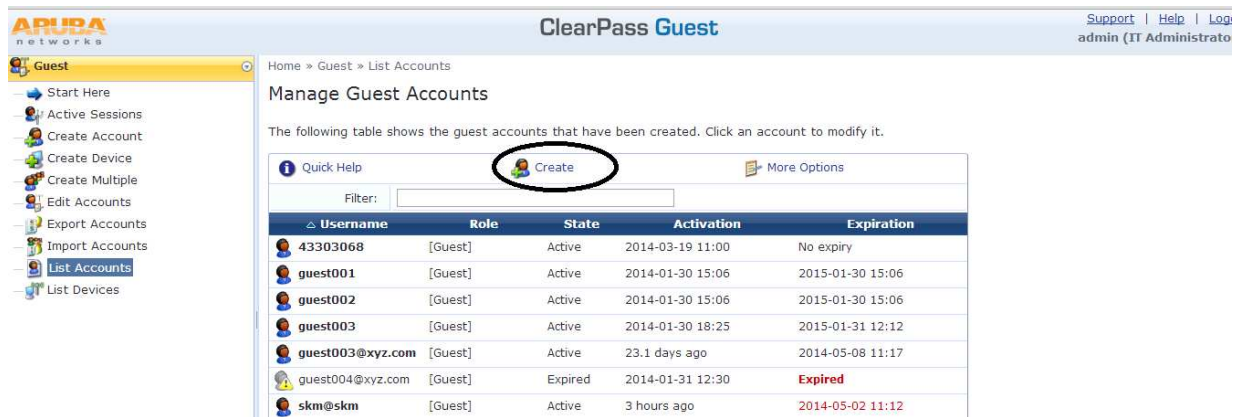
### 5.5.2.1 Configuring Guest User

Configuration steps are as follows:

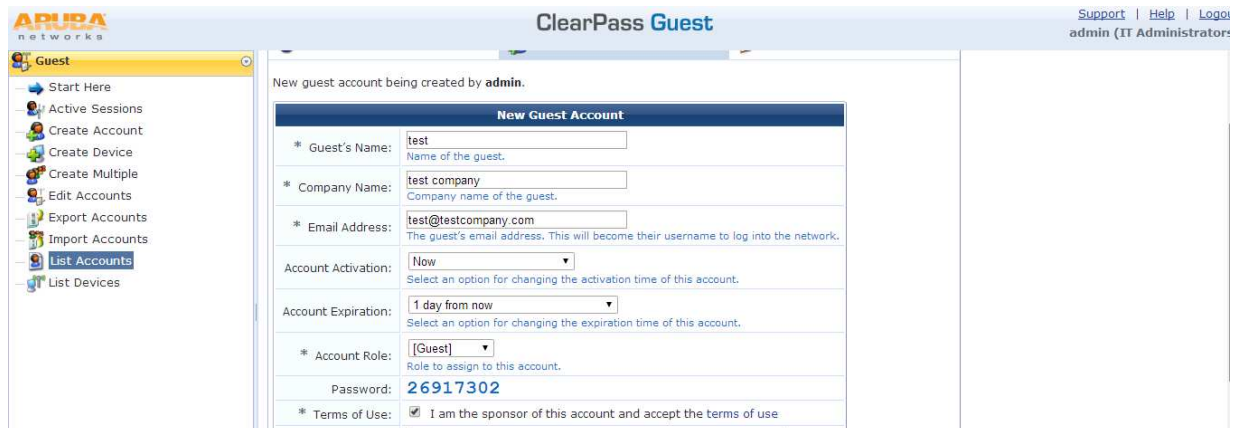
1. Go to Dashboard. Select ClearPass Guest as shown.



2. Go to Guest/List Accounts. Select Create.



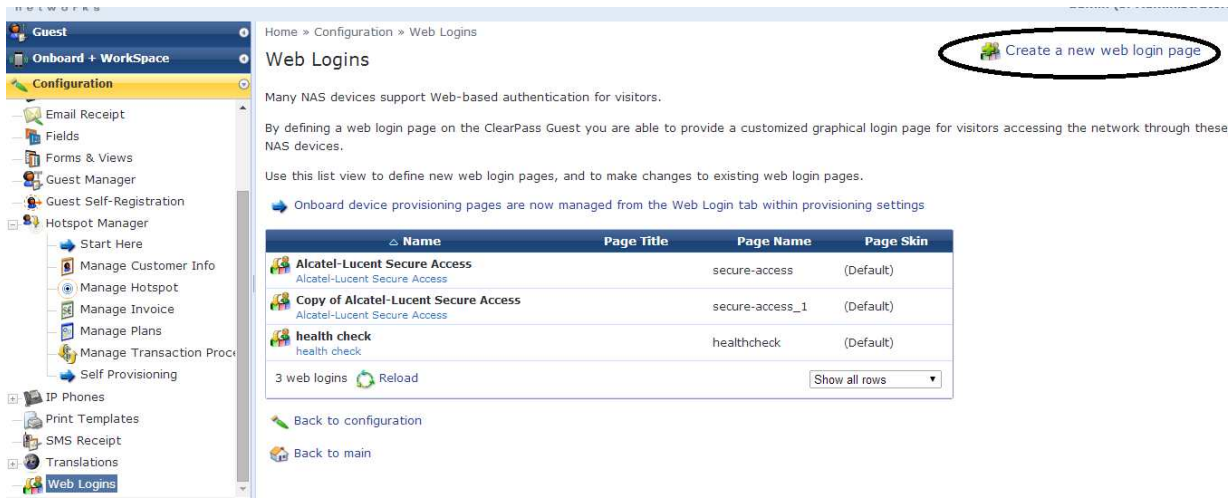
3. Create the visitor's name, company, email, username, password, activation time, validity period, user role, etc. as required by the form and Create Account. This creates the user in the Guest User database.



The user should be added and shown as part of the List Accounts.

### 5.5.2.2 Configuring Captive Portal Page

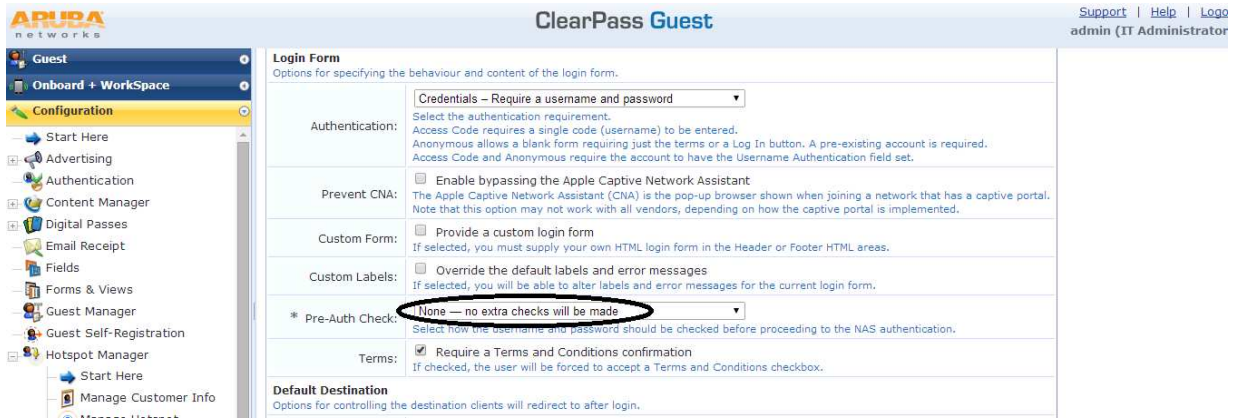
1. Go to Guest/Configuration/Web Login.
2. Select “Create a new web login page”.



3. Enter a name for the profile and provide the page name. If the name is secure-access, then the page is <http://cppm-ip-address/guest/secure-access.php>.
4. Set Vendor as Alcatel-Lucent. Select “server initiated RADIUS COA....”
5. Select “None” for pre-auth checks.



6. Select the default URL to send the client to after registration/login and select “override” of the user URL.
7. Select login delay of 5 and save changes.



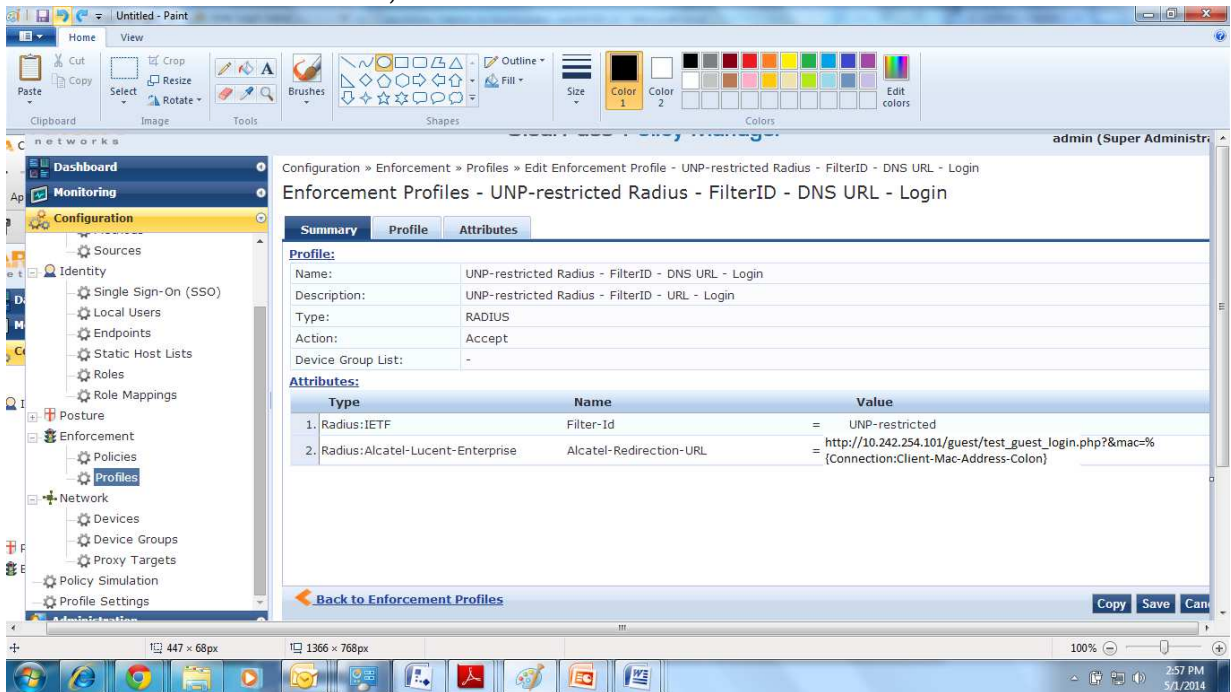
### 5.5.2.3 Configuring the enforcement profiles

Multiple enforcement profiles are needed:

1. Enforcement profile to return UNP-restricted to put the user in restricted role
2. Enforcement profile to return the role post user login

Create the enforcement profiles as follows:

1. Go back to the CPPM Page/Configuration/Enforcement/Profiles
2. Create a “Restricted Enforcement Profile”
  - a. Select Add and Enforcement Profile
  - b. Set Template with RADIUS-based enforcement
  - c. Enter name and description. Select defaults for the rest on this tab and go to Next.
  - d. Select Type - RADIUS:IETF, Name - Filter-Id(11), Value - UNP-restricted. Make sure to select UNP-restricted.
  - e. Add the second row with Type - RADIUS: Alcatel-Lucent Enterprise, Name - Alcatel-Redirection-URL, Value - URL shown below. Click Save.



3. Create a post-login “Guest COA Enforcement Profile”. This is returned using a RADIUS COA.
  - a. Select Add and Enforcement Profile.



- b. Set Template with RADIUS CoA-based enforcement.
- c. Enter name and description. Select defaults for the rest on this tab and go to Next.
- d. Select Type - RADIUS:IETF CoA, Name - Filter-Id(11), Value - UNP-guest and add Calling-Station-id and a RADIUS:Alcatel-Lucent-Enterprise - Access-Policy-List for guest role as shown below. Click Save.

The screenshot shows the ClearPass Policy Manager web interface. The browser address bar displays the URL: <https://10.255.95.251/tips/tipsContent.action#1398981569273>. The page title is "ClearPass Policy Manager". The user is logged in as "admin (Super Administrator)".

The navigation menu on the left includes: Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, and Administration. The "Configuration" menu is expanded, showing "Start Here", "Services", "Authentication", "Identity", "Posture", "Enforcement", and "Administration". The "Enforcement" menu is further expanded to show "Policies", "Profiles", and "Network".

The main content area shows the "Edit Enforcement Profile" page for the profile "UNP-guest CoA - FilterID - PolicyList". The "Summary" tab is selected, showing the following details:

Profile:		
Name:	UNP-guest CoA - FilterID - PolicyList	
Description:	UNP-guest CoA - FilterID	
Type:	RADIUS_CoA	
Action:	CoA	
Device Group List:	-	

The "Attributes" tab is also visible, showing a table of attributes:

Type	Name	Value
1. Radius:IETF	Filter-Id	= UNP-guest
2. Radius:IETF	Calling-Station-Id	= %{Radius:IETF:Calling-Station-Id}
3. Radius:Alcatel-Lucent-Enterprise	Alcatel-Access-Policy-List	= guest-role

At the bottom of the page, there is a "Back to Enforcement Profiles" link and buttons for "Copy", "Save", and "Cancel". The footer of the page includes: "Copyright 2014 Aruba Networks. All rights reserved.", "May 01, 2014 14:31:32 PDT", and "ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform".

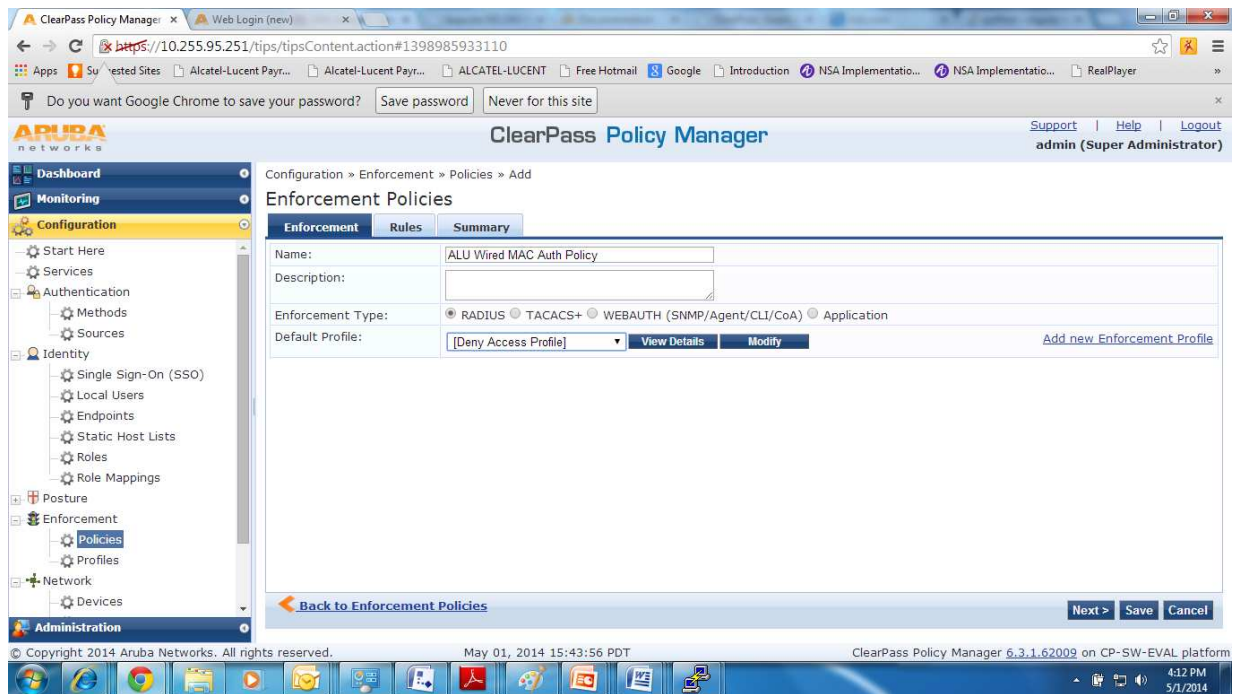
#### 5.5.2.4 Configuring the enforcement policies

Multiple enforcement policies are required:

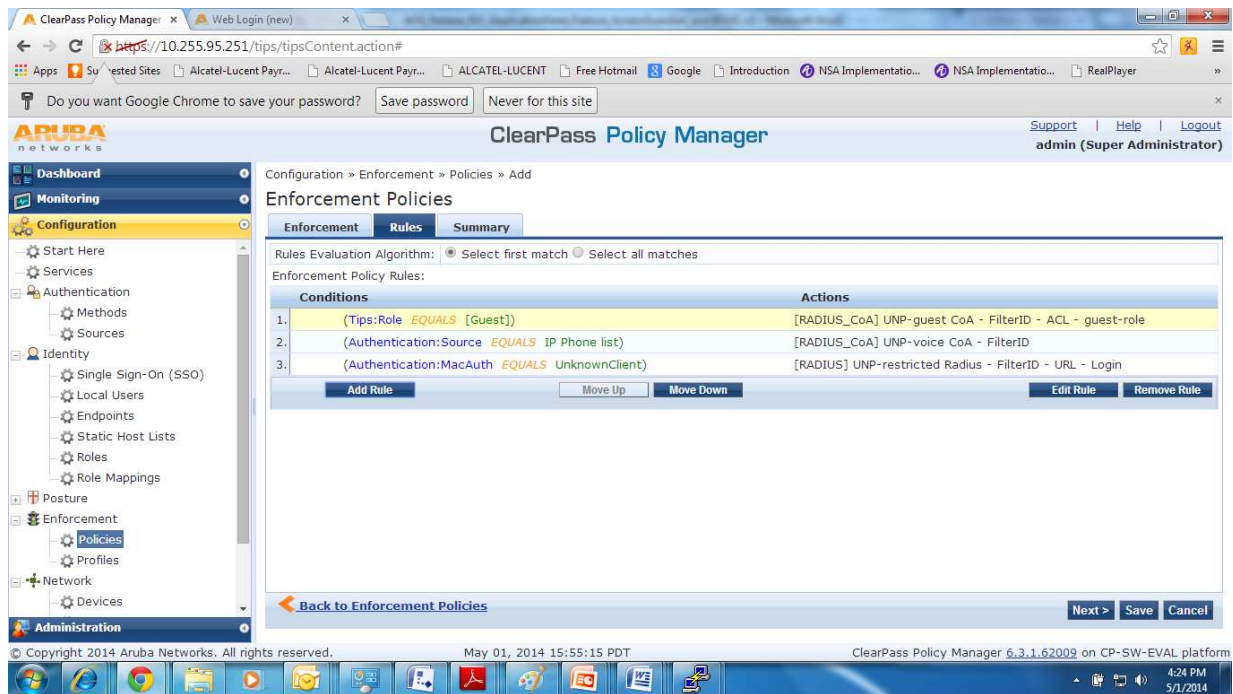
1. Enforcement policy for wired MAC authentication service
2. Enforcement policy for web authentication service

Create enforcement policies as follows:

1. Go to Configuration/Enforcement/Policies
2. Create Policy for Wired MAC Authentication service
  - a. Select Create a new Enforcement Policy
  - b. Follow the instruction for enforcement policy creation

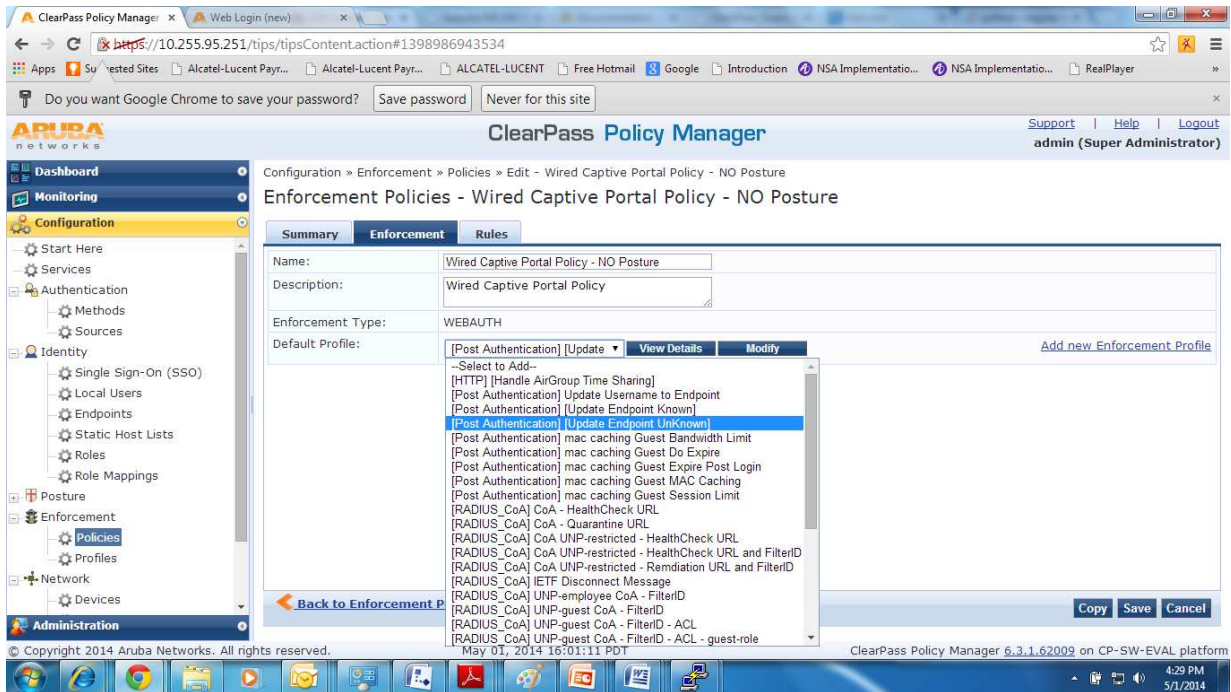


- c. Set Attributes tab with the following rules:
  - i. Tips:Role EQUALS [Guest], then return use Enforcement Profile that returns UNP-guest
  - ii. Authentication:MAC Auth EQUALS Unknown Client, then use the Enforcement Profile that returns UNP-restricted and redirection URL



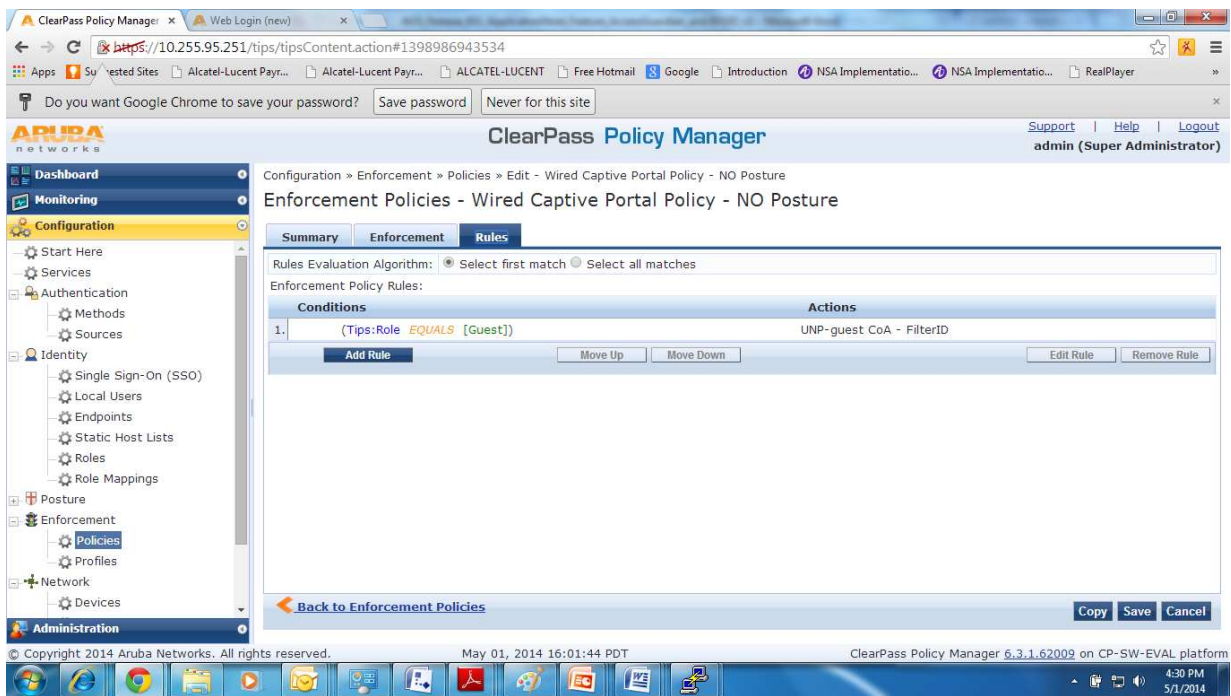
- 3. Create policy for Web Authentication service:
  - a. Select Create a new Enforcement Policy

b. Follow the instructions for new enforcement policy creation



c. Set attributes tab with the following rules:

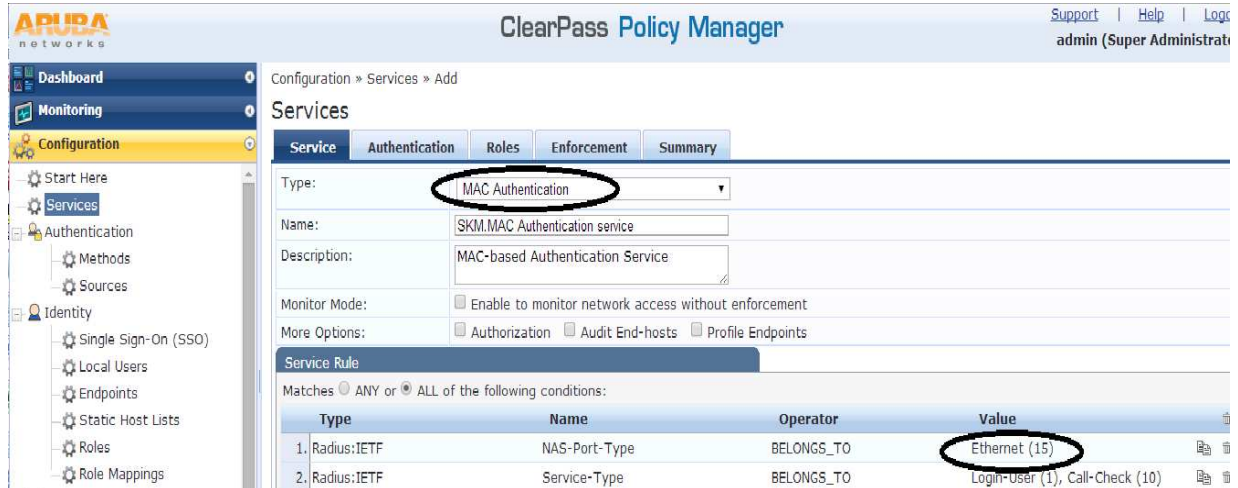
Tips:Role EQUALS [Guest], then use “Guest COA Enforcement Profile”



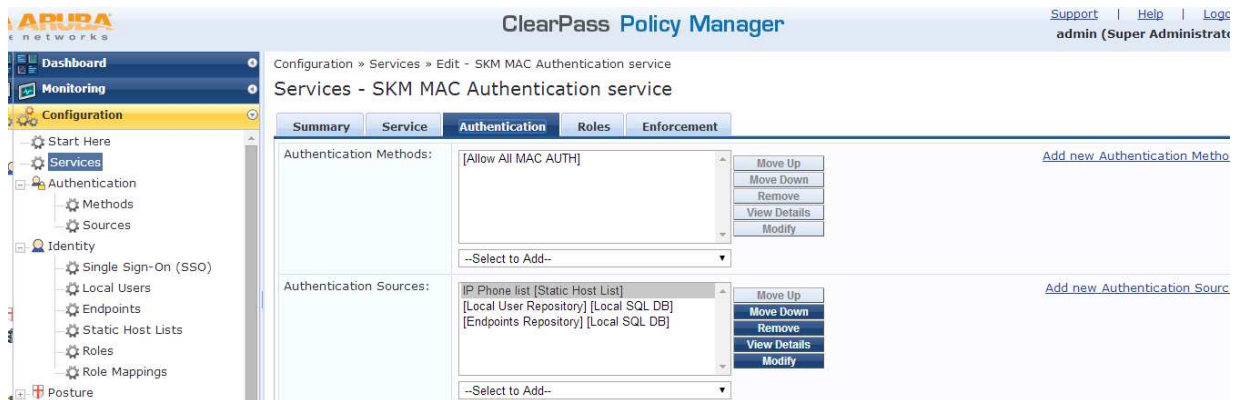
5.5.2.5 Configuring the MAC authentication and Captive Portal Web Auth Services

Multiple services are required for this use case.

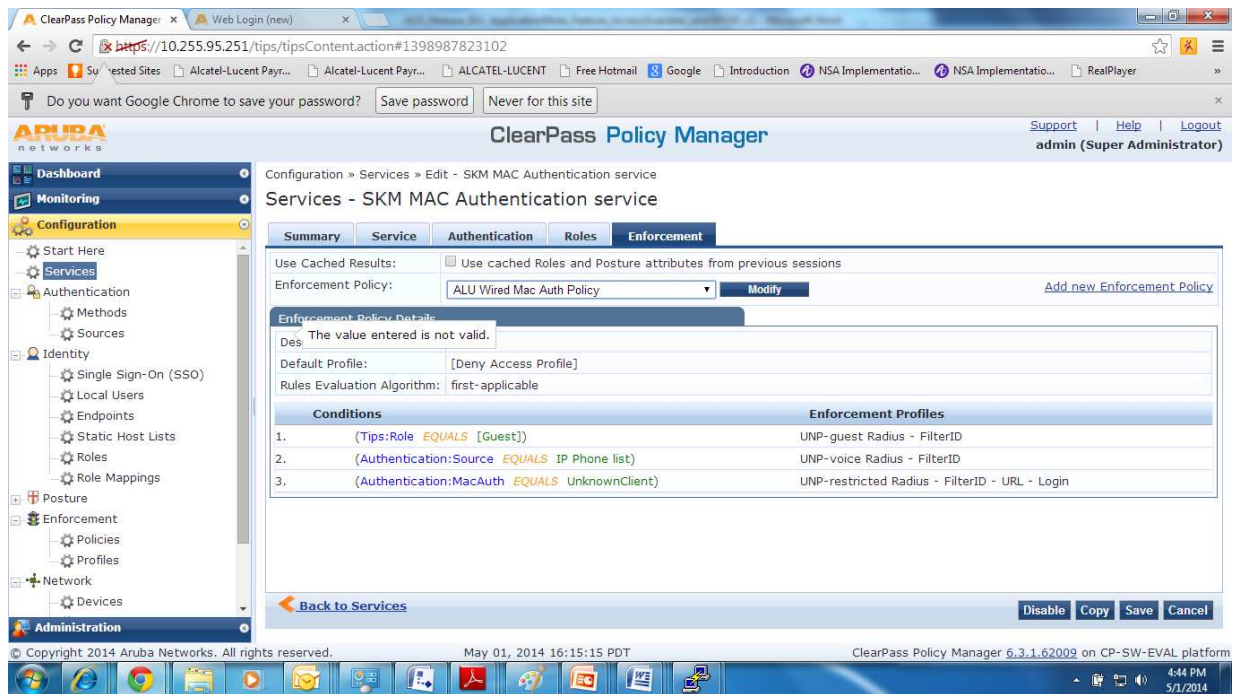
1. First create MAC authentication service
  - a. Go to Configuration/Service
  - b. Add new Service
  - c. Select - Type - MAC Authentication
  - d. Modify the first service rule: Value - Ethernet(15) and go to Next



- e. On Authentication tab:
  - i. Authentication Methods: Remove [MAC-AUTH] and select [Allow All MAC AUTH]. This selection allows the CPPM to return RADIUS Access-Accept even if the user is not known and provide the restricted profile and URL.
  - ii. Authentication Sources: Use Local User Repository or external source or Static Host List.

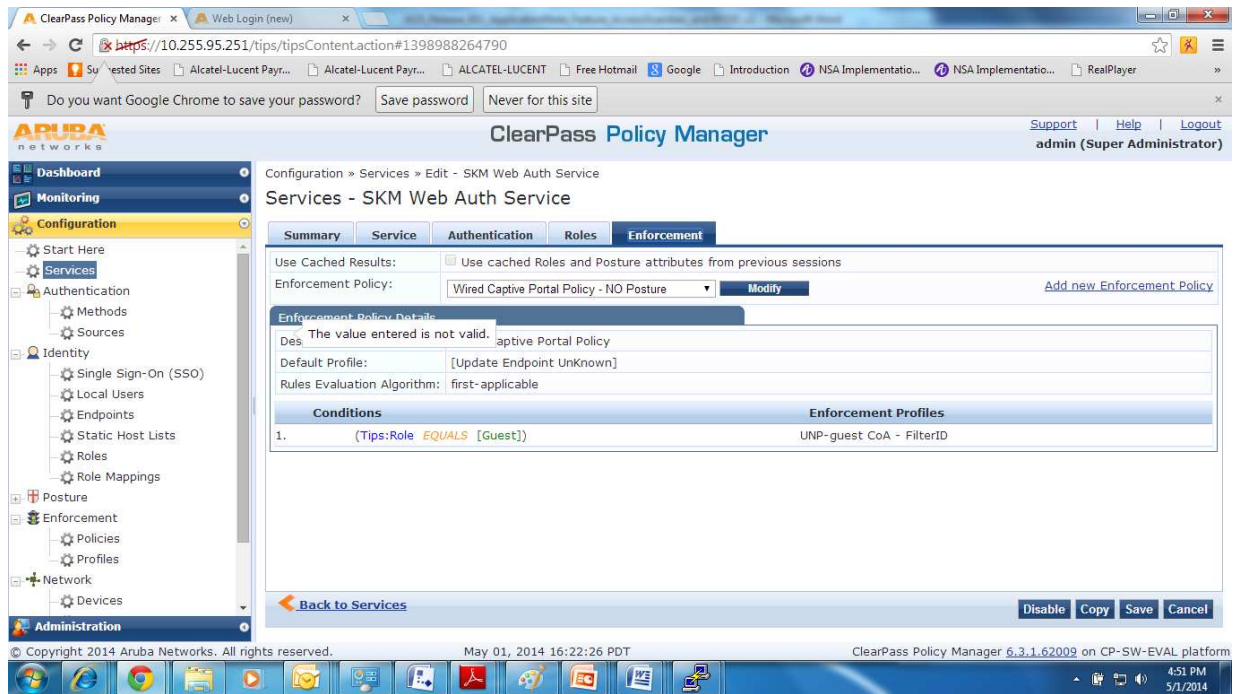


- f. On Enforcement tab:
  - i. Select configured MAC Auth Enforcement Policy created before



2. Create Web Auth Service

- a. Add new service
- b. Select Type: Web Authentication
- c. Enter Name/Description and accept defaults and move onto Authentication tab
- d. Select Authentication Source- [Guest User Repository]
- e. Go to Enforcement profile and select configured Captive Portal Auth Enforcement Policy created above.



NOTE: The Authentication services created have to be ordered in the way one would want them to be applied.

## 5.6 BYOD USE CASE 2: Unified authentication of IT-issued device

This use case covers the secure access to the network for IT-issued supplicant devices. The 802.1x authentication workflow is as follows:

1. The user connects the IT-issued device (supplicant) to the switch port that is configured as an edge-port with 802.1x authentication enabled.
2. The device sends an EAP frame to the switch and the switch initiates a RADIUS request with embedded EAP packet information to the CPPM configured as the RADIUS server.
3. The 802.1x Wired Service configured on the CPPM is selected for processing the RADIUS request.
4. The CPPM authenticates the device/user against the Active Directory database configured for this service and the device is expected to use one of the authentication methods configured on the service. Optionally any of the other authentication sources may be used.
5. The 802.1x authentication service on CPPM is configured with an Enforcement Policy. The enforcement policy can check for several possible criteria and decide on the role of the user. It could be attributes from the Active Directory database or Local User database. In this example we check for the presence of the device/user in the Active Directory database and if present, then an Enforcement Profile returns UNP-employee in the RADIUS Filter-id.
6. The switch enforces the client with the policy list associated with the UNP-employee if one is configured. The default policy list is to allow all.

### 5.6.1 Switch configuration

1. Configure a RADIUS server

```
aaa radius-server "cppm-authserver" host 10.242.254.101 hash-key secret retransmit 3 timeout 2
auth-port 1812 acct-port 1813
```

2. Create an "aaa" profile

```
aaa profile "byod-aaa-profile"
aaa profile byod-aaa-profile device-authentication 802.1x "cppm-authserver"
aaa profile byod-aaa-profile accounting 802.1x "cppm-authserver"
```

3. Create the required VLANs

```
vlan 10 admin-state disable name vlan-block
vlan 20 admin-state enable name vlan-corporate-employee
```

4. Create the policy list

It is not required to define a policy list if the policy is going to be to allow all traffic.

5. Create the required UNP edge-profiles

```
unp edge-profile UNP-employee
```

6. Map the edge-profile to an appropriate VLAN

```
unp vlan-mapping edge-profile UNP-employee vlan 20
```

7. Create a default profile

```
unp edge-profile default-profile
```

8. Map the default edge-profile to vlan 10

```
unp vlan-mapping edge-profile default-profile vlan 10
```

9. Create an edge-template

```
unp edge-template byod-template
```

10. Enable 802.1x on the edge-template. Pass alternate UNP edge-profile may be configured if the RADIUS server doesn't return an UNP edge-profile on authentication pass.

```
unp edge-template byod-template 802.1x-authentication enable
```

```
unp edge-template byod-template 802.1x-authentication pass-alternate edge-profile UNP-employee
```

11. Assign the edge-template to a port

```
unp port 2/1/1 edge-template byod-template
```

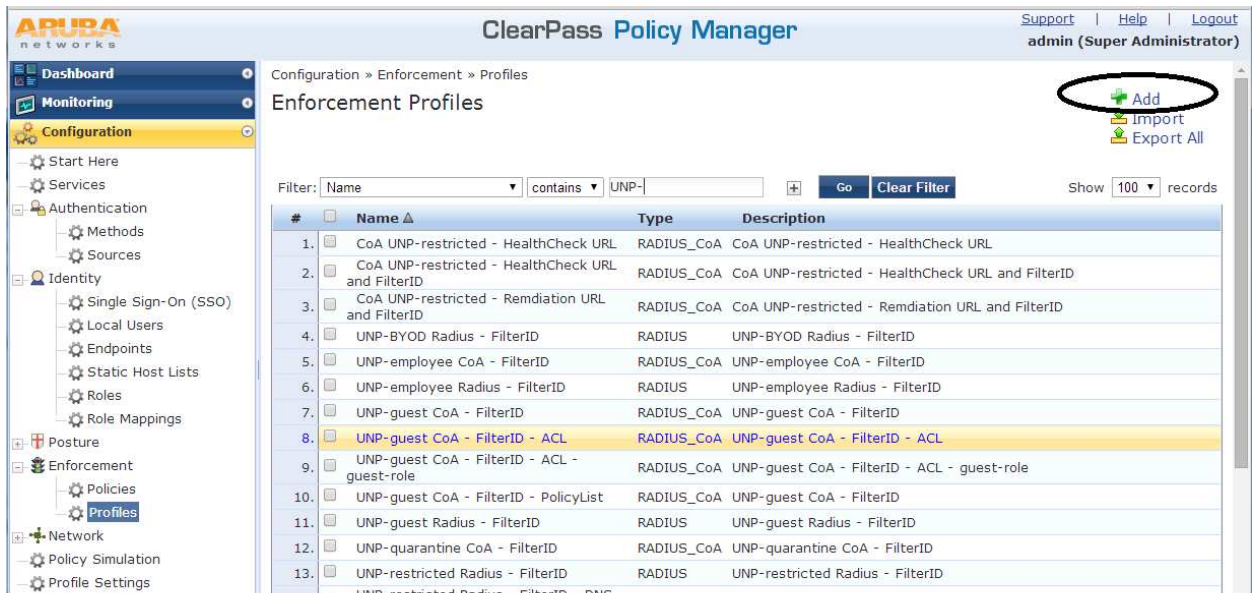
## 5.6.2 CPPM configuration

In addition to the generic configuration defined above, the following specific configuration should be done on the CPPM to support 802.1 x authentications. A service uses the following configuration objects: an authentication method, an authentication source, a role, a role-mapping, an enforcement policy and an enforcement profile. The configuration objects can be created first before referencing them during service creation or can be created within the service during service creation. It is better to plan ahead the configuration objects one would use before proceeding with the service creation.

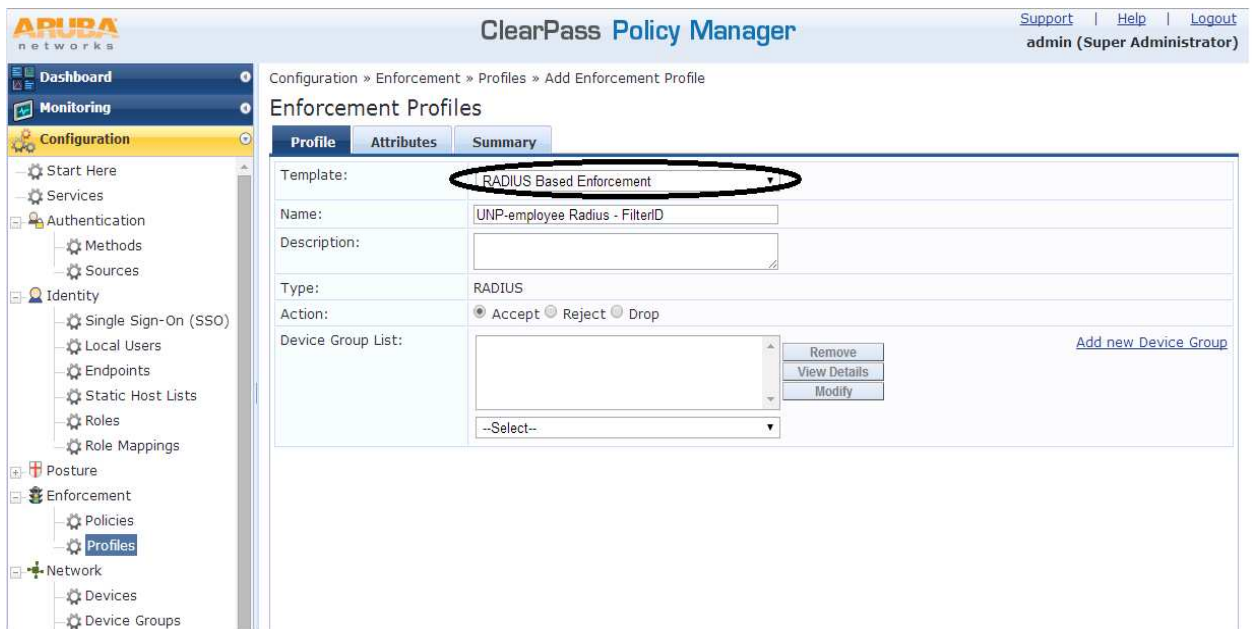
### 5.6.2.1 Configuring enforcement profile

The enforcement profile defines what should be communicated to the switch for a transaction be it authentication process, registration process, onboarding process or posture check status reporting, etc. In this use case the enforcement profile is required to just return a UNP edge-profile name.

1. Go to Configuration/Enforcement/Profiles and select “Add” to add a new enforcement profile.



2. Add the attributes for the profile. Make sure to select RADIUS Based Enforcement from the drop-list for Template. Add a name.



3. Move to Attributes tab and configure the following. Use the standard RADIUS filter-id attribute to send the UNP edge-profile name to the switch. Press Save to save the profile.



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Type	Name	Value
Radius:IETF	Filter-Id (11)	UNP-employee
Click to add...		

### 5.6.2.2 Configuring enforcement policy

The enforcement policy is an object used to define the conditions to be matched after the authentication process.

1. Go to Configuration/Enforcement/Policies and select to add a new enforcement policy.

Configuration » Enforcement » Policies

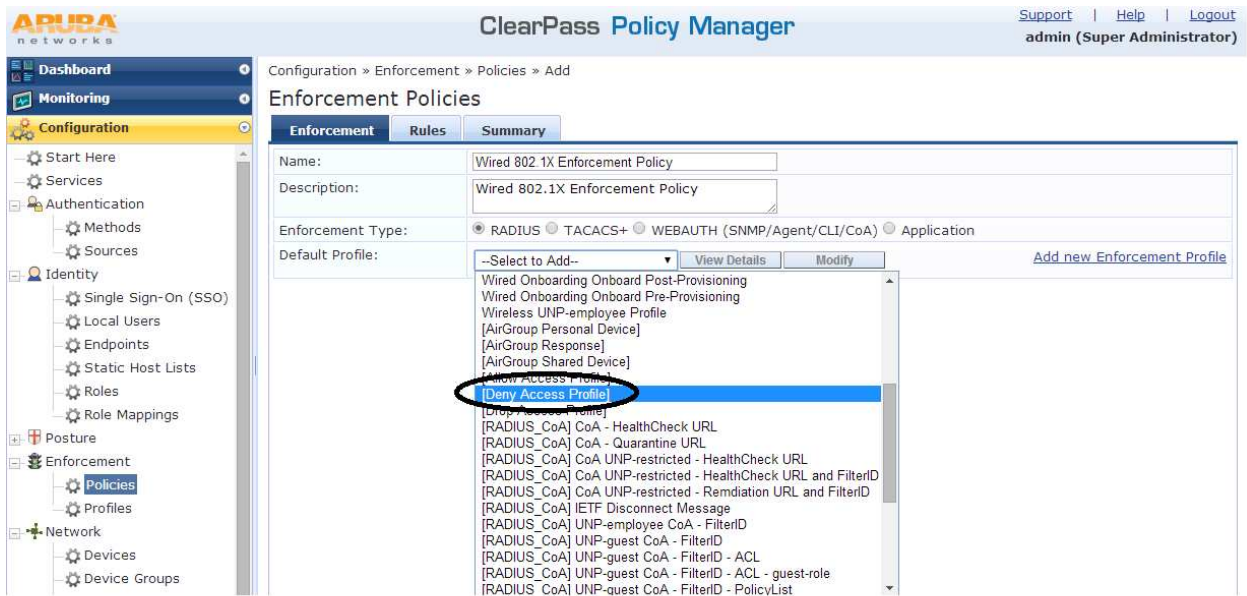
Enforcement Policies

Filter: Name contains Wired Go Clear Filter Show 50 records

#	Name	Type	Description
1.	Wired Onboarding Onboard AppAuth Policy	Application	
2.	Wired Onboarding Onboard Pre-Auth policy	Application	
3.	Wired Onboarding Onboard Provisioning Policy	RADIUS	Enforcement policy controlling network access for device provisioning
4.	Wired Alcatel-Lucent IP Touch Enforcement Policy	RADIUS	Wired MAC Enforcement Policy

© Copyright 2014 Aruba Networks. All rights reserved. Apr 28, 2014 17:04:34 PDT ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

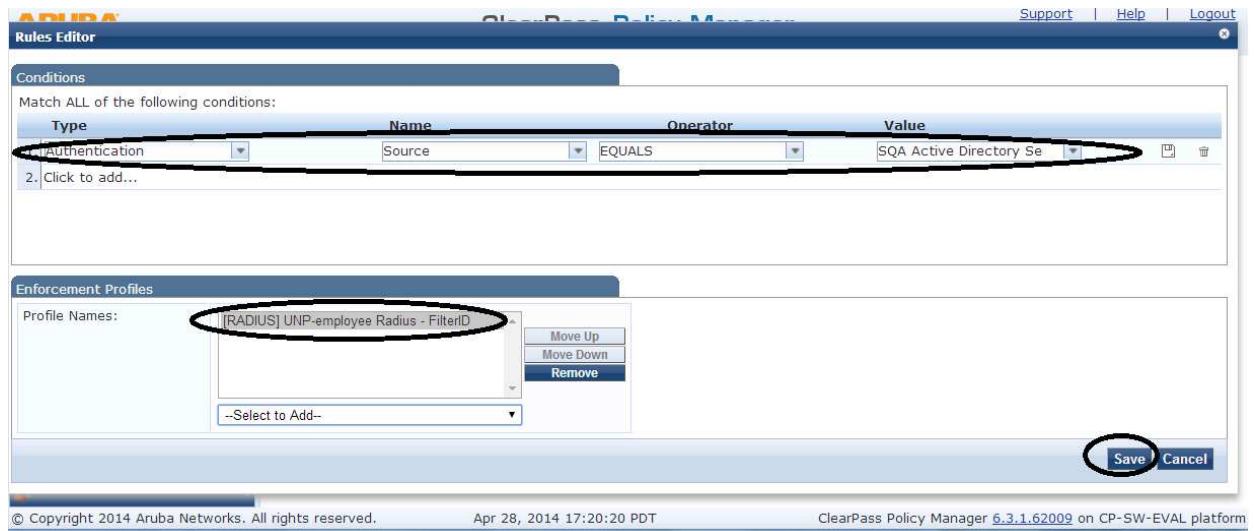
2. On the Enforcement tab, update the following information as shown. Note that anything in square brackets [] is CPPM pre-defined Enforcement policy. The [Deny Access Profile] just returns a RADIUS Access-Reject to the switch, if none of the conditions defined by the Enforcement profile match.



3. On the Rules tab, select Add to add a new rule.

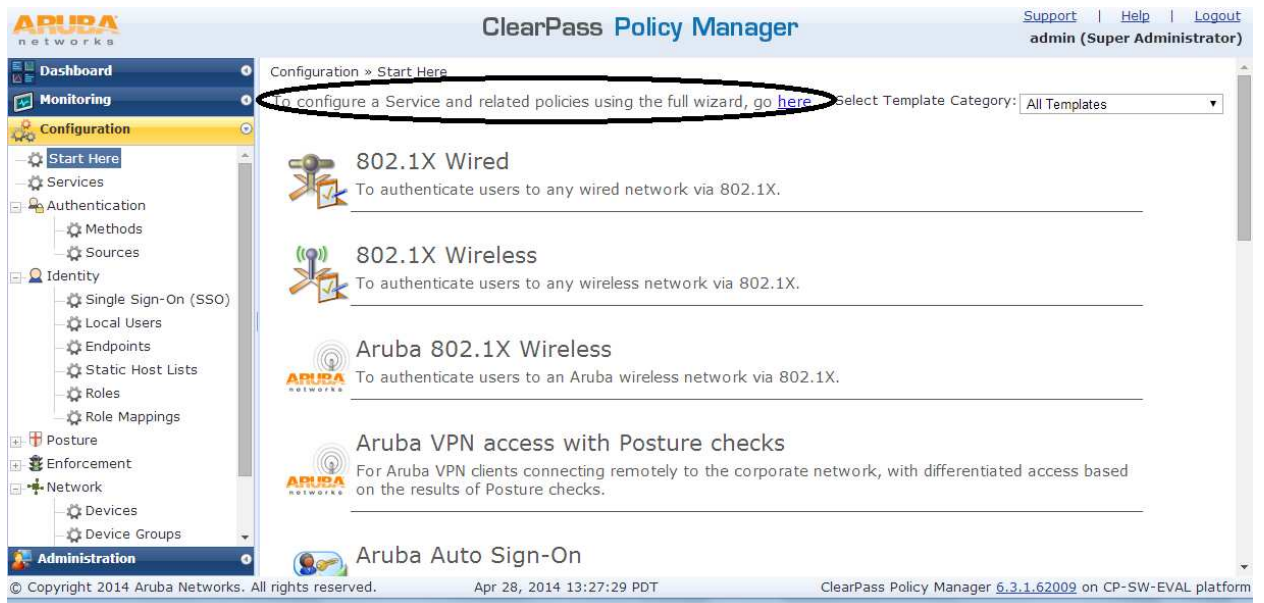


4. Add new conditions and assign enforcement profiles. The conditions state that if the user is found in the Active Directory used as the authentication source then assign UNP-employee enforcement profile. Press Save to save the profile.

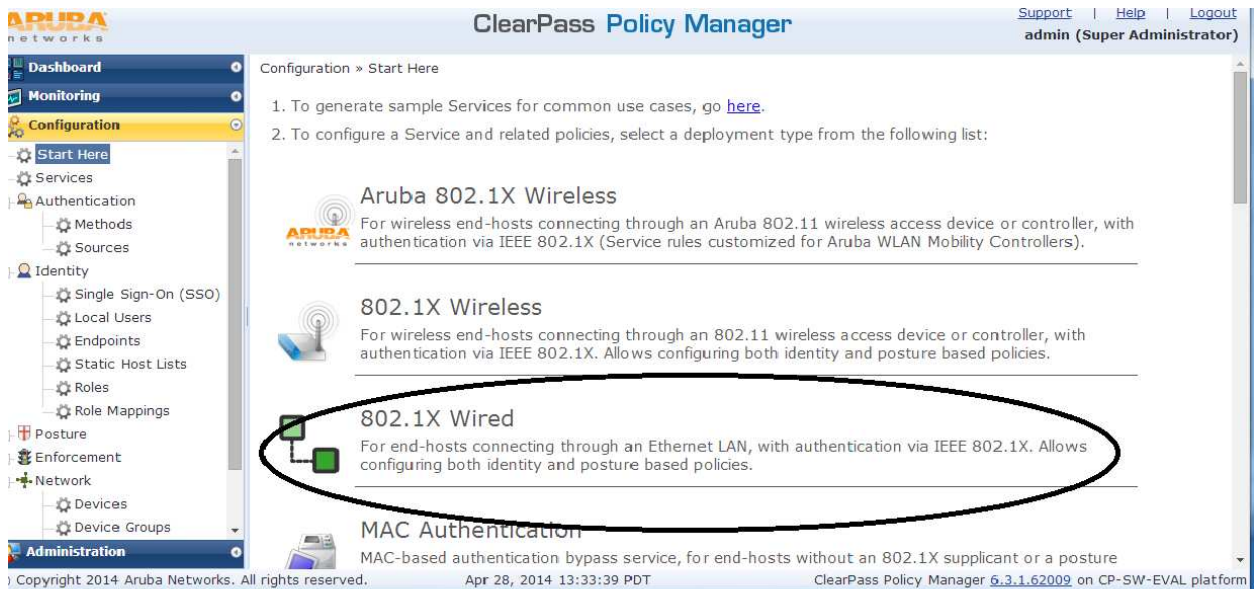


### 5.6.2.3 Configuring an 802.1x service

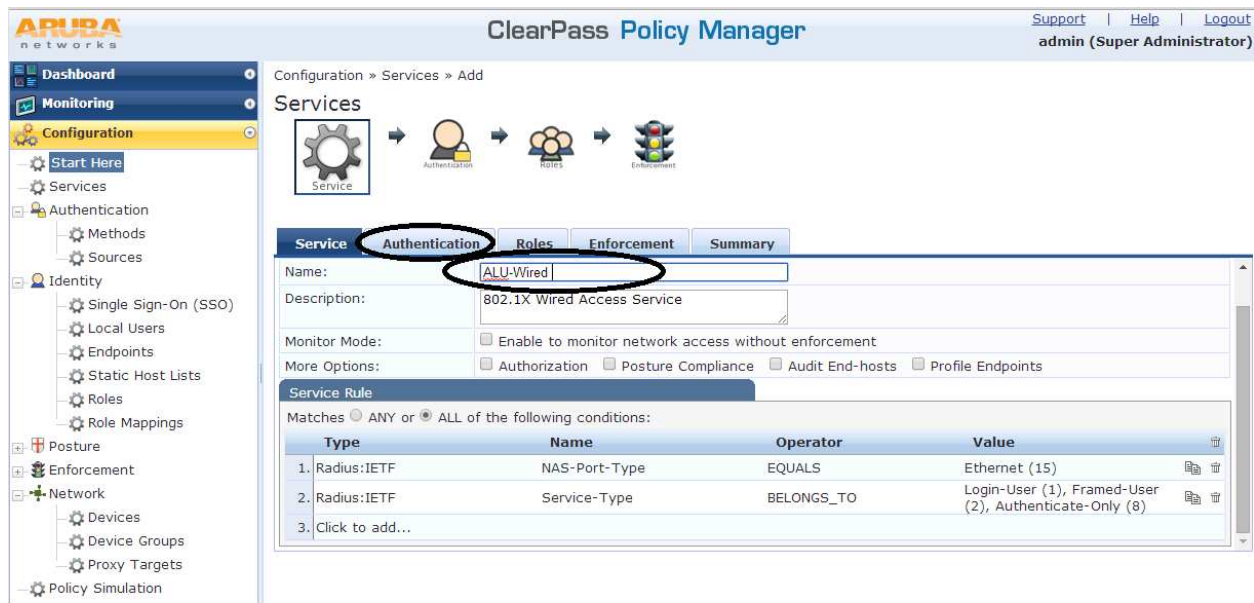
1. Create a service in the CPPM to intercept the RADIUS requests initiated from the switch for the 802.1x EAP packets. This is created using a Wired 802.1x template. Go to Configuration/Start. Select the link highlighted below.



2. Select the 802.1X Wired service shown below



3. Configure the Service. Posture Check could be enabled. This use case will focus on only authentication. Hence it is sufficient to configure the name of the service and select the Authentication tab.



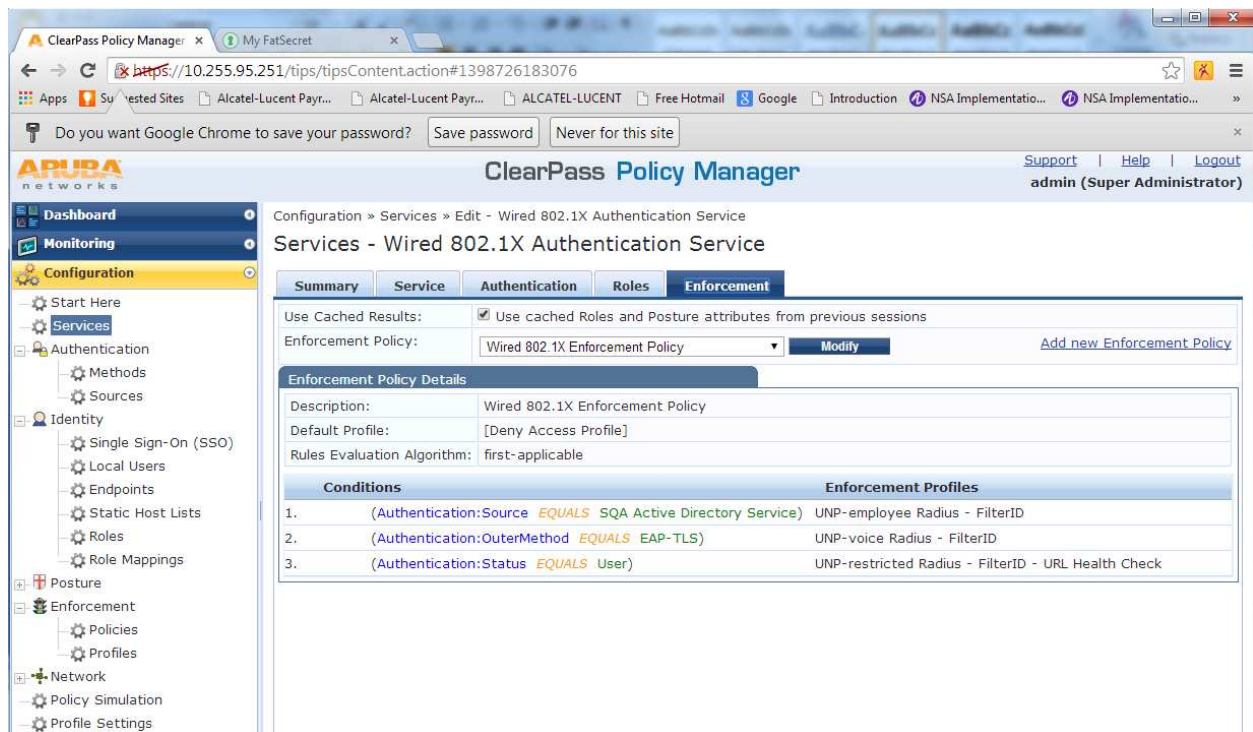
4. On the Authentication tab:

- a. The default set of authentication methods are sufficient if only 802.1 x authentications of the IT-issued devices are being done. But the same service is used for onboarding non-IT issued devices. Hence additionally “EAP TLS with OSCP Enabled” must be added to the list and moved to the topmost on the list to get the highest precedence. OSCP is supported by the Onboard CPPM Module to provide a real-time check on the validity of the certificate.
- b. The authentication sources must be selected from the drop-down list also. The authentication sources could be local or an external Active Directory server or anything on the list. In the example below the Active Directory database is chosen as

authentication sources. The assumption is that the authentication sources have been created before.



5. The next tab is Roles. There is no requirement to define roles. In this use example, a role is not defined in the 802.1X service
6. The next tab is Enforcement. Here the Wired 802.1X Enforcement Policy is selected with the set of conditions and Enforcement Profiles associated with it. The Enforcement Profiles define the actual attributes to be communicated back to the switch. The Enforcement Policy and Enforcement Profiles can be created before and selected here.



NOTE: The Authentication Services created have to be reordered based on which order one wants the services to be applied.

## **5.7 BYOD USE CASE 3: Device onboarding with non-IT devices**

This use case is used to allow employees with non-IT issued devices to get access to the network.

ClearPass Onboard has certain requirements that must be met by the provisioning network and provisioned network as follows:

- The provisioning network must use a Captive Portal to redirect a new device to the device provisioning page.
- The provisioning server (Onboard server) must have an SSL certificate that is trusted by devices that will be provisioned; it means a commercial SSL certificate is required.
- The provisioned network must support EAP-TLS (IOS and OSX) and PEAP-MSCHAPv2 (other devices) authentication methods.
- The provisioned network must support OSCP checks to detect when a device has been revoked and deny access to the network.

The Onboard workflow is as follows:

1. A new device, if supplicant, will authenticate via PEAP with domain credentials or, if non-supplicant, will use MAC authentication.
2. The device does not have unique device credentials. This will place the device in a provisioning role, which is the UNP-restricted profile on our switch with limited network access and Captive Portal that redirects users to the device provisioning page.
3. The link to the provisioning page will prompt the user for domain credentials. The credentials are used to authenticate the user against an Active Directory or Local User database.
4. After authentication, the CPPM Onboard module also generates a unique certificate for the specific device and creates unique credentials that are used to create a user account on the CPPM. Future PEAP/MSCHAPv2 authentication will use these credentials.
5. Then the authenticated user is prompted to install the enterprise's root certificate. Installation of the root certificate enables the user to establish authenticity of the provisioning server.
6. After provisioning, the device switches to EAP-TLS/PEAP-MSCHAPv2 authentication using the new certificate/credentials. The client is authenticated and gets access to the provisioned network.

Please refer to the ClearPass Onboard Deployment Guide to understand the workflow differences for Android and other device types.

### **5.7.1 Switch configuration**

The switch configuration remains the same as in Unified Access USE CASE 2 with the addition of the following lines of configuration. Addition of the following lines can support both Unified Access USE CASE 1, 2 and 3 on the same port. It is assumed that a non-IT-issued device could be a supplicant or non-supplicant. If the device is a supplicant, it is expected that it is not using EAP-TLS.

1. Set CPPM as the RADIUS server for MAC authentication

```
aaa profile byod-aaa-profile device-authentication mac "cppm-authserver"
```

```
aaa profile byod-aaa-profile accounting mac "cppm-authserver"
```

2. Enable MAC authentication on the edge-template associated with the port  
**unp edge-template byod-template 802.1x-authentication enable**  
**unp edge-template byod-template 802.1x-authentication pass-alternate edge-profile UNP-employee**
  
3. Create a restricted edge-profile by name UNP-restricted. This UNP has a built-in default policy list (allow DHCP, DNS, ARP, ICMP, trap http/https ports to CPU and redirect to the CPPM redirect server configured)  
**unp edge-profile UNP-restricted**
  
4. Create a restricted VLAN and map the restricted edge-profile to a restricted VLAN  
**vlan 1000 admin-state enable name vlan1000-restricted**  
**unp vlan-mapping edge-profile UNP-restricted vlan 1000**
  
5. Create a BYOD edge-profile and map it to a VLAN.  
**unp edge-profile UNP-byod**  
**unp vlan-mapping edge-profile UNP-byod vlan 20**

### 5.7.2 CPPM configuration

In addition to the configuration done for Unified Access USE CASE 1, the following configurations have to be added to CPPM:

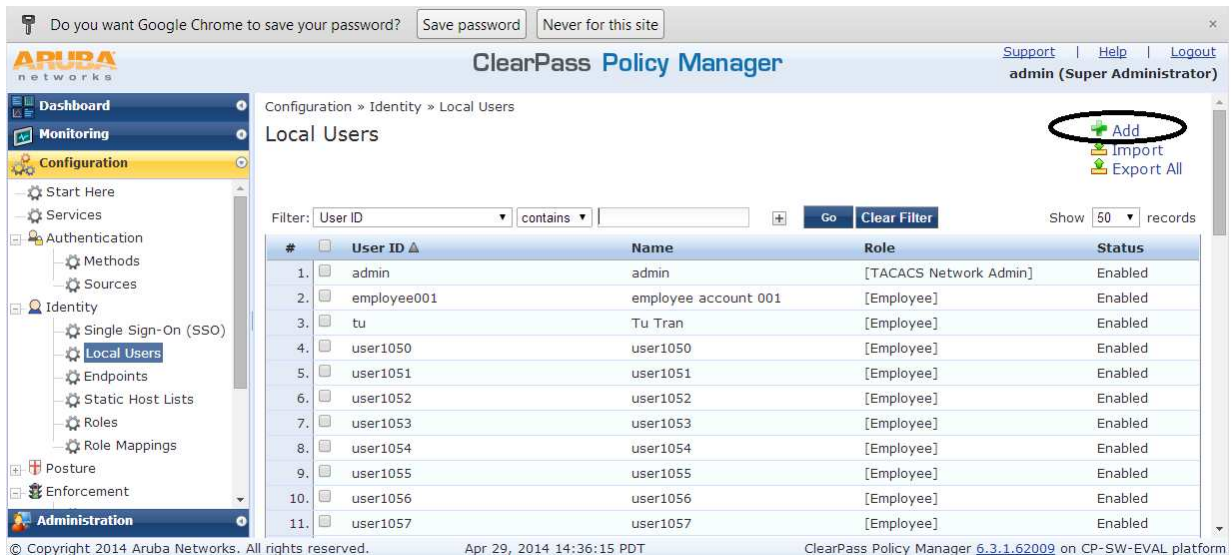
- Configure Employee Account/Onboard setting in the local database
- Configure appropriate Enforcement profiles and policies
- Configure MAC and Onboarding service
- Update the 802.1x authentication services

Please refer to the ClearPass Onboard Deployment Guide for CPPM as reference for complete details and all the configuration options available for “Onboard” module configuration. The following steps show just the one basic configuration.

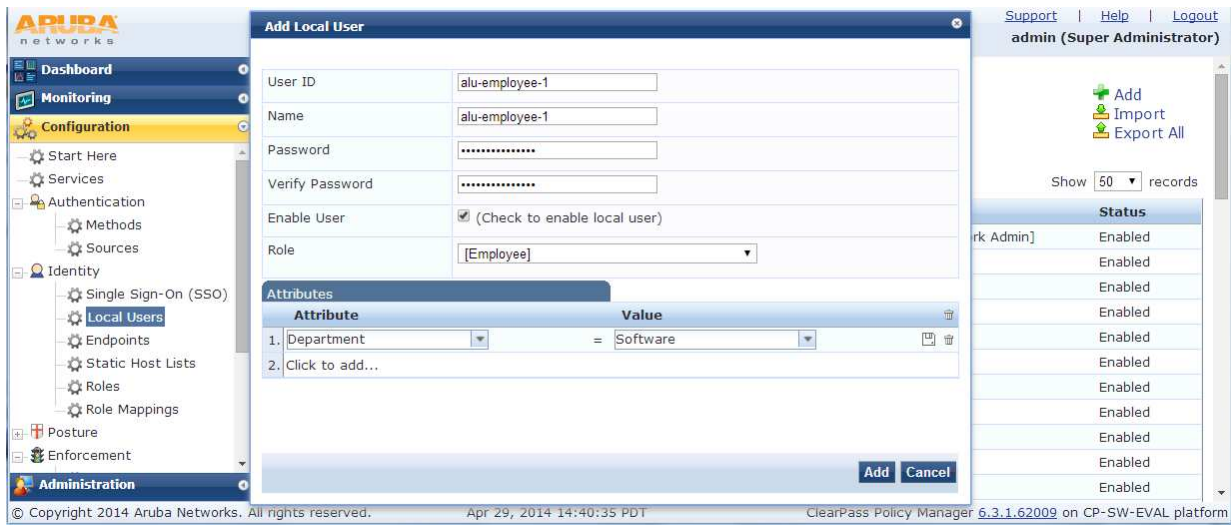
#### 5.7.2.1 Configuring Employee account

The employee account could be in the Active Directory server or could be created on the Local Users database in the CPPM.

1. Go to Configuration/Identity/Local Users and select Add.



2. Create a user with the relevant information as shown in the example below. The user is put in an [Employee] role. A role defined in square brackets like [Employee] is a pre-defined CPPM role.

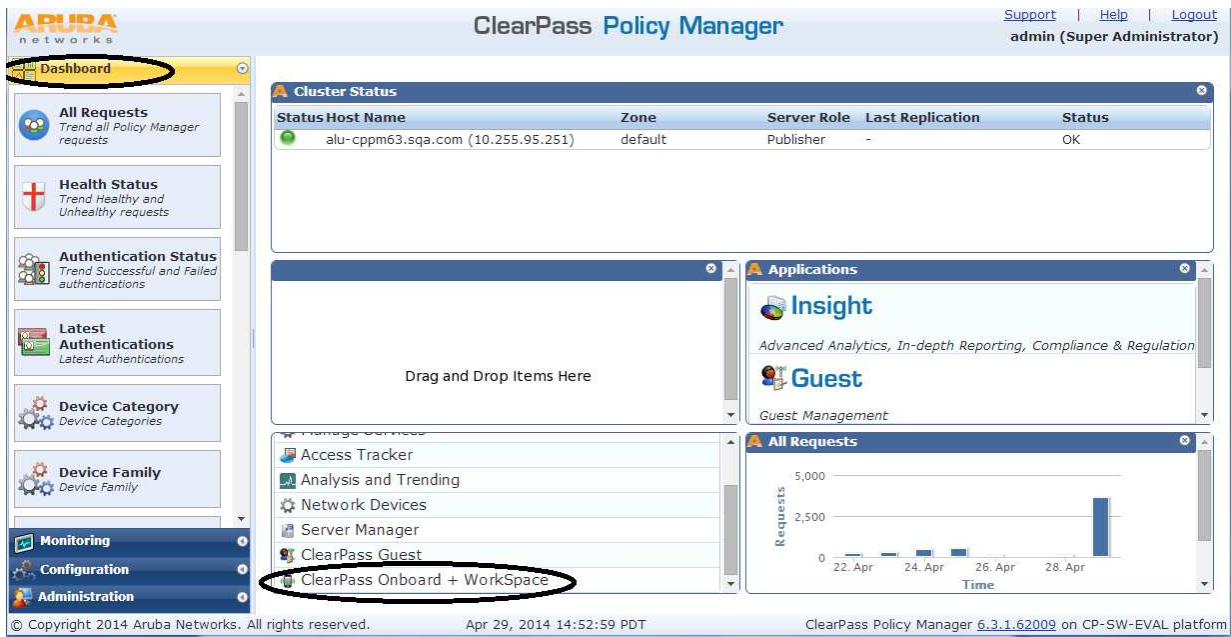


### 5.7.2.2 Creating device certificates

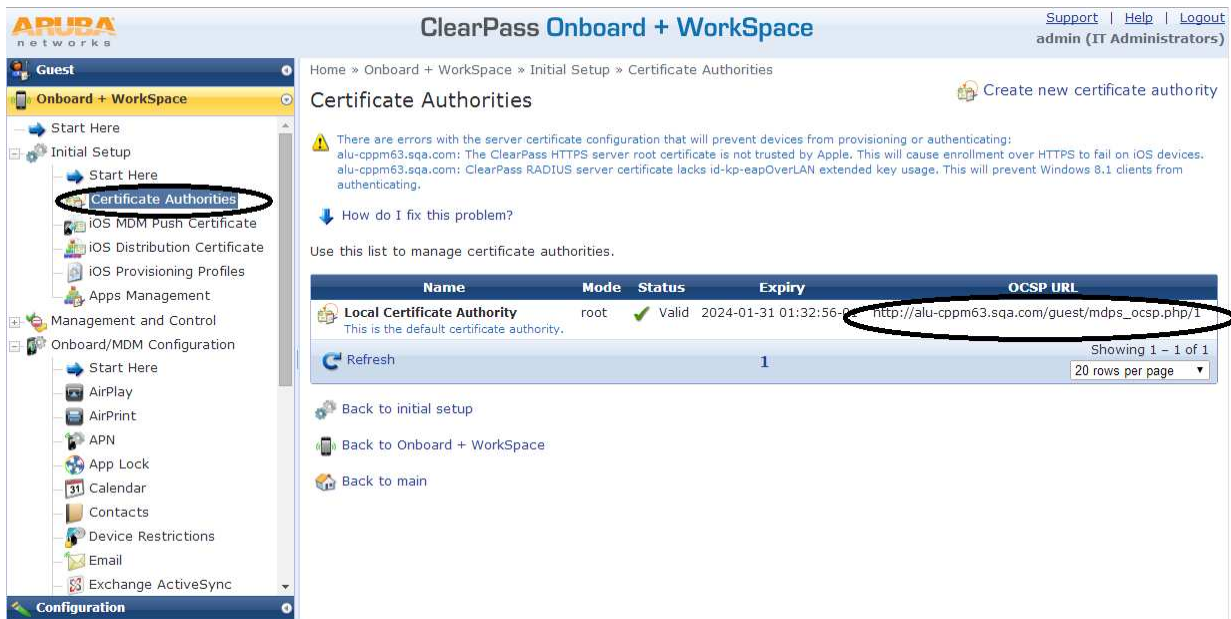
During the device provisioning process, one or more digital certificates is issued to the device. These are used as the unique credentials for the device. To issue the certificate, the CPPM can operate as the CA.

1. Go to Dashboard/QuickLinks and select “ClearPass Onboard + Workspace” tab as shown below.





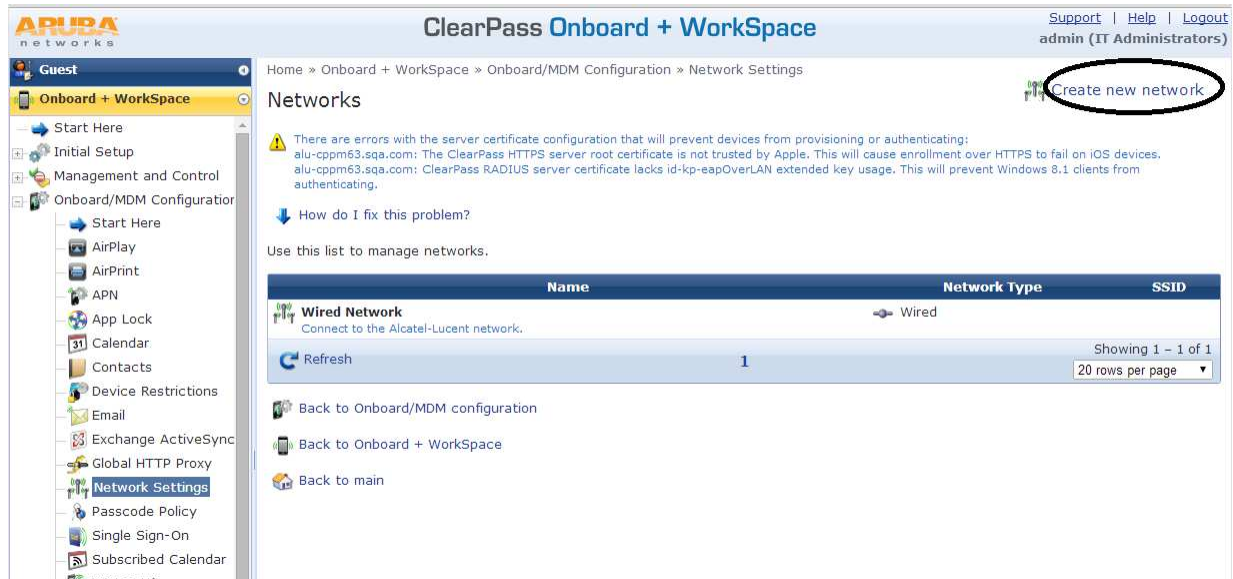
2. Go to Initial Setup/Certificate Authorities and use the default Local Certificate Authority. Notice the OSCP URL to be used for the authentication service.



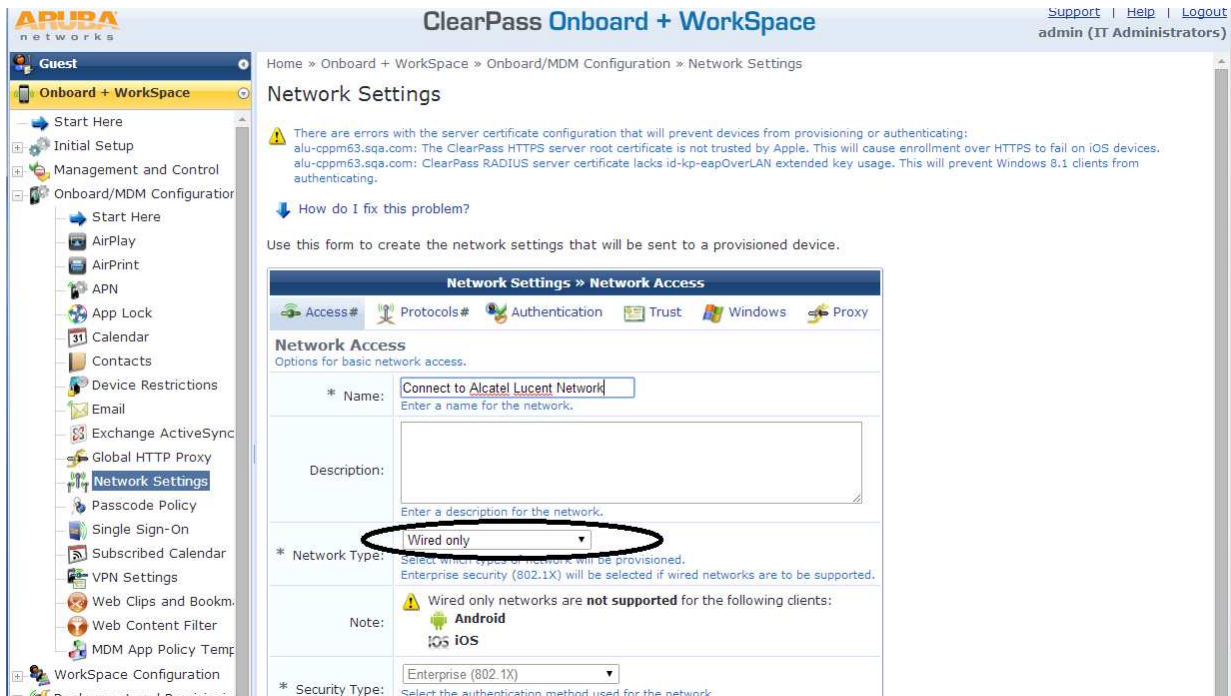
3. Next navigate to the Onboard/MDM Configuration and select Network Settings.



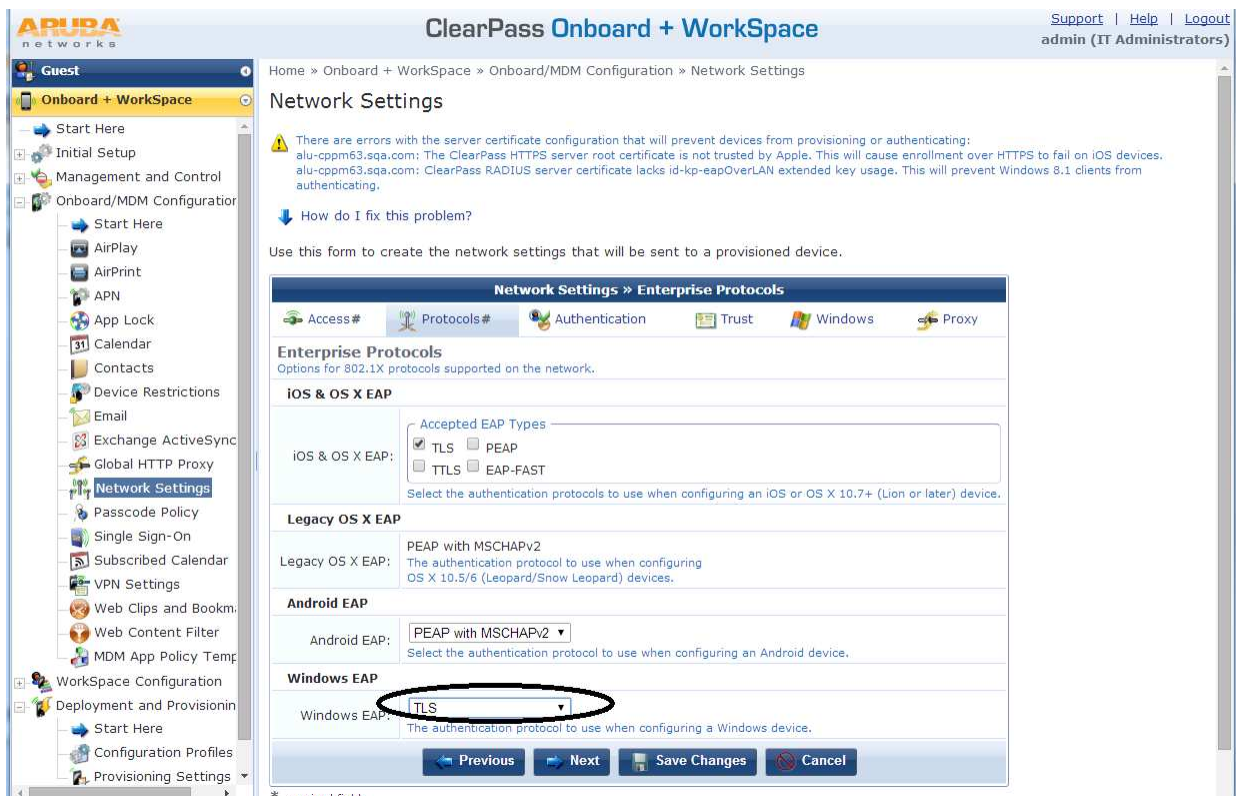
4. Select Create new network as shown.



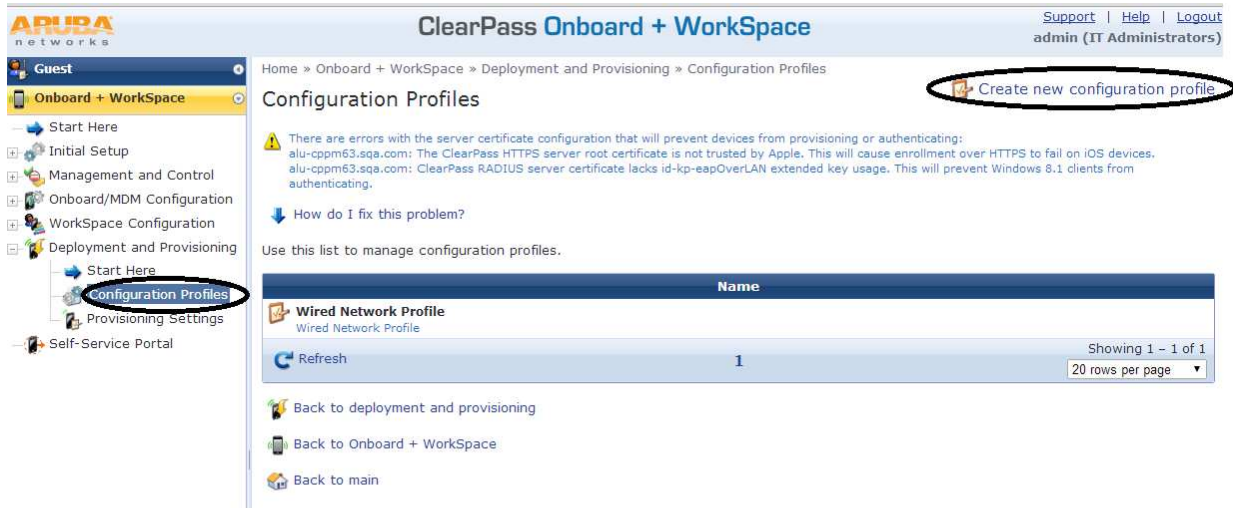
5. Enter a name, select “Wired” and click Next.



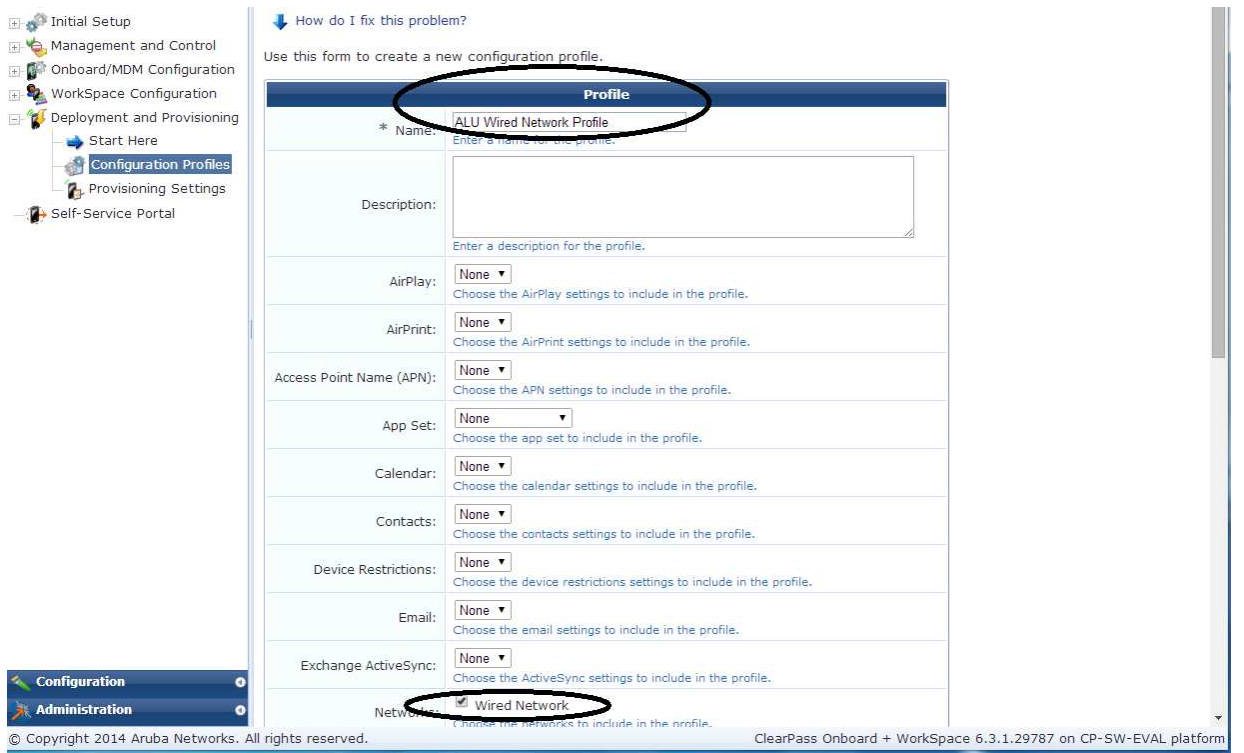
6. Select TLS for Windows and accept all defaults. Go to next page and accept defaults for Authentication/Trust/Windows and Proxy tabs and finally Save changes.



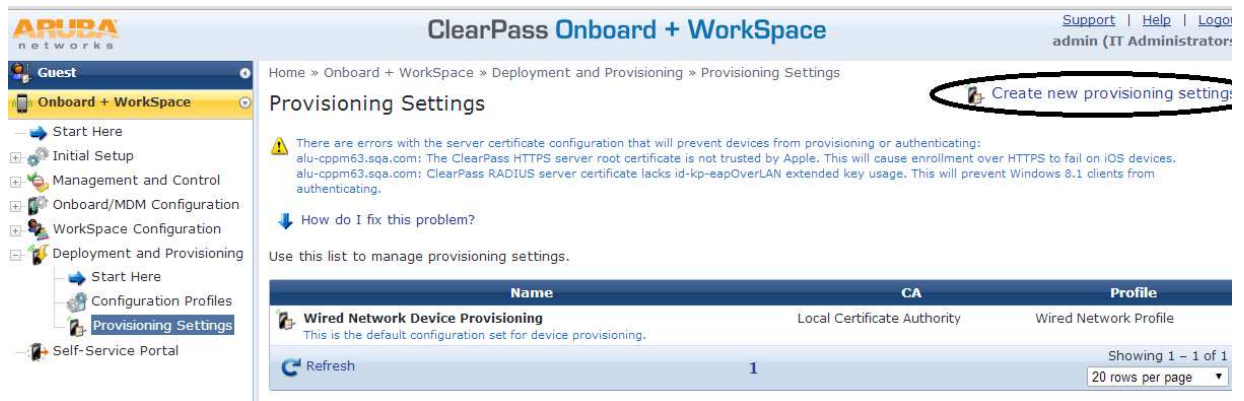
7. Go to Deployment and Provisioning/Configuration Profiles and select "Create a new configuration profile".



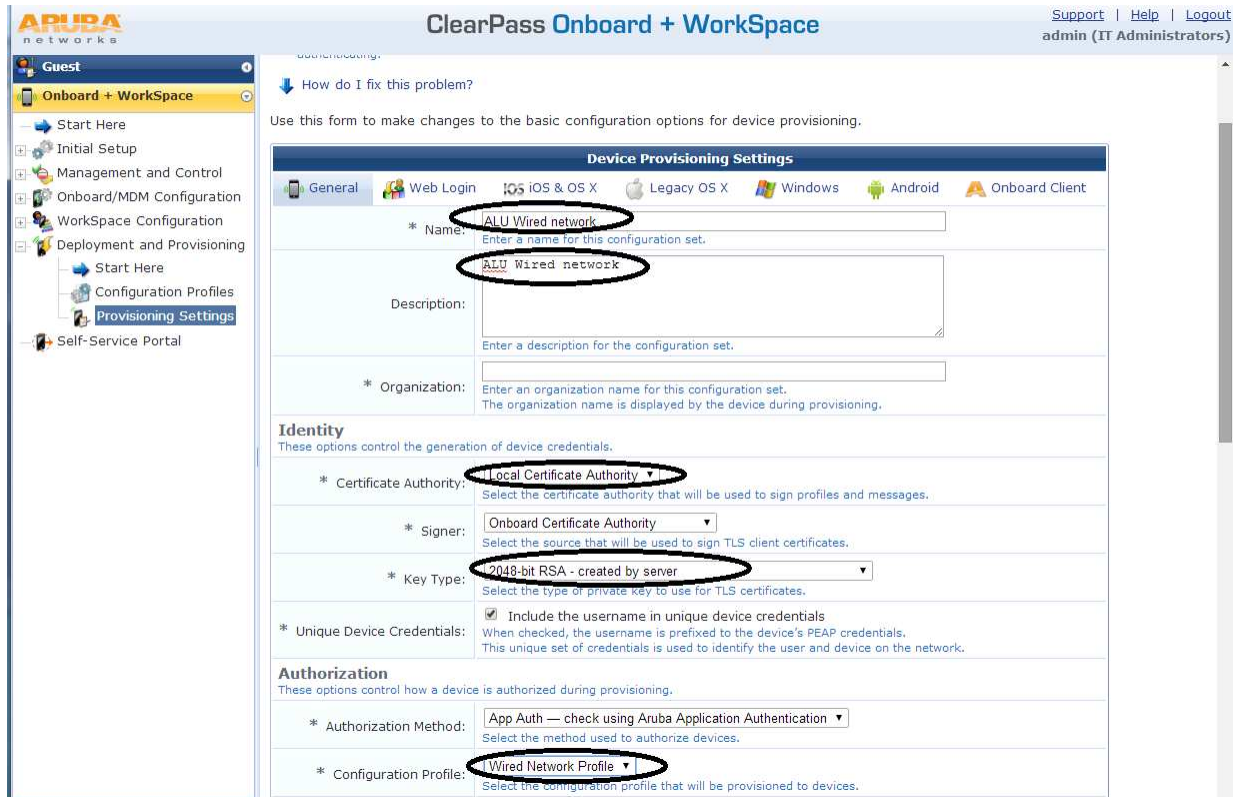
8. Go to Deployment and Provisioning/Configuration Profiles and “Create a new configuration profile”. Configure a name, select “Wired Network” below, and save changes.



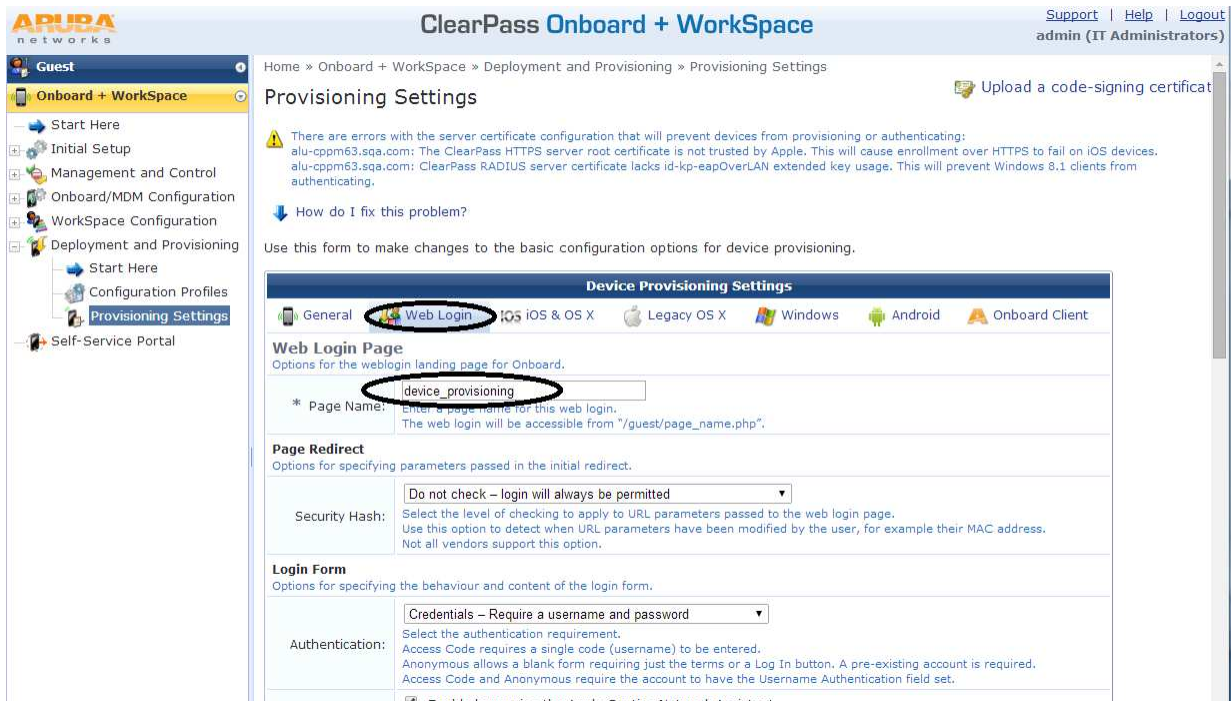
9. Go to Deployment and Provisioning and Select “Provisioning Settings”. Then select “Create new provisioning setting”.



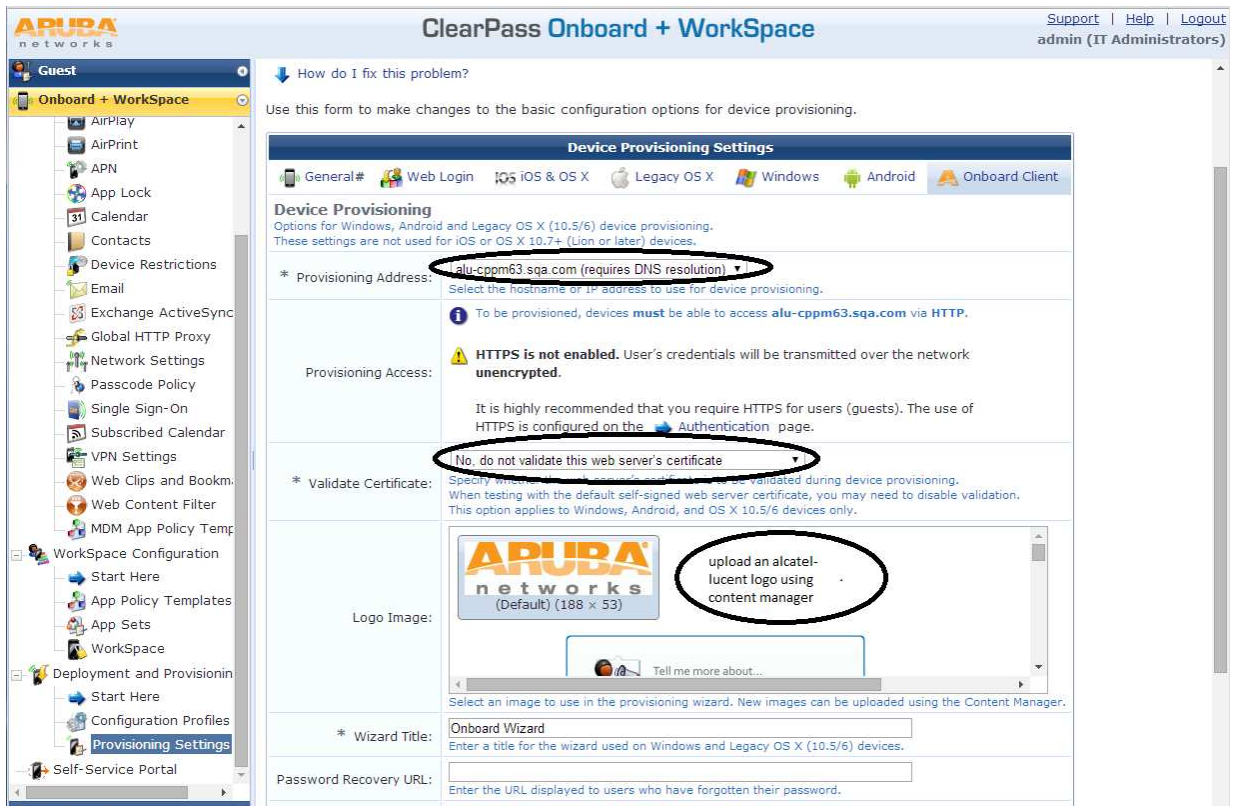
10. Enter the name and description. Under “Identity”, select “Local Certificate authority”, “2048-bit RSA - created by server”, and select the Configuration Profile that was previously created for the wired network. Then select “Next”.



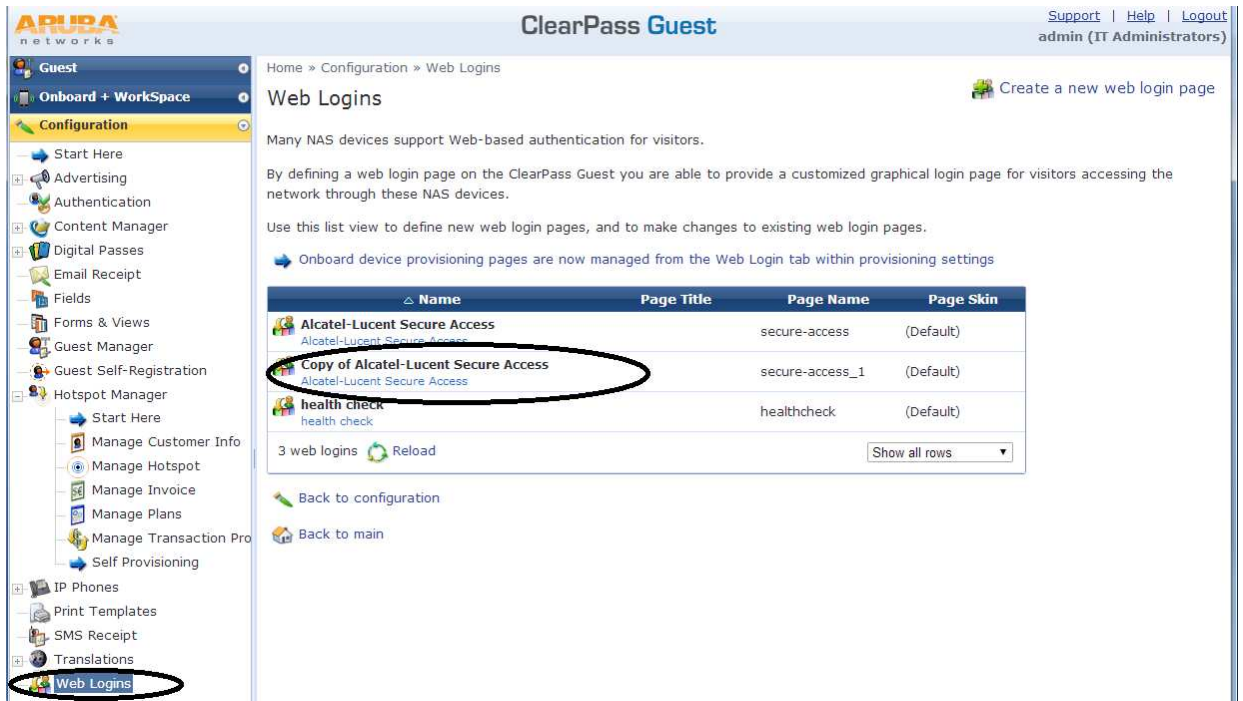
11. On the Web-Login Page fill in the appropriate web login page name and select Next. If the page name given is “device\_provisioning” then the actual page is [http://cppm-ip-address/guest/device\\_provisioning.php](http://cppm-ip-address/guest/device_provisioning.php). Accept all defaults of IOS, OSX, Windows and Android tabs.



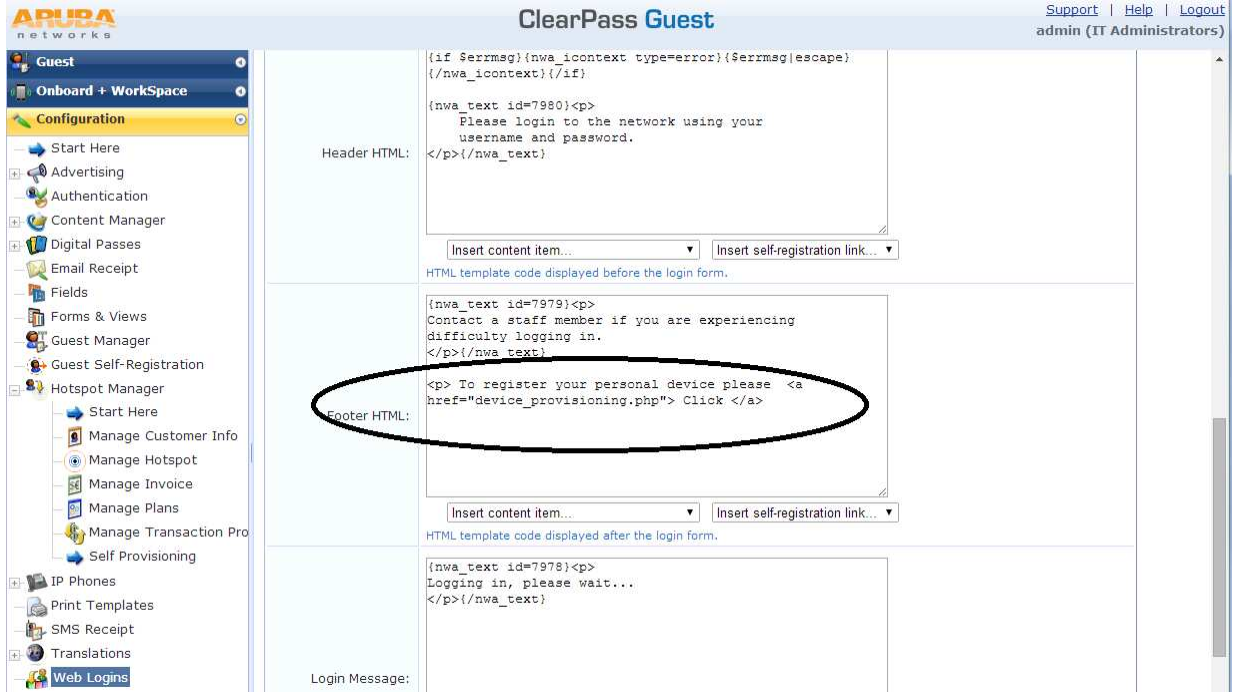
- For Onboard Client tab, for the Provisioning Address, input the IP address of the CPPM or the DNS name for CPPM. Select “No do not validate this web server’s certificate” and select the appropriate logo



- Once the Provisioning setting is done, then the Onboard Web Login page has to be linked to the “guest registration” page. Assume the guest login page has been configured. Go to Configuration/Web Logins. Select the Web Logins page and select Edit.



14. Update the Footer HTML with the following “<p> To register your personal device please <a href=“device\_provisioning.php”> Click </a>”. Please see below. Once this is done, save and test to see if the Onboard page is shown.



### 5.7.2.3 Configuring enforcement profile

Enforcement profiles define the attributes/status that has to be communicated to the entity

requesting the service. For device onboarding typically we need the following enforcement profiles:

1. Restricted profile, which returns UNP-restricted to put the device with limited access and redirection
2. [Allow All Access] profile to communicate to the internal Onboard module
3. BYOD profile, which returns UNP-byod to the device post onboard provisioning

The edge-profiles returned by the enforcement profiles must be present on the AOS switches.

### 5.7.2.3.1 Creating an ALU Restricted enforcement profile

This enforcement profile should be used to put the client in Restricted/Pre-provisioning mode. This should return edge-profile UNP-restricted with a redirection URL. Follow the steps for enforcement profile creation as shown in the previous section and update with the following information for this enforcement profile.

1. Modify the Attributes tab as shown below to return
  - a. RADIUS Filter-Id with UNP edge-profile UNP-restricted. The Edge-profile must be "UNP-restricted" because this is the UNP that has a default built-in restricted policy list associated with it.
  - b. RADIUS VSA Alcatel-Redirection-URL with a guest registration portal hosted by CPPM appended with the client MAC. Note the URL is based on the configuration done on Web Login configuration for guest as shown in the USE CASE 1 Ex:  
<https://10.255.221.137/guest/secure-access.php?mac=%{Connection:Client-Mac-Address-Colon}>

Configuration » Enforcement » Profiles » Edit Enforcement Profile - ALU Restricted Profile

Enforcement Profiles - ALU Restricted Profile

Summary Profile Attributes

**Profile:**

Name:	ALU Restricted Profile
Description:	return a radius UNP-restricted profile
Type:	RADIUS
Action:	Accept
Device Group List:	-

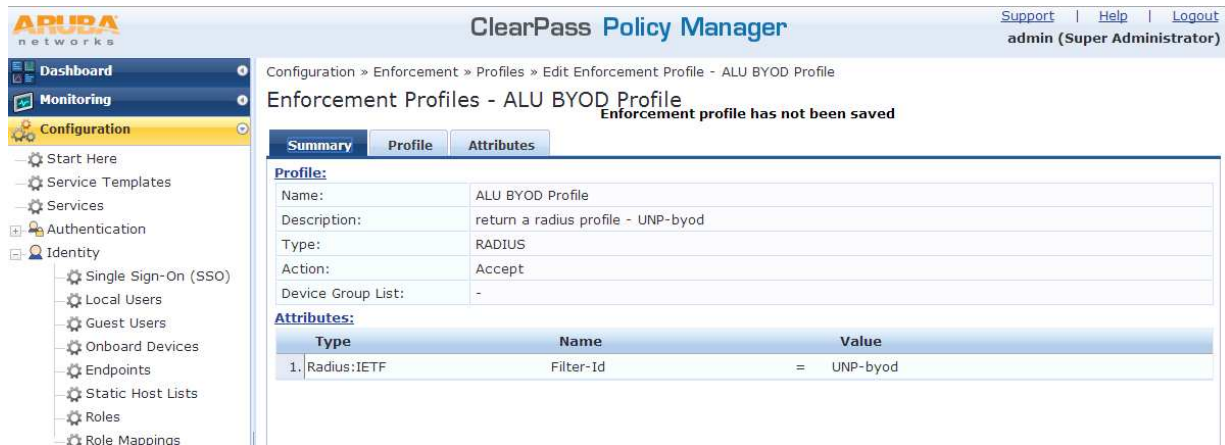
**Attributes:**

Type	Name	Value
1. Radius:IETF	Filter-Id	= UNP-restricted
2. Radius:Alcatel-Lucent-Enterprise	Alcatel-Redirection-URL	= https://10.255.221.137/guest/secure-access.php?mac=%{Connection:Client-Mac-Address-Colon}

### 5.7.2.3.2 Creating an ALU-BYOD enforcement profile

This enforcement profile should return the edge-profile defined for post onboard process for a device with the right certificate and unique user credentials obtained from the onboarding process. Create a profile as shown below. A policy list may be returned as a RADIUS VSA attribute. If not specified, the default QoS policy list of UNP-byod will be used. If an edge-profile has no default policy list, the default [Allow All] policy list is enforced by the switch.





### 5.7.2.4 Creating enforcement policy

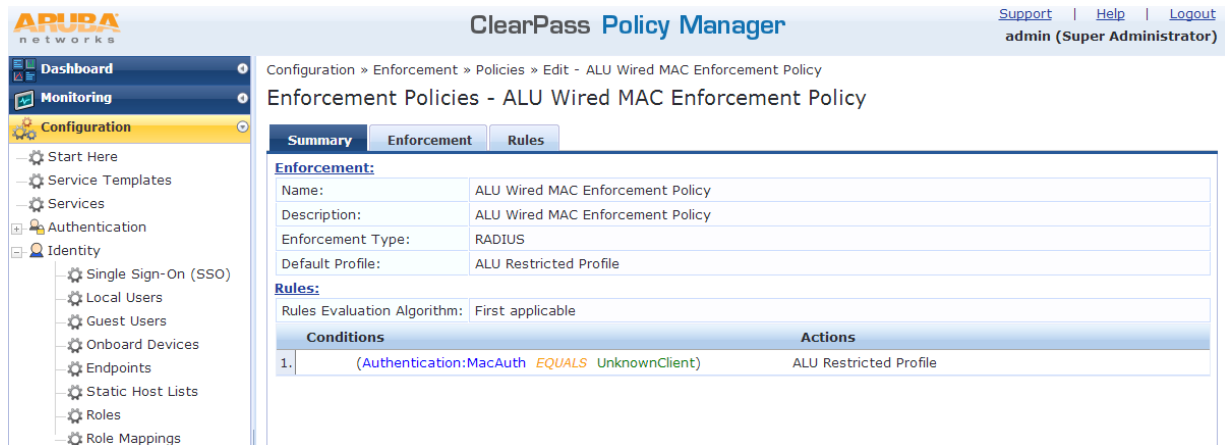
Every service is associated with an enforcement policy. Enforcement policy is configured to return different enforcement profiles based on a set of rules defined. For the Onboarding use case, there are three services that come into play:

1. MAC authentication service
2. Onboard service
3. 802.1x - post provisioning service

Each service is configured to use a different enforcement policy.

The following enforcement policies may be created as shown.

1. ALU Wired MAC Enforcement Policy to be used with MAC authentication service when user is unknown



2. Create a Wired Onboard Provisioning policy that is used in the onboard service
3. Create a Wired 802.1x enforcement policy that is used in the 802.1x post onboarding

### 5.7.2.5 Creating authentication services

We need the following services:

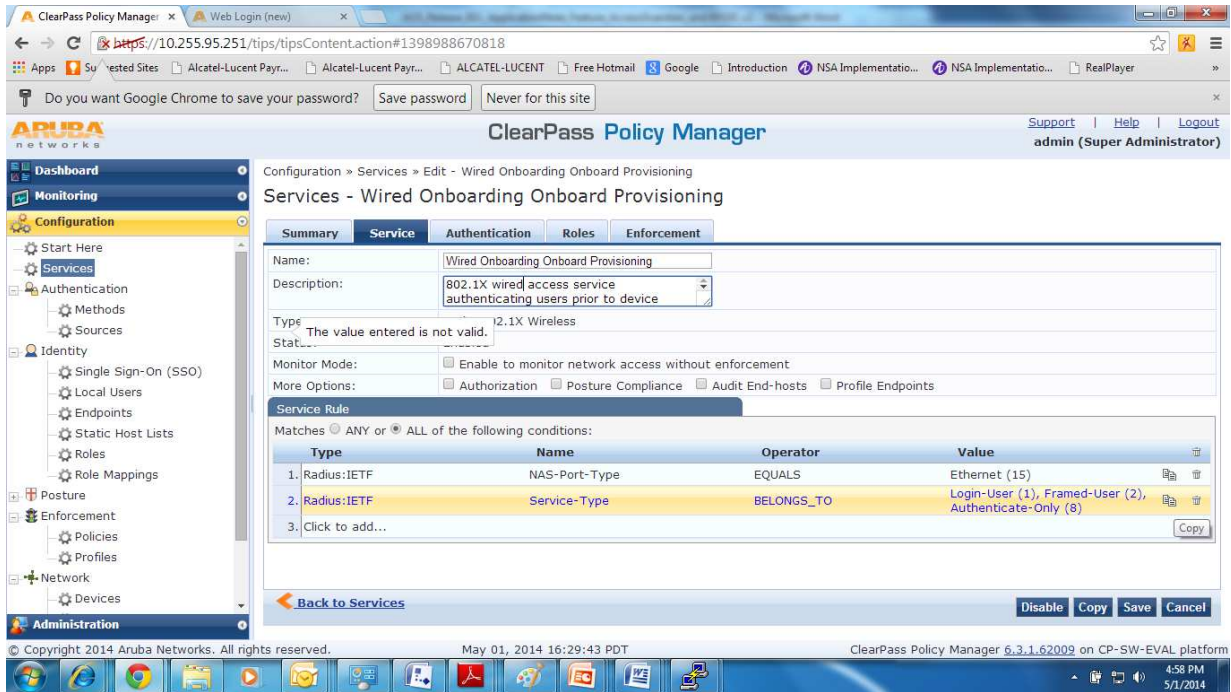
- MAC Authentication service for pre-onboard

This is the same as the one created for MAC authentication

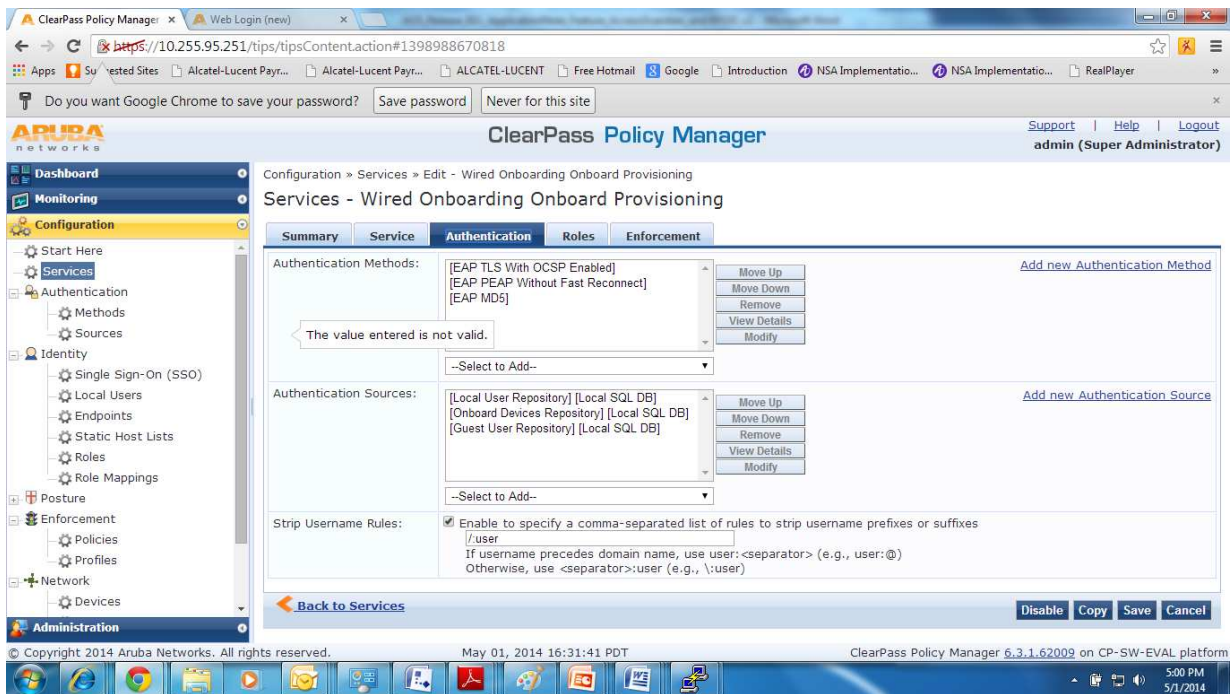
- Onboard service to accept the interaction from the Onboard module to the CPPM

A new service for wired onboarding has to be created by using the following steps:

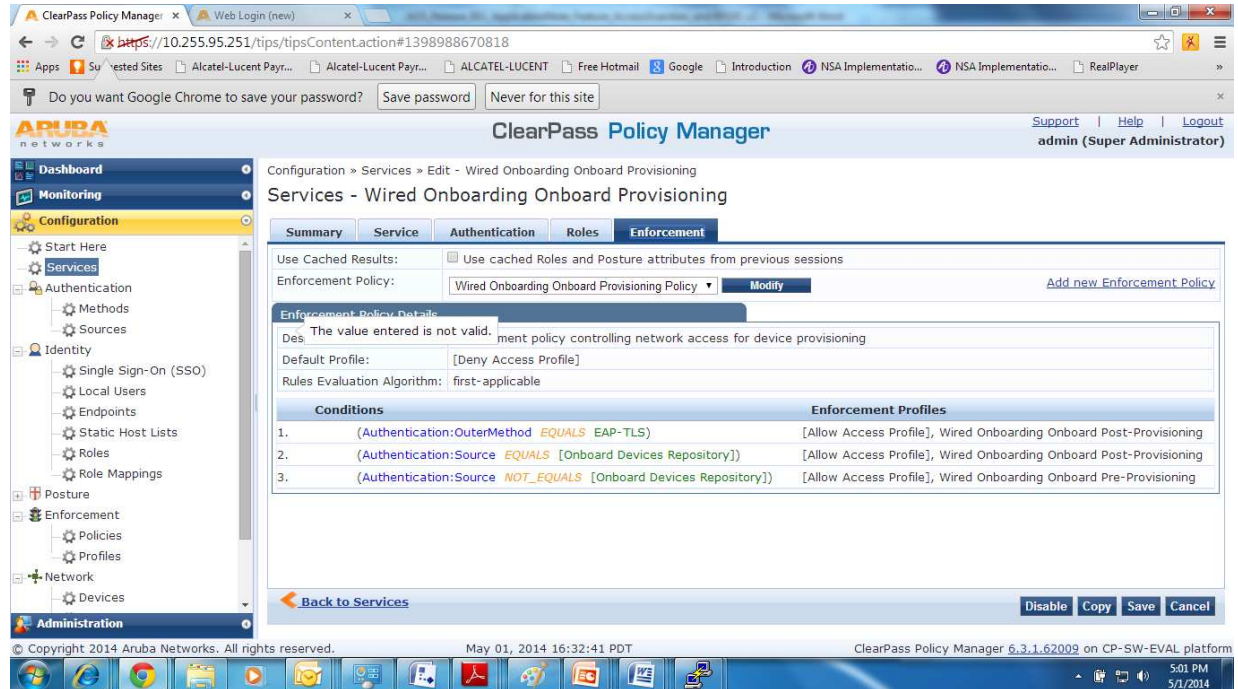
- Go to Configuration/Services and select Create a New Service



- Select the following authentication methods and sources as shown



- Set the enforcement policy that was previously created.



- 802.1x authentication service for post-onboard authentication

This is the same as the one created for 802.1x authentication.

MAC authentication service is the first service that is matched for both guest/onboard workflow. This service is configured with an enforcement policy that returns ALU Restricted Profile, which will redirect the user to a guest login/onboard page. The user is prompted to enter their user/domain credentials at this stage.

Onboard service is the next service that is matched in the workflow. This is an internal transaction triggered from the onboard device provisioning module to the CPPM. The Onboard Authorization Profile is used to authenticate the user credentials entered from the device provisioning page against the specified authentication sources Guest User Repository, Local User Repository, Onboard Device Database. Once authenticated the user certificate will be created and prompted to install the certificate and the device credentials are updated in the CPPM device database.

802.1X service is the last service that is matched in the workflow after the device provisioning and the device changes to 802.1x authentication using the new certificate and credentials installed during the provisioning phase.

NOTE: The Authentication services created have to be reordered based on which order one wants the services to be applied.

## 5.8 BYOD USE CASE 4: Guest Access/BYOD Access with Posture Check

The ClearPass Onguard module performs endpoint health checks and posture assessments to ensure that the devices are compliant. This protects the network against vulnerabilities.

ClearPass supports persistent or dissolvable agents to check for compliance and they can be used together in environments where the endpoints are either IT-owned devices or devices owned by employees or visitors.

The difference between persistent and dissolvable agents is that, persistent agents provide nonstop monitoring and automatic remediation and control. When running persistent agents on endpoints, the CPPM can centrally send system-wide notifications and alerts and allow or deny network access to the endpoints. The non-persistent agents are http-based and perform a one-time check at login to ensure compliance. Once the browser page used for authentication is closed, the dissolvable agent is removed.

If unhealthy, the endpoints receive a message about the status and the message can include reasons for remediation, links to helpful URLs and the switch authenticating the user puts the client in a restricted mode with instructions to redirect the http traffic to the remediation URL.

### 5.8.1 Enabling BYOD USECASE 1 - Guest Access with Posture

This use case can be enhanced to support Posture by taking the following steps:

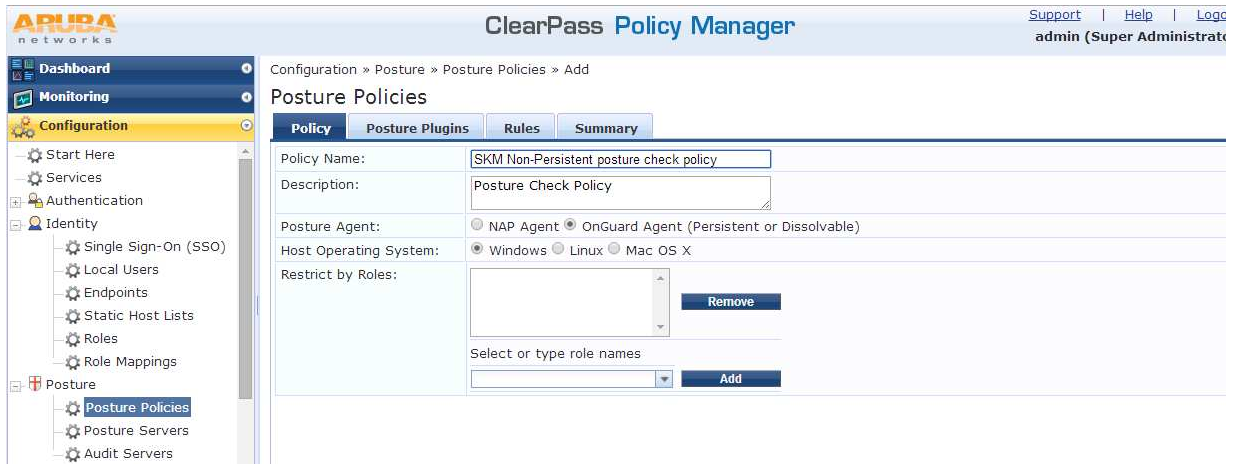
#### 5.8.1.1 Configuring the OnGuard Module on the CPPM

1. Go to Configuration/Posture/Posture Policies and select Add.

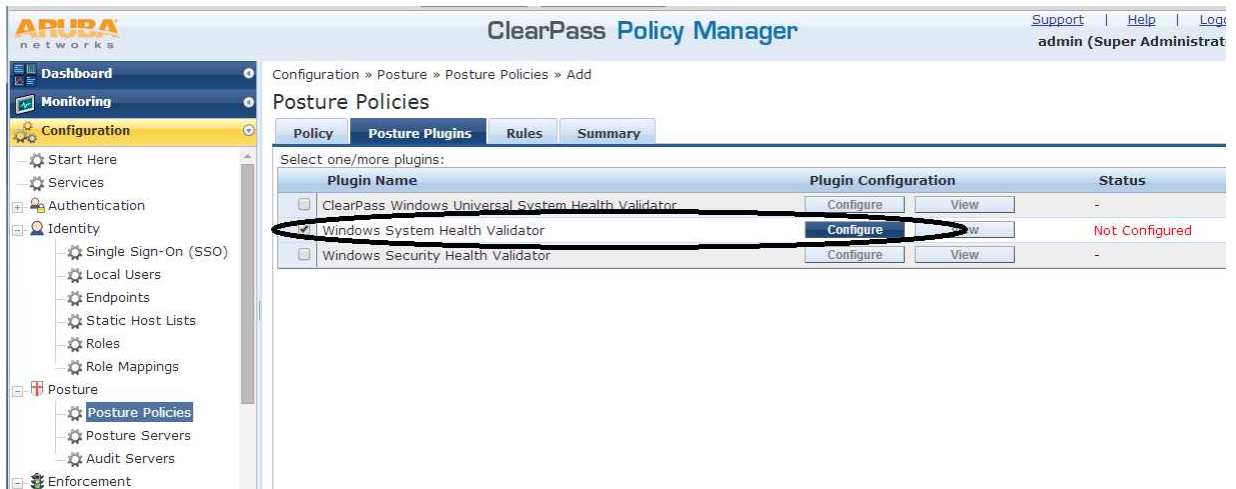


The screenshot displays the ClearPass Policy Manager web interface. The breadcrumb navigation shows 'Configuration » Posture » Posture Policies'. The page title is 'Posture Policies'. In the top right corner, there are links for 'Support', 'Help', and 'Logout', and the user is identified as 'admin (Super Administrator)'. A red circle highlights the 'Add' button in the top right corner. Below the navigation and title, there is a filter section with a dropdown menu set to 'Name' and a search box containing 'contains'. There are 'Go' and 'Clear Filter' buttons. To the right of the filter, there are 'Show 10 records' and 'Import' and 'Export All' buttons. Below the filter, there is a table with columns for '#', 'Name', and 'Description'. The table is currently empty, and a message at the bottom of the table area says 'Showing 1-2 of 2'. At the bottom right of the table area, there are 'Copy', 'Export', and 'Delete' buttons.

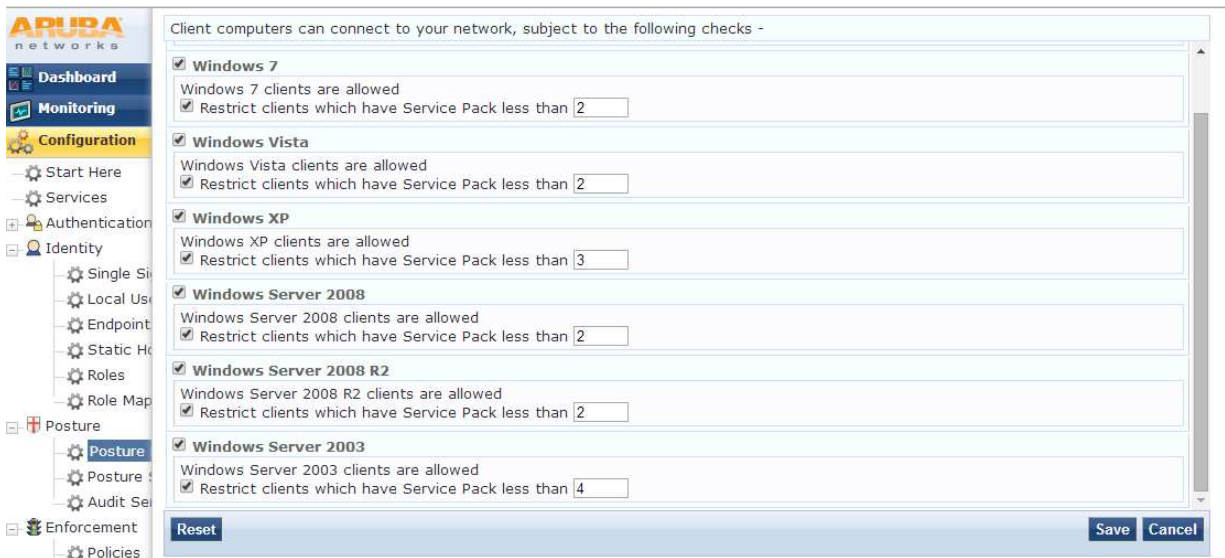
- In the Policy tab, update the Policy Name and Description. Choose the client types to validate. The example shows a health check for Windows clients only.



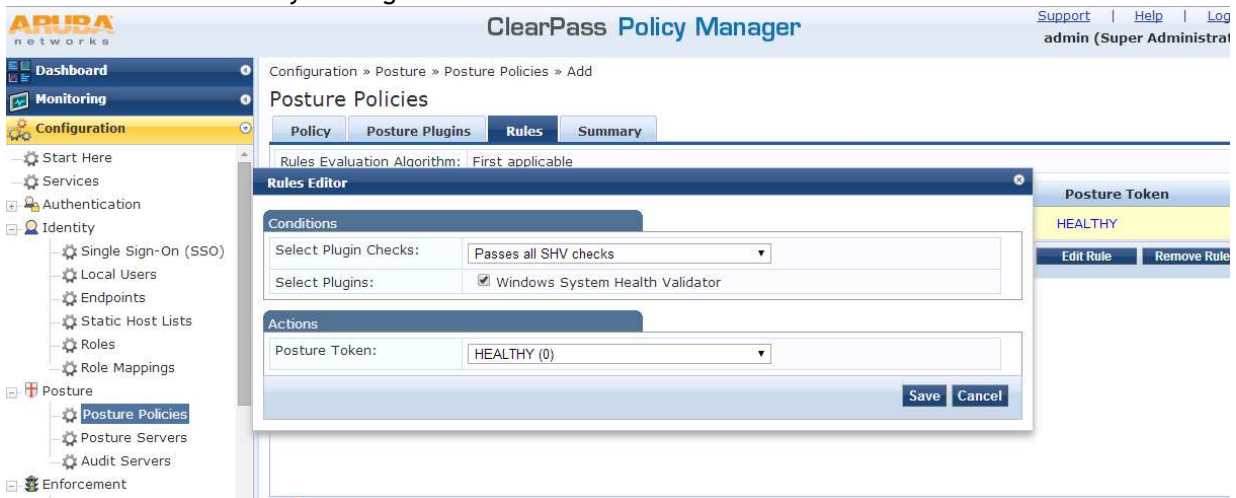
- In the Posture Plugins tab, select “Windows System Health Validator” and “Configure”.



- Select the requirements of the Windows health check appropriate for your organization and Save. The example is shown below.



5. In the Rules tab, add Rule. If all the System Health Values are PASS, then give a Posture Token of Healthy. Configure as shown below and Save.



6. In the Rules tab, add Rule. If one or more of the System Health Values are FAIL, then give a Posture Token of Quarantine. Configure as shown below and Save.



7. The Summary of the Posture Policy should be as shown below. Press Save and exit.

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar has 'Configuration' expanded to 'Posture' > 'Posture Policies'. The main content area shows the 'Summary' tab for a policy named 'Posture Check Policy'. A message at the top states 'Internal posture policy has not been saved'. The configuration details include:

- Description: Posture Check Policy
- Posture Agent: Web Agent
- Host Operating System: WINDOWS
- Restrict by Roles: (empty)

The 'Posture Plugins' section lists one plugin:

Plugin Name	Plugin Configuration	Status
1. Windows System Health Validator	<a href="#">View</a>	Configured

The 'Rules' section shows the evaluation algorithm as 'First applicable' and a list of conditions:

Conditions	Posture Token
1. Passes all SHV checks - Windows System Health Validator	HEALTHY
2. Fails one or more SHV checks - Windows System Health Validator	QUARANTINE

8. The Configured Posture Policy should be referenced in the Web Authentication Services that are enabled for Posture Check as shown in the following sections.

### 5.8.1.2 Enabling Posture Check in the Web Login page defined for guest registration

1. Go to the Guest Module.
2. Go to Guest/Configuration/Web Login.
3. Select the Web Login page that was created before.
4. Select "Edit" to edit the Web Login page configuration.
5. Go to the bottom of the page and check Health Check as shown below and Save.

The screenshot shows the 'ClearPass Guest' configuration page. The left sidebar has 'Guest' expanded to 'Configuration' > 'Web Login'. The main content area shows the 'Post-Authentication' section. Under 'Actions to perform after a successful authentication', the 'Health Check' checkbox is checked, and the text 'Require a successful OnGuard health check' is circled in red. Below this, it says 'If selected, a health check will be required before the user is granted access to the network.'

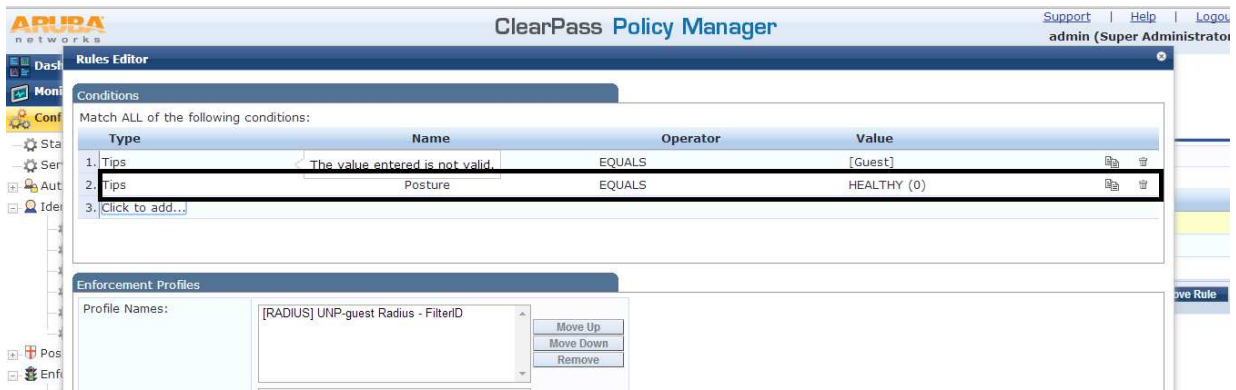
This will trigger a health check on the endpoint post authentication process. The health check will stop as soon as the browser used for login is closed. If the health check process was incomplete, the endpoint will remain in an Unhealthy state. If the health check was successful, the endpoint status is set to Healthy and the appropriate edge-profile/role is enforced on the switch for the endpoint.

### 5.8.1.3 Modify or create an enforcement policy with Posture Check

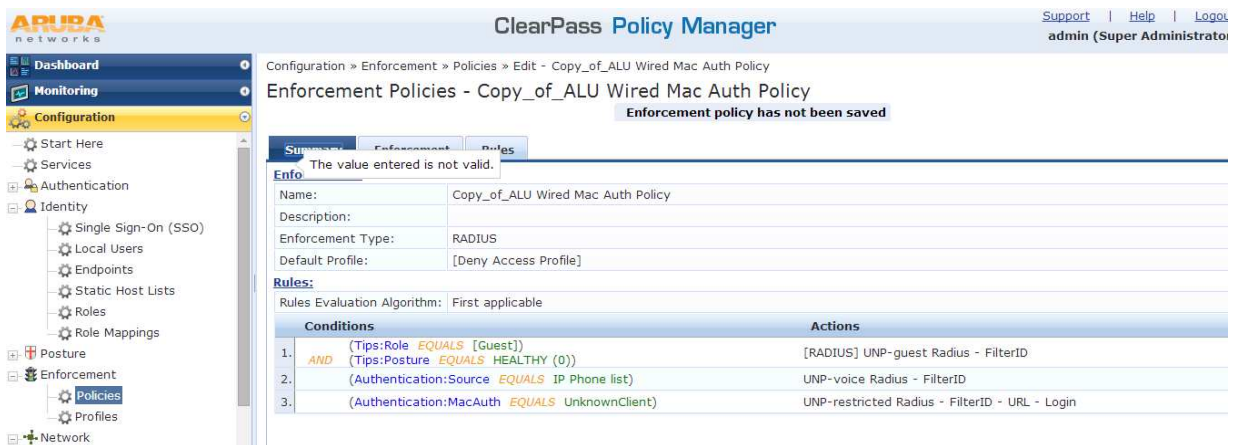
1. Go to Configuration/Enforcement/Policies, select Wired MAC Auth Enforcement Policy and add a rule to check for healthy state of the client. Select the rule and select Edit.



2. Add a new rule as shown below: Type (Tips) Name(Posture) Operator(EQUALS) Value (HEALTHY(0))



3. The modified Enforcement Policy should be as follows

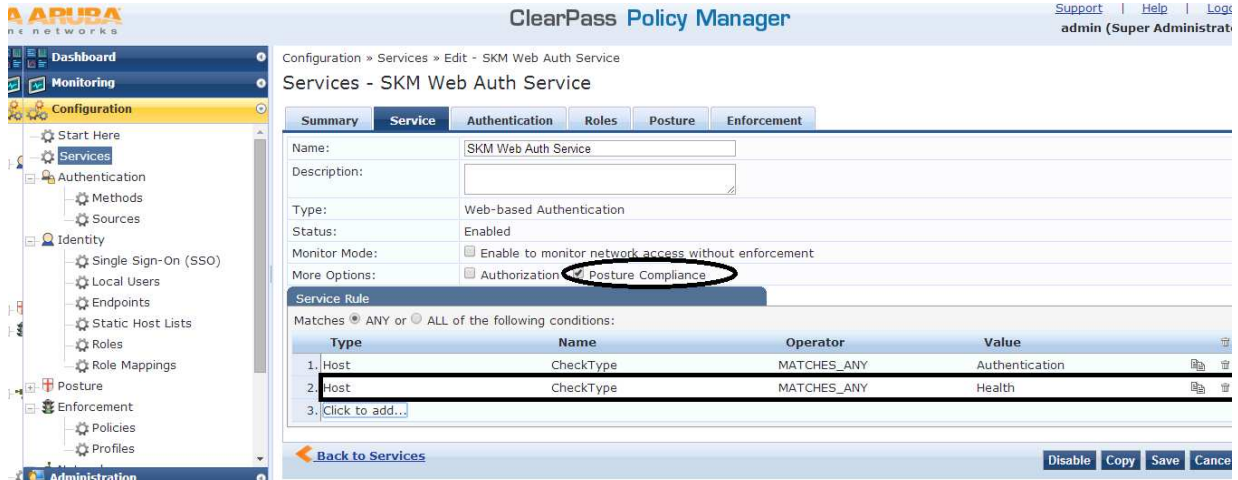


### 5.8.1.4 Modify the Web Authentication Service

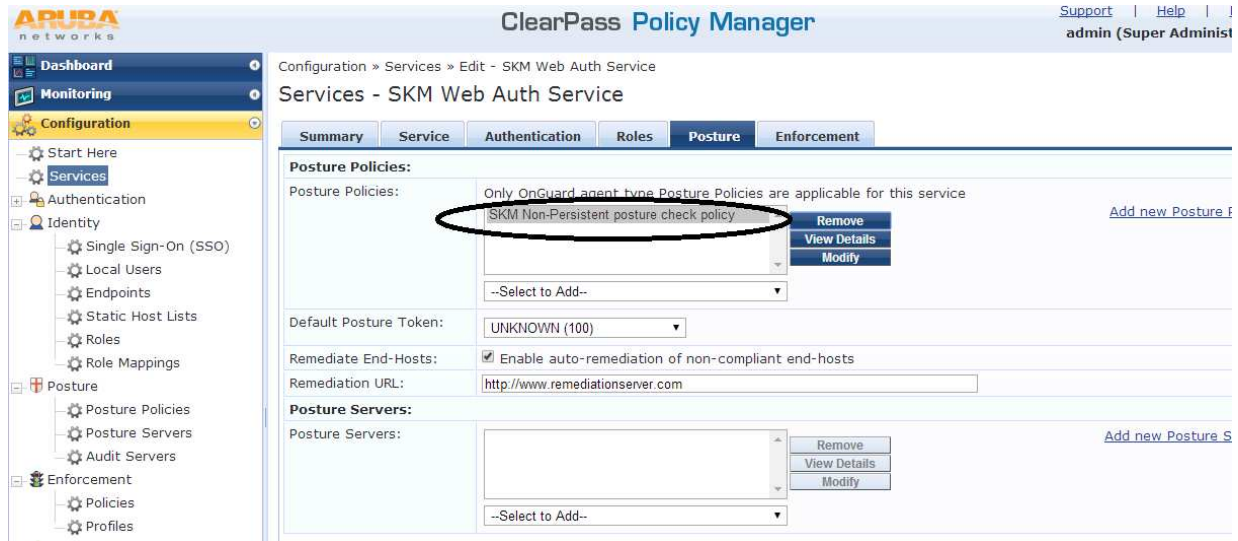
1. Go to CPPM/Configuration/Services.



2. Select the Web Authentication Service created for Guest Registration/Login.
3. Select Posture Compliance and add a new Service Rule as shown below.



4. Go to the Posture tab and select the following settings as shown. The remediation URL may be specified to assist the user to get remediation



5. Go to the Enforcement tab and apply the appropriate enforcement policy which was created.

The screenshot shows the ClearPass Policy Manager interface. The left sidebar contains a navigation menu with sections: Dashboard, Monitoring, and Configuration. Under Configuration, there are sub-items: Start Here, Services, Authentication, Identity, Posture, Enforcement, Policies, Profiles, and Network. The main content area is titled 'Services - SKM Web Auth Service' and has tabs for Summary, Service, Authentication, Roles, Posture, and Enforcement. The Enforcement tab is active, showing 'Use Cached Results' and 'Enforcement Policy' dropdown set to 'SKM\_Non-persistent Wired Posture Enforceme'. Below this is the 'Enforcement Policy Details' section with a table:

Enforcement Policy Details	
Description:	Wired Posture Enforcement Policy
Default Profile:	[Update Endpoint Unknown]
Rules Evaluation Algorithm:	first-applicable
Conditions	Enforcement Profiles
1. AND (Tips:Posture EQUALS HEALTHY (0)) (Tips:Role EQUALS [Guest])	UNP-guest CoA - FilterID
2. (Tips:Posture NOT_EQUALS HEALTHY (0))	UNP-quarantine CoA - FilterID

Steps of the Guest Access and Posture Check are as follows:

1. The client connects to a UNP edge port enabled for MAC authentication.
2. The switch sends a RADIUS MAC authentication request to the CPPM.
3. Since the client is UNKNOWN, the MAC authentication service will send a RADIUS response with:
  - a. Filter-Id equals UNP-restricted
  - b. Redirection URL equals the Guest registration URL appended with the client MAC
4. The switch applies the built-in restricted policy list associated with UNP-restricted, which allows only DHCP, DNS, ARP, ICMP and traps http/https traffic to CPU.
5. The client MAC is learned in the VLAN associated with UNP-restricted and the client gets the IP address in the VLAN from the DHCP server.
6. When the client opens a browser, the traffic is redirected to the redirection URL.
7. The client can enter the username/password received via sponsorship or self-register to get a username/password. The sponsored or self-registered user information is created in the Guest User Database.
8. After authentication, the posture process checks the conditions defined by the posture policy.
9. Once the posture check determines the client is healthy, the RADIUS CoA is sent with the Filter-Id equals UNP-guest.
10. If the VLAN associated with UNP-guest VLAN is different from the VLAN associated with UNP-restricted VLAN (which will most likely be the case), the port-bounce (or pause-timer) will be enforced.
  - a. Port bounce will result in client information flushed and the MAC authentication initiated on the first packet from the client after port bounce. The MAC authentication service will determine the client is KNOWN from the previous authentication cycle and using the cached role and posture status information send RADIUS response with Filter-Id equals UNP-guest.
  - b. Port timeout will result in client traffic being filtered for a duration of time and after that the client is learned and the new role assigned.

### 5.8.2 Enabling BYOD USECASE 3 - Onboard with Posture

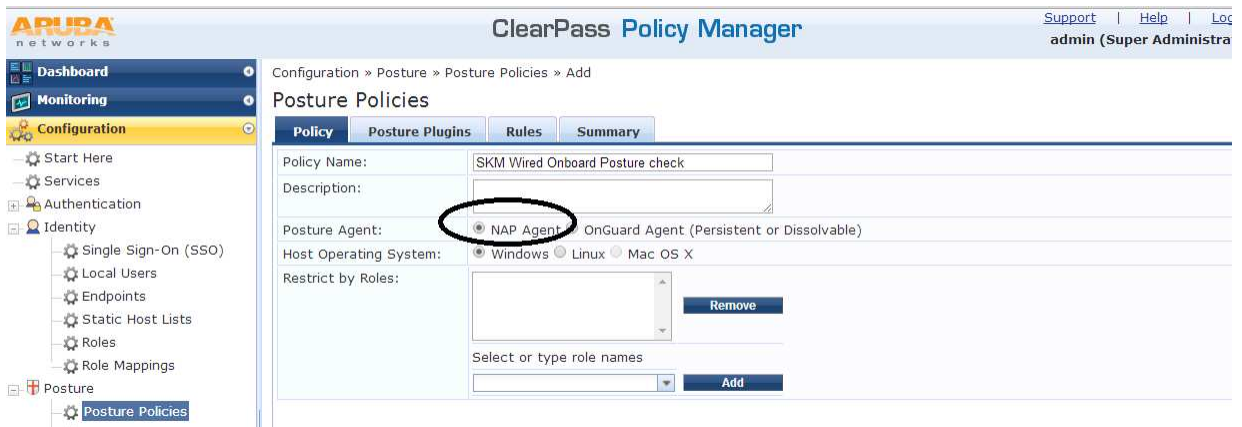
This process is required to check the status of the employee-owned devices that are being onboarded onto the organization's network.

### 5.8.2.1 Configuring the OnGuard Module on the CPPM

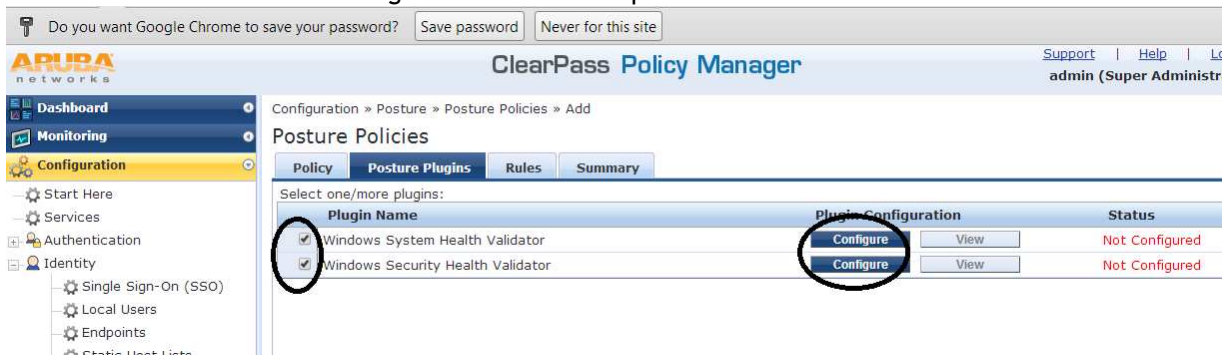
1. Go to Configuration/Posture/Posture Policies and select Add.



2. In the Policy tab, update the Name/Description. Choose the client types to validate. The Posture Policy for onboard only supports a NAP agent.



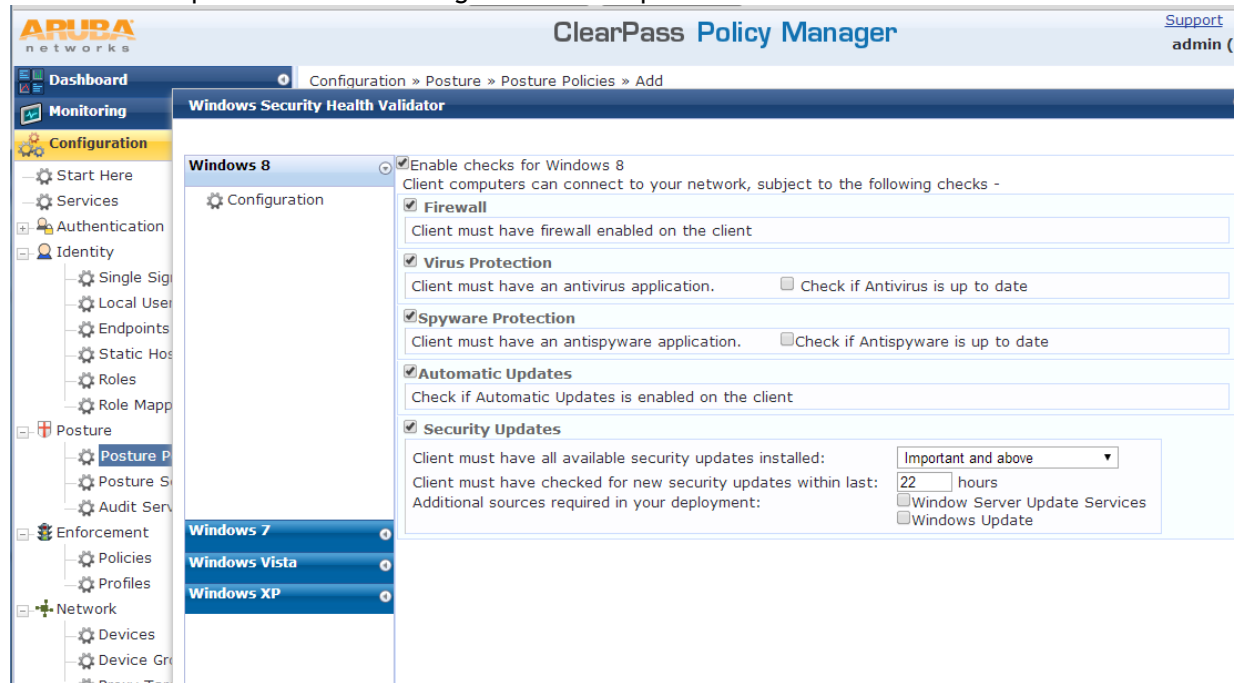
3. In the Posture Plugins tab, select “Windows System Health Check” and “Windows Security Health Validator”. Configure each one as required.



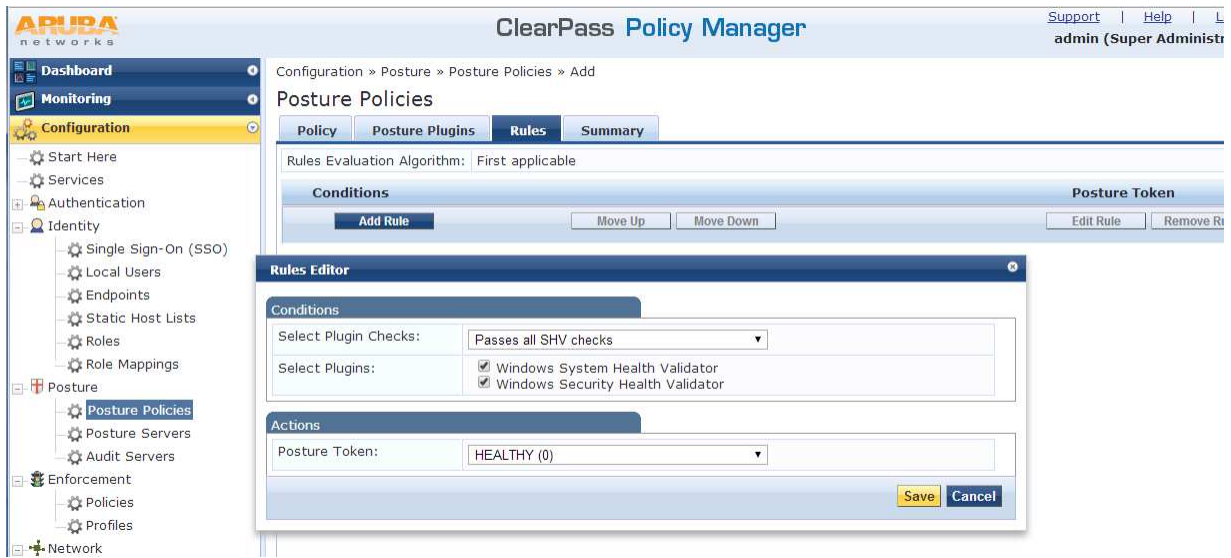
4. Select the requirements of the Windows health check appropriate for your organization and Save. An example is shown below.



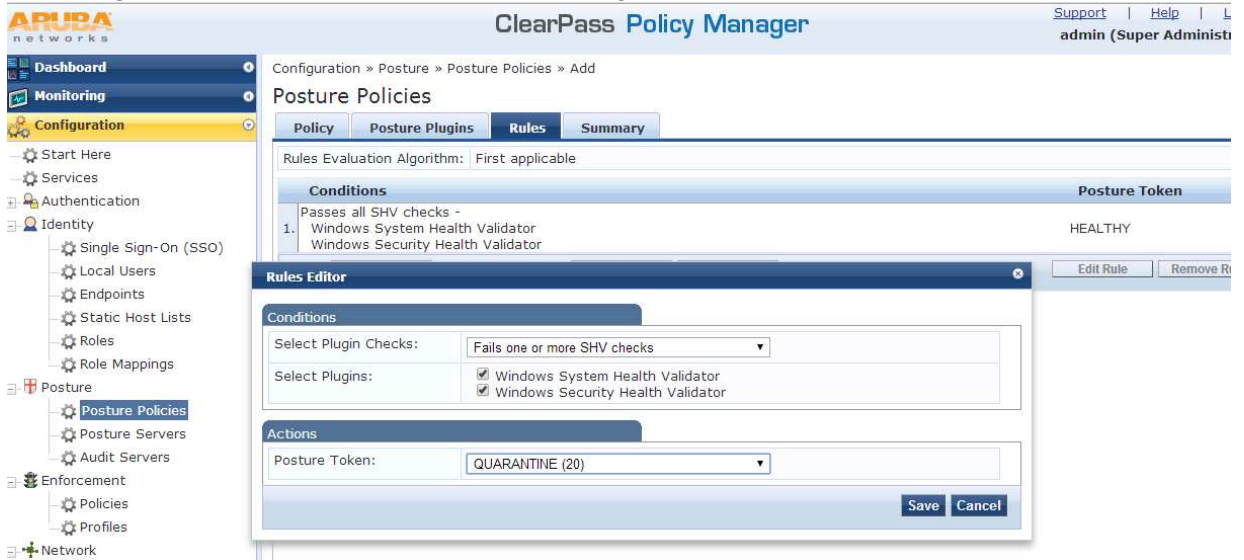
- Continue to configure the Windows Security Health by selecting Configure and then Save. An example is shown below. Configure for all the Windows OS and select the applications to check for and update based on the organization’s requirement.



- In the Rules tab, add Rule. If all the System Health/Security Values are PASS, then give a Posture Token of Healthy. Configure as shown below and Save.



7. In the Rules tab, add Rule. If one or more of the System Health/Security Values are FAIL, then give a Posture Token of Quarantine. Configure as shown below and Save.



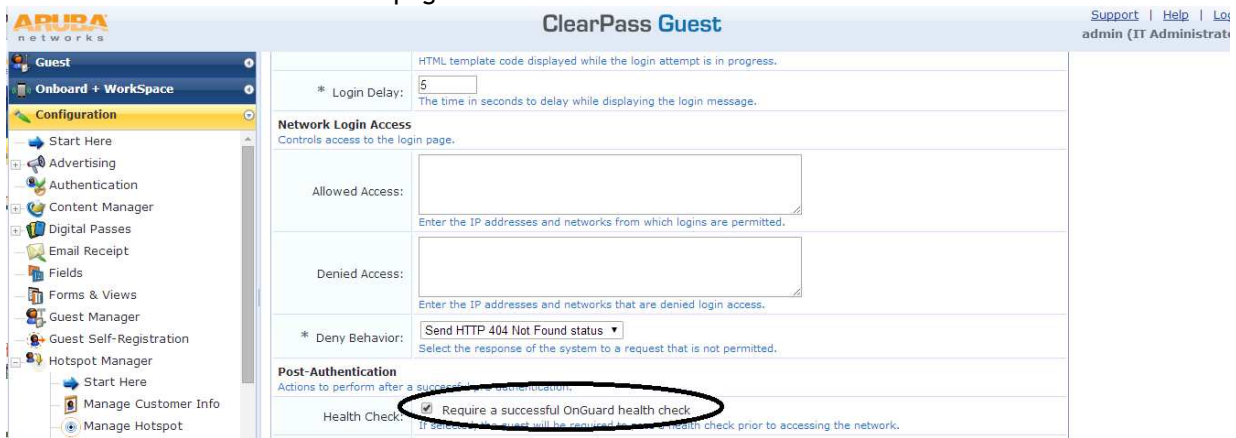
8. The Summary of the Posture Policy should be as shown below. Press Save and exit.



9. The Configured Posture Policy should be referenced in the Onboard Web Provisioning Service that is enabled for Posture Check as shown in the following sections.

### 5.8.2.2 Enabling Posture Check in the Web Login page defined for onboarding

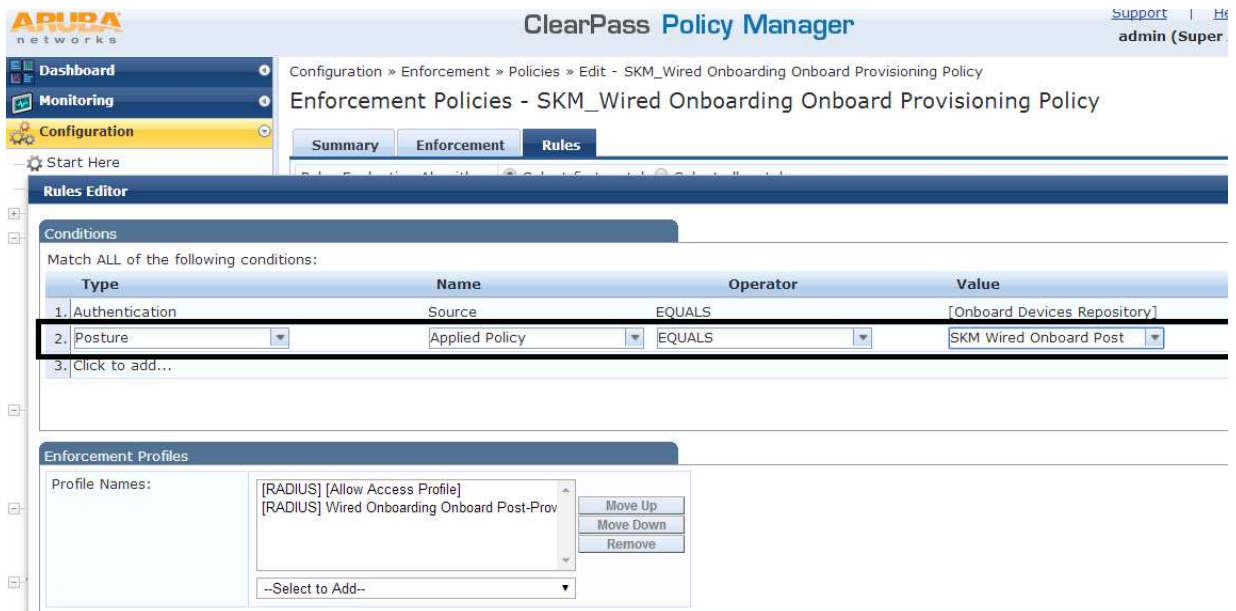
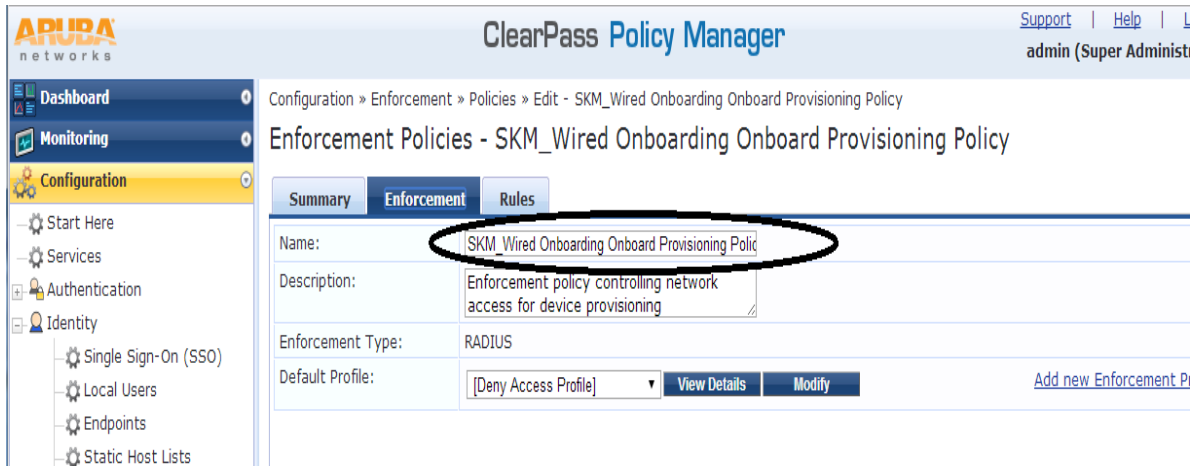
1. Go to the Guest Module.
2. Go to Guest/Configuration/Web Login.
3. Select the Web Login page that was created before.
4. Select “Edit” to edit the Web Login page configuration.
5. Go to the bottom of the page and check Health Check as shown below and Save.



This will trigger health check on the endpoint post authentication/onboarding process. The health check will stop as soon as the browser used for login is closed. If the health check process was incomplete, the endpoint will remain in the UnHealthy state. If the health check was successful, the endpoint status is set to Healthy and the appropriate edge-profile/role is enforced on the switch for the endpoint.

### 5.8.2.3 Modify or create an Onboard Enforcement Policy with Posture Check

1. Go to Configuration/Enforcement/Policies and select SKM Wired Onboard Enforcement Policy. Add a rule to check for healthy state of the Client. Select the rule and select Edit.

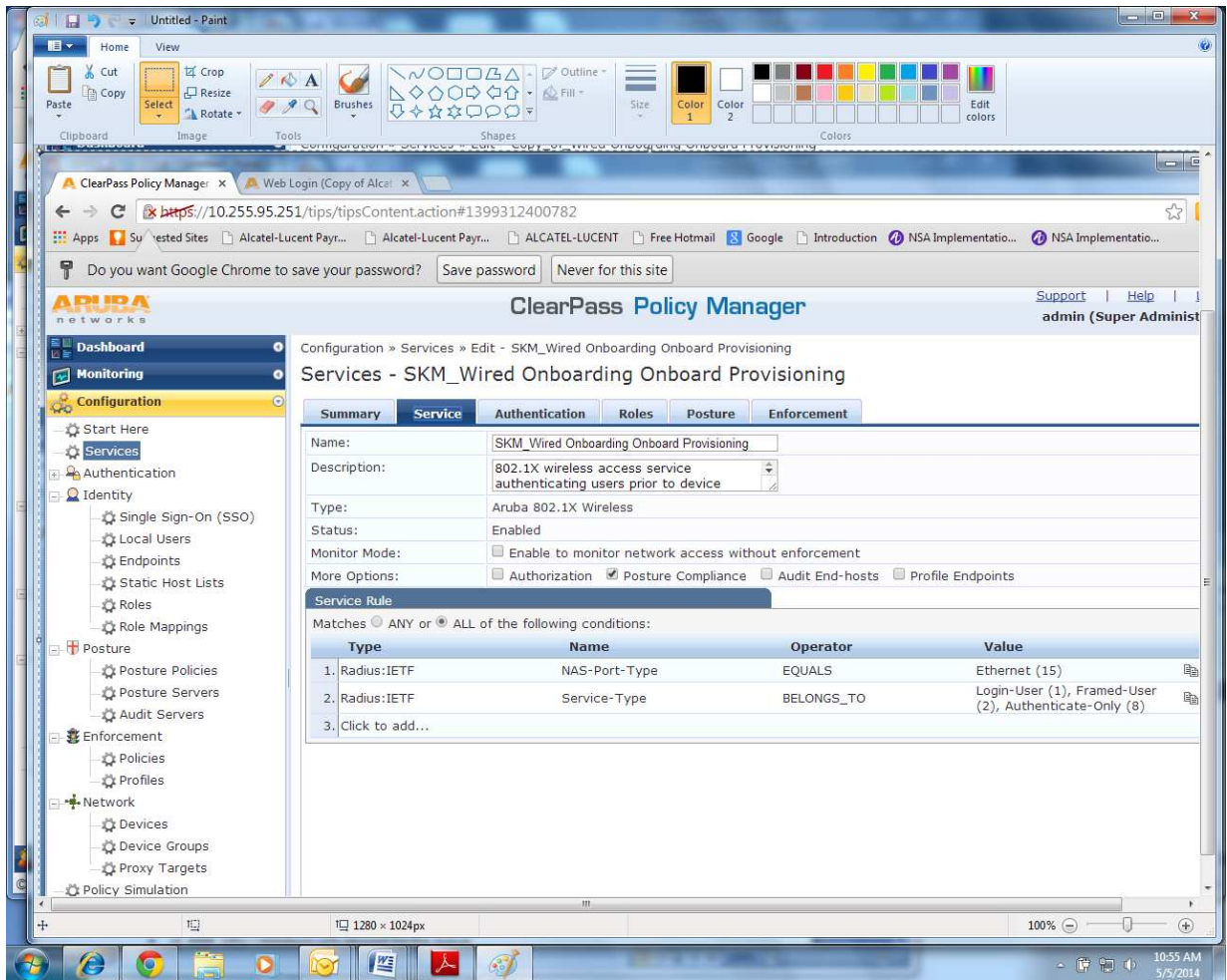


2. The modified Enforcement Policy should look like the following:



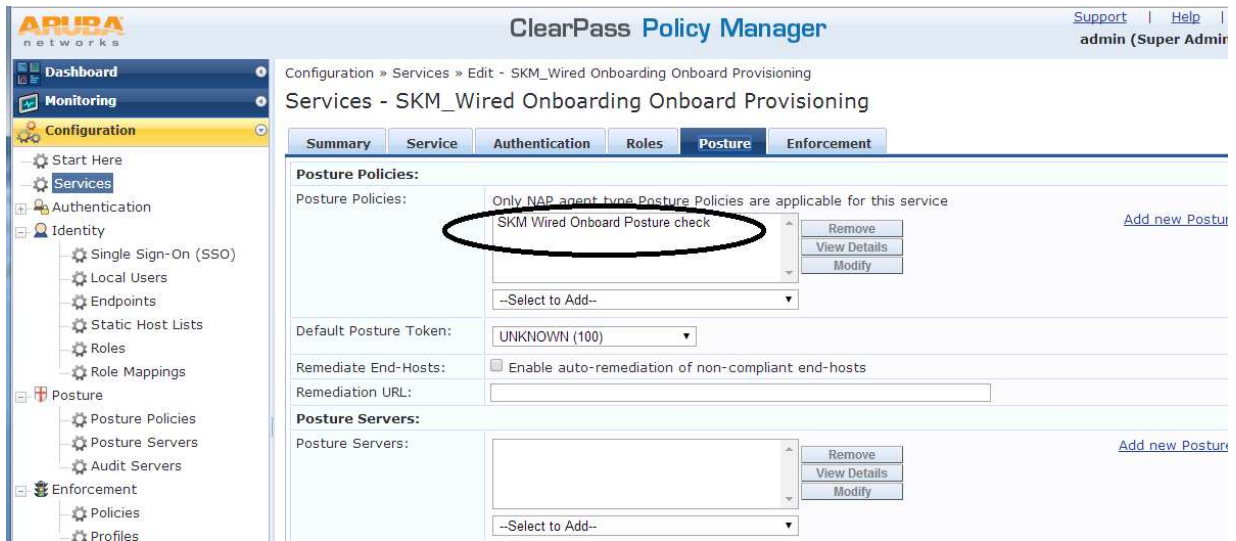
### 5.8.2.4 Modify the Wired Onboard Provisioning Service

1. Go to CPPM/Configuration/Services.
2. Select the Onboard Provisioning Service created for Guest Registration/Login.
3. Select Posture and add a new Service Rule as shown below.

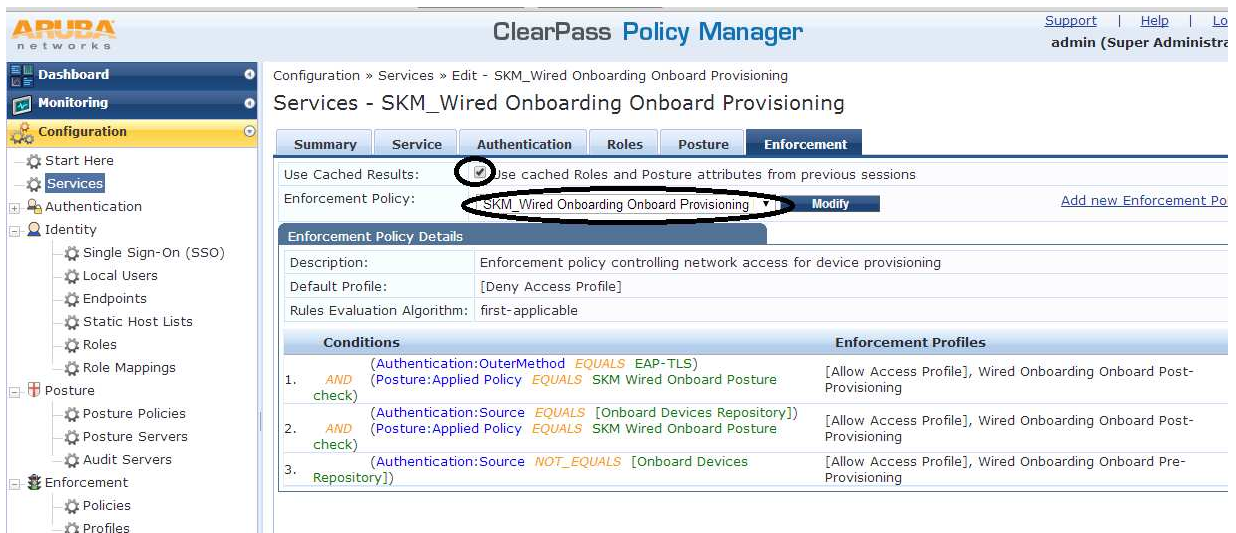


4. Go to the Posture tab and select the following settings as shown. The remediation URL may be specified to assist the user to get remediation.



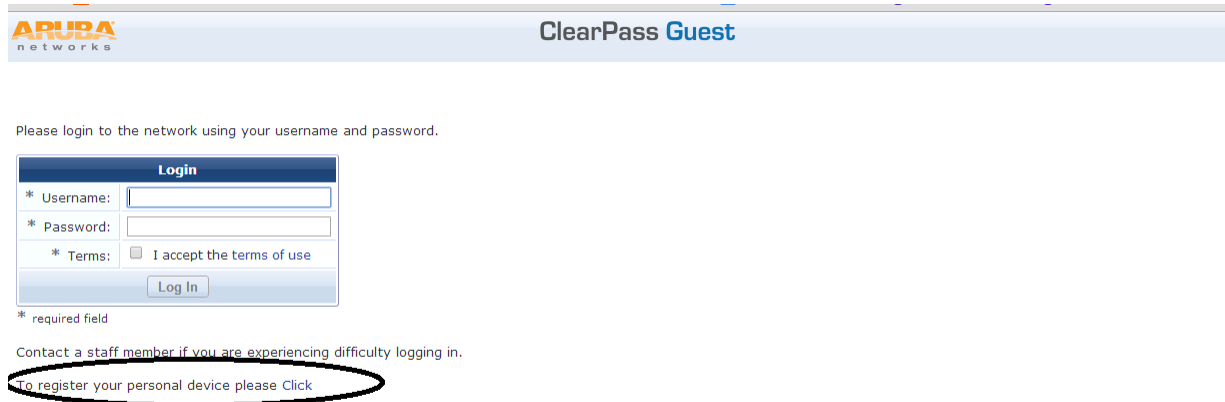


5. Go to the Enforcement tab and apply the appropriate enforcement policy which was created above.

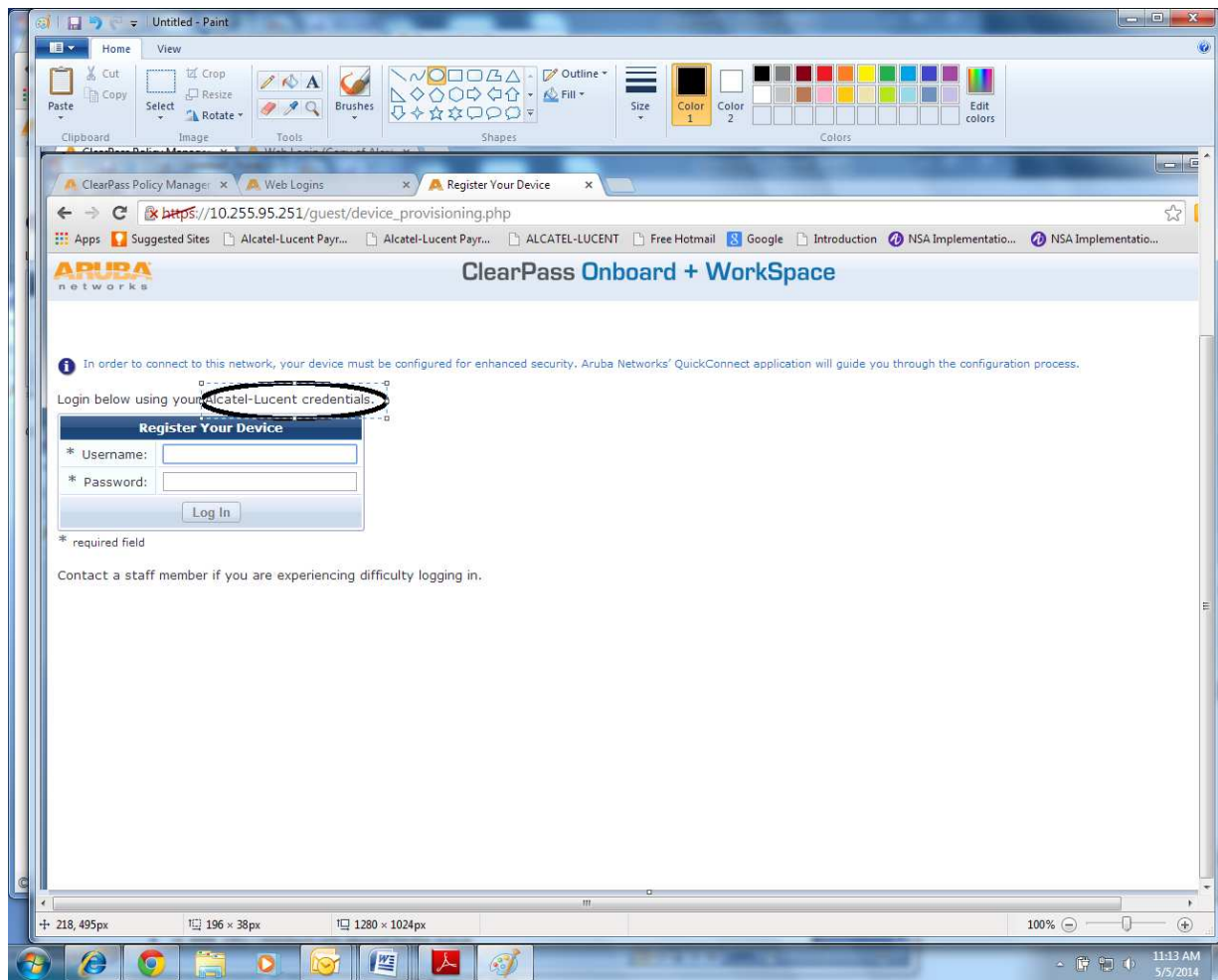


Steps of the Onboarding and Posture Check are as follows:

1. The Client connects to a UNP edge port enabled for MAC/802.1x authentication.
2. Consider a non-suplicant device, the switch sends a RADIUS MAC authentication request to the CPPM.
3. Since the client is UNKNOWN, the MAC authentication service will send a RADIUS response with:
  - a. Filter-Id equals UNP-restricted
  - b. Redirection URL equals the Guest registration URL appended with the client MAC
4. The switch applies the built-in restricted policy list associated with UNP-restricted, which allows only DHCP, DNS, ARP, ICMP and traps http/https traffic to CPU.
5. The client MAC is learned in the VLAN associated with UNP-restricted and the client gets the IP address in the VLAN from the DHCP server.
6. When the client opens a browser, the traffic is redirected to the redirection URL.
7. Since the client is an employee with a non-IT device, the appropriate onboarding link should be selected from the Redirection page as shown below.



8. The employee is required to enter the employee credentials to be able to onboard the device.



9. The onboarding will first begin where the client is prompted to install an agent. This will include installing certificates, changing the 802.1x settings on the client and installing the NAP agent that is enabled.

10. The NAP agent will update the CPPM of the posture status. The client port is bounced automatically.
11. The 802.1x authentication is initiated with the newly installed certificates and the client is authenticated and onboarded.

## 6 Glossary

AAA	Authentication, Authorization and Accounting
AG	Access Guardian
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CA	Certificate Authority
COA	Change of Authorization (RADIUS RFC3576)
CPPM	ClearPass Policy Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPI	Deep Packet Inspection
EAP	Extensible Authentication Protocol (RFC 3748)
EAP-TLS EAP	Transport Layer Security (RFC 5216), a certificate-based authentication method supporting mutual authentication, integrity protected cipher suite negotiation and key exchange between two endpoints
EAP-PEAP	Protected EAP is a protocol for securely transporting authentication data across a network
ICMP	Internet Control Message Protocol
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
NAC	Network Access Control
QMR	Quarantine Manager and Remediation
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
URL	Universal Resource Locator

[www.alcatel-lucent.com](http://www.alcatel-lucent.com) Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2014 Alcatel-Lucent. All rights reserved. 20140600002 (July)